A Methodology for Monitoring the Ground-Based Augmentation System (GBAS) Category I Integrity Risk

Paulo Elias, Osamu Saotome
ITA – Instituto Tecnológico de Aeronáutica – Praça Marechal Eduardo Gomes, 50 - Vila das Acácias, CEP 12.228-900 - São José dos Campos – SP – Brasil

Abstract **— This paper describes a method to accomplish the Ground-Based Augmentation System (GBAS) 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 (GBAS) ground station. The methodology described here is based on the Risk Tree Analysis (RTA) technique, which is an optional way to design and develop an engineering solution named as integrity risk monitor (IRM) that assures the integrity risk requirement for standard system architecture. The results demonstrated here is regarding to the qualitative and the 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 (IRM) explained here is an optional architectural solution (a practical way) which have demonstrated a satisfactory result to meet the certification basis of the Aeronautical Authorities.**

Keywords **— GBAS, Risk, Integrity, Safety.**

I. INTRODUCTION

In the last years the Aeronautical Industry has been worked in development of a variety of assurance technologies to meet, or to exceed, the design assurance levels (DAL) of airborne systems, and it has been reached satisfactorily. Once the certification aspects are met, then the system safety and the design assurance levels (DAL) can be accomplished and demonstrated through analyses, tests, and in-the-field services and statistical data. But, in the ground systems segment there is no useful body of knowledge (BoK), or almost nothing has been done to solve the engineering problems regarding to the requirements to develop a safe-design. In this context the new generation of aeronautical navigation aids appears, in special the ground-based augmentation system (GBAS) for Category I approach and landing procedures. The GBAS CAT I system is the current World Wide 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 system is part of GBAS total system, which is based on GNSS satellite signals pseudo range measurements and corrections. The integrity requirement for a GBAS system, specified by ICAO [2], is:

$$\text{Integrity} = 1 - 2\times10^{-7} / approach.$$

Paulo Elias, pelias2011@bol.com.br, Osamu Saotome, osaotme@ita.br,

From this value, this paper presents a methodology to meet the minimum aspects of the GBAS system safety, in special the integrity risk requirement of the ground station Category I GBAS, by applying an engineering architectural solution based on risk assessment considerations and good practices. A technique for risk assessment is presented here and is known as risk tree analysis (RTA) [2]. Some definitions are important to clarify the rationale and facilitate the understanding of results, for example, the meaning of integrity, misleading information, and integrity risk are defined upon the sections of this paper.

Integrity Allocation Methodology

The integrity allocation methodology considered for this paper is the same issued in [3] and is illustrated in Fig. 03.

Integrity, considered a system attribute, is defined [3] 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 time-to-alert (TTA) of a GBAS Category I is 3 seconds [2].

An implicit assumption is that a Navigation System Error (NSE) greater than the alert limit bound for greater than the time-to-alert is a condition that is hazardous for a CAT I approach. This paper refers to this condition as misleading information (MI). All misleading information 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 and on all ranging sources. The H1 hypothesis represents a fault associated with any one, and only one, reference receiver. Under the H1 hypothesis, a fault includes any erroneous measurement(s) that is 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 SIS is further allocated into two basic categories:

1. Integrity resulting from the NSE being bounded by the protection levels under the H0 and H1 hypothesis.
2. Integrity resulting from all other conditions not covered by H0 and H1.

The total integrity requirement on the probability of misleading information is allocated to the categories illustrated in Fig. 03. The figure 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. The cases not covered by H0 and H1 include the following:

- Failures in the ground system
- Erroneous broadcast of critical data due to failure in ground sub-system processors (e.g., corrections, B-values, sigma terms, etc.);
    - Undetected failures of measurements from more than one reference receiver (e.g., correlation between RR measurements becomes unacceptably high and is not accounted for in broadcast terms);
    - VDB channel message failure or 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 estimate
    - Environmental conditions (e.g., failure of ground monitor to detect change in environment that affects broadcast 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 such that the probability of misleading information 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 [3]. Generically, it represents the time during which the loss of integrity, and potentially resulting misleading information, exposes the aircraft to a hazard. Final approach begins at the final approach fix, which is nominally located at 5 NM and an altitude of 1600 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 sec. The hazard severity for misleading information 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).

Integrity Risk Computations with GBAS

The issue then is how to apply this approach to computing integrity for GBAS [3]. Since GBAS architectures typically are not the same as conventional navigation systems, which consist of a transmitter and an independent monitor, the equation for calculating risk can be represented more generically as:

$$Risk = 1 - Integrity = P_{SIS} P_{md}$$

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 types 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. Fig. 03 is the risk allocation tree for GBAS CAT-I.

$$Risk(Total) = Risk(H_0) + Risk(H_1) + Risk(H_2)$$

Each of these risk types is explained and broken down in more detail in the following sections. The relationship between the computed risk and time is described along with a proposed methodology for handling time.

Fault Free Integrity Risk (H_0)

$$Risk(H_0) = P_{ffmd}$$

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 (2 times 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, etc.). 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 10 seconds for CAT I [3]. Therefore, there are a number of independent events during the period of an approach. This has to be taken into account in determining K_{ffmd} .

Single Reference Receiver Fault Integrity Risk (H_1)

$$Risk(H_1) = P_{RR\_Fault} P_{H1\_md}$$

Where

P_{RR_Fault} = Probability of a fault associated with one Reference Receiver

P_{H1_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 [3]:

- Ranging source faults
- Ground-subsystem faults, and
- Atmospheric anomalies (Ionospheric effects, etc.)

$$Risk(H_2) = Risk(Ranging\_Source\_Fault) + Risk(Ground\_Subsystem\_Fault) + Risk(Atmospheric\_Anomaly)$$

$$Risk(Ranging\_Source\_Fault) = P_{RS\_Fault} P_{RS\_md}$$

$$Risk(Ranging\_Source\_Fault) = \lambda_{RS\_Fault} T_{RSIS} P_{RS\_md}$$

Where

P_{RS_Fault} = Probability of Hazardous Ranging Source Failure

λ_{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

$$Risk(Ground\_Subsystem\_Fault) = P_{Corr\_Fault} P_{Corr\_Mon\_md}$$

$$Risk(Ground\_Subsystem\_Fault) = \lambda_{Corr\_Fault} T_{Corr\_Mon\_Ver} P_{Corr\_Mon\_md}$$

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 system 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 sec. This does not take into account failures that not be detected by the voting scheme.

$$Risk(Atmospheric\_Anomaly) = P_{AA} P_{AA\_md}$$

$$Risk(Atmospheric\_Anomaly) = \lambda_{AA} T_{AAIS} P_{AA\_md}$$

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 to detect it.

A Methodology for Designing the Integrity Risk Monitor (Subsystem Level)

Step 1: Define the system architecture to be monitored (e.g., GBAS CAT I ground station presented in RTCA/DO-245A [3]):

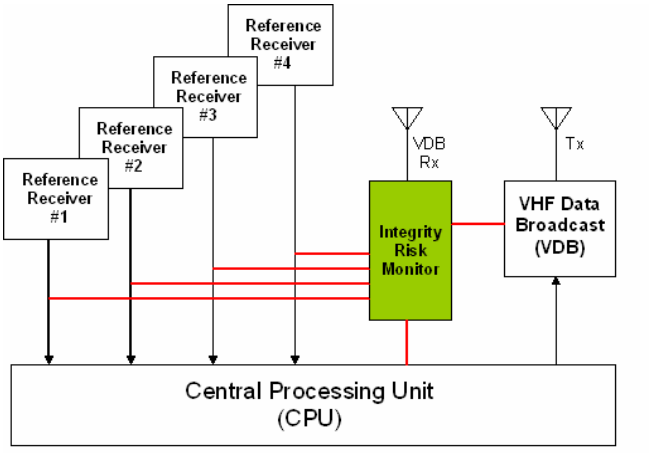


Fig. 01. GBAS Ground System Block Diagram with IRM

The Integrity Risk Monitor (IRM) architecture showed in the Fig. 01 is a generic concept that may be applied to the GBAS ground systems composed by four Reference Receivers (RR), where these four RR are identical and only 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) [2]. The ICAO, Annex 10 [2] has a section which 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.

Step 2: Define the integrity risk tree of the GBAS ground system to be monitored (qualitative approach).
The Integrity Risk Tree is the second step for constructing the Integrity Risk Monitor structure, and then an algorithm may be architected (it will be embedded to the Integrity Risk Monitor). For a system hierarchical purpose, the IRM is a GBAS Subsystem Unit.
The GBAS Integrity Risk Allocation [3] is presented in the Figure 2.

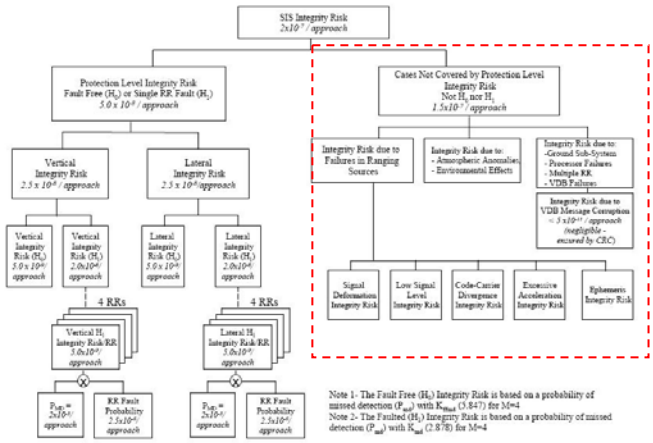
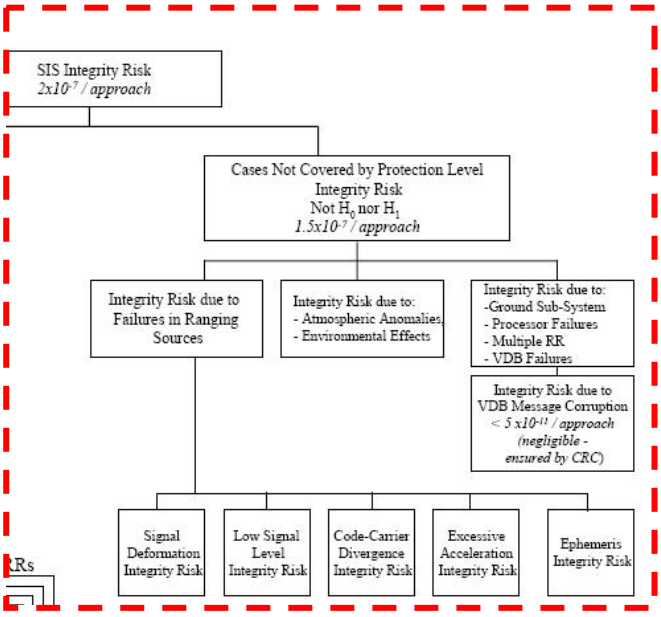


Fig. 02. Integrity Risk Allocation Tree [3]

Zoom in Fig.02:



In accordance to DO-245A [3], 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 implementing the system architecture modifications and improvements. It is not only a technical issue, but it is also a management issue because 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.

The Table 01 [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 01 – RISK ASSESSMENT MATRIX EXAMPLE [5]

	Severity			
Likelihood	Catastrophic (1)	Critical (2)	Marginal (3)	Minor (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 risk of the system. It is the risk analysis process and 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. The result is a qualitative risk represented by a number (1 to 4) and a letter (A to E). This pair is the representation of the risk level (e.g., 1A, 3C, 2B, etc.).

Risk Computations and Exposure Time

The exposure time associated with the operation also has to be taken into the account in the risk computations. In the case of ILS and MLS, the computed risk is simply the risk 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 checks performed manually.

The risk grows (usually exponentially) over time, and the time chosen to initiate the monitor verification action is such that the maximum risk is never greater than the performance requirement. The maximum risk can't 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 where the time between independent samples is greater than the landing time 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 to compute the cumulative risk over the landing period. Fig. 03 illustrates an example of this. In this example, there are 5 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 5 (five).

Another issue concerns how to account for failures that can remain undetected for time 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.

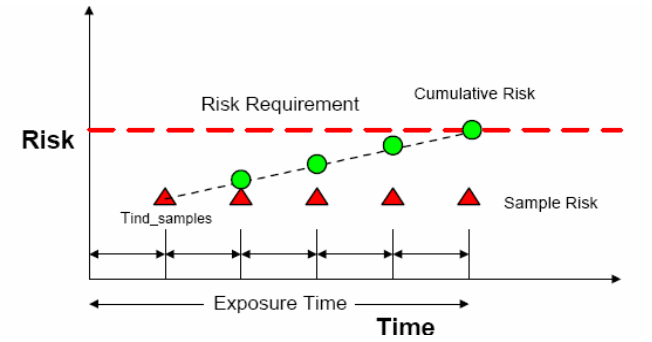


Fig. 03. Integrity Risk and Sample Intervals

Step 3: Define the logic of Risks and determine the minimal Cut Sets of the Integrity Risk Tree. (Qualitative approach)
The system items arrangement in a tree is a powerful graphical tool to visualization of threats (or hazards) of the system and provide an accurate evaluation of items dependencies and interrelationships among them. Over the last fifteen years this technique is used by safety 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.

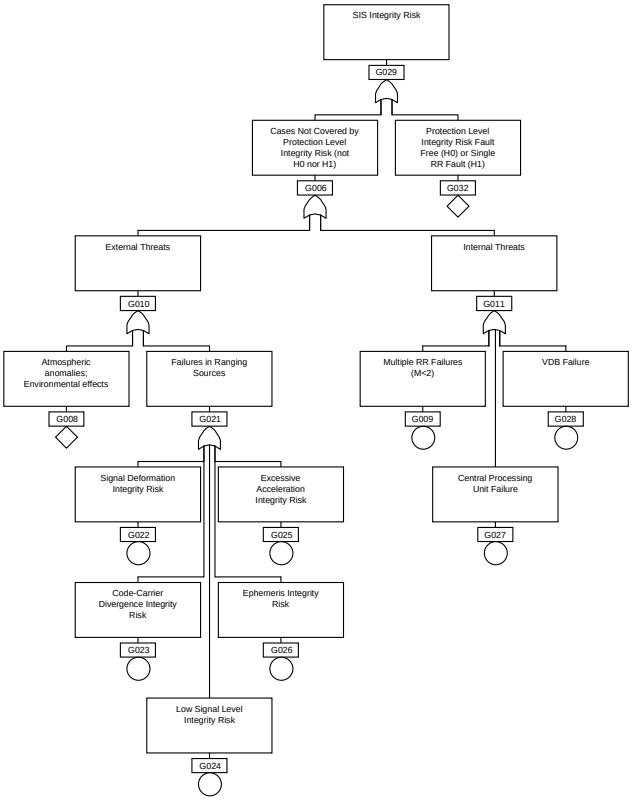


Fig. 04. Qualitative Integrity Risk Tree

The Figure 04 represents the integrity risk tree of the GBAS ground system under analysis. It is a preliminary evaluation of the root-causes of loss of integrity that may happen during the system operation and threats the approach and landing of the aircrafts equipped with a GBAS aircraft system.
The branch named as “Protection Levels Integrity Risk”, represented by gate 032 is the aircraft portion integrity risk, so it is not considered to integrity risk calculation of GBAS ground system. For this it is represented with an “undeveloped branch” or “undeveloped event” in accordance to [1], [2] and [3].

Step 4: Allocate the SIS Integrity Risk budget to the system items of the Integrity Risk Tree and calculate the minimal cut sets (quantitative approach).

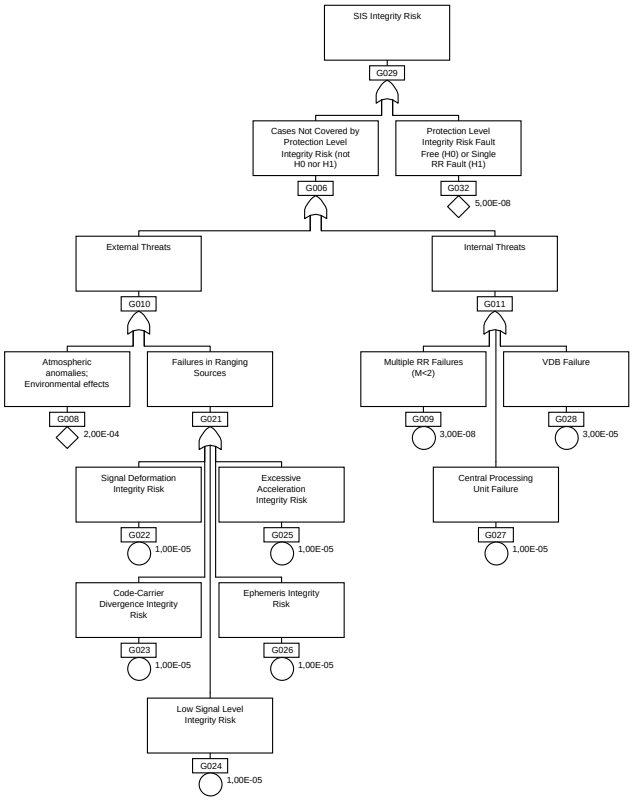


Fig. 05. Integrity Risk Tree with Probabilities of Events

Preliminary Results:

Cut Sets for G029
Top Event Probability = 2,90E-04

TABLE 02 – 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

Analyzing the preliminary results of cut sets probabilities, it is very important to check if the top event probability (Gate 029) is within the limit established in the [1], [2], and [3], which must be lower than 1.50E-07 per 15 seconds or per approach (time approach is 150 seconds approximately). It means that the integrity level (or DAL) of the GBAS ground system must be equivalent to Level B of the DO-178B (Software Design Assurance Level) and DO-254 (Hardware

Design Assurance Level). So, 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 [5] is also known as ALARP (As low as reasonably practicable) [6].

Step 5: 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). 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)

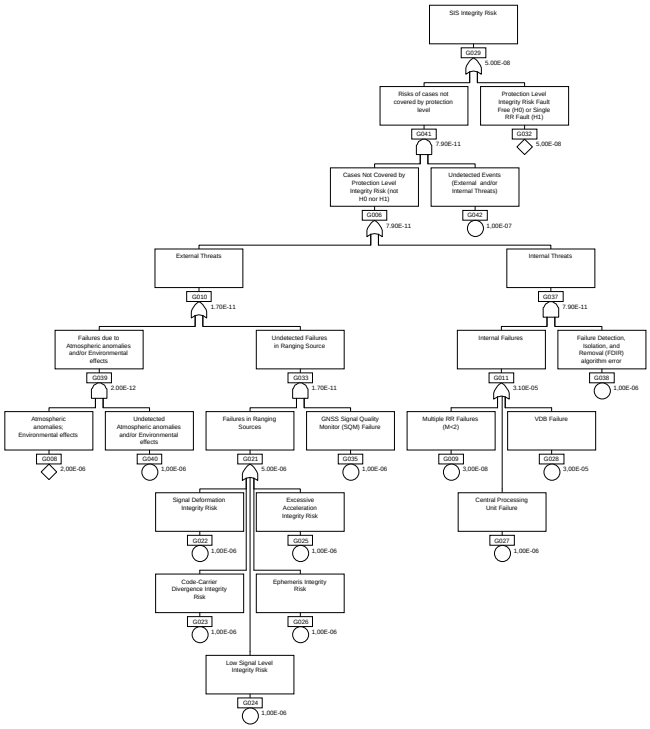


Fig. 06. Final Integrity Risk Tree

Final Result of Probability Calculation of Top Event:

```
Cut Sets for G029
Cut Set #1: 5,00E-08  G032
```

Top Probability = 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 [4] can be fed back and follow-on.

Step 6 (final): designing the integrity risk algorithm to be embedded on IRM subsystem. This process is not treated in this paper because it is software engineering issue and the goal of this paper is not the algorithm design and development, but is the methodology of preparing the inputs for the algorithm design.

II. CONCLUSION

The RTCA [3] and ICAO [2] integrity risk requirement is met by using the Risk Tree Analysis (RTA) [2] technique to identify, evaluate, display and calculate the risks associated to the system architecture, environments and operations. 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. That method shown here is a way to lead the safety efforts to certification activities of the system and contribute to safety specialists and risk managers by providing a new alternative for treating and solving the engineering problems which threat the feasibility (or success) of the GBAS programs around the World.

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

Finally, the methodology presented here has shown the importance of integrity risk monitor (IRM) to automatically managing the risks of the system, and belongs to a fundamental part of the GBAS ground station and helps the safety engineers to assure the safe design and the operational safety of the GBAS total system.

REFERENCES

[1] EUROCAE / ED-114, MOPS to GBAS Category I.

[2] ICAO. 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, Nov 2007 and amendment 83, Aug 2008.

[3] RTCA / DO-245A, Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS), 2004.

[4] SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. 1996.

[5] DOD, MIL-STD-882D, Standard Practice for System Safety. 2000.

[6] ICAO, Doc 9859, Safety Management Manual (SMM), 2nd edition. 2009.