

High Integrity GPS-SBAS Receiver Using Innovative Correlator and Software Approach for Avionics Applications

J.K. Ray, R.A. Nayak, Muralikrishna S., Kiran S., Shashidhara K.R., M.R. Shenoy
Accord Software and Systems Private Limited
Bangalore, India

ABSTRACT

A GPS-SBAS Receiver is developed around a Digital Signal Processor with optimize usage of hardware and software in the system. The receiver is designed and engineered for use in avionics application after FAA TSO certification.

Important aspects of the receiver are reliable hardware and safety features. The failure analysis of the receiver hardware for various navigation functionalities shows acceptable performance. The power-on self test and continuous online tests to detect hardware failure enhance the safety and reliability of the equipment. Additional hardware to detect failure improves the test coverage of the equipment.

Comprehensive Receiver Autonomous Integrity Monitoring (RAIM) ensures reliable performance and safety of the system while in use in an aircraft anywhere in the world during the en-route, terminal and non-precision approach phases of the flight.

INTRODUCTION

A GPS-SBAS avionics receiver is different from conventional survey or automotive grade receivers in many ways. The major focus of the avionics receiver is safety and reliability, in addition to the availability and accuracy. The safety and reliability requirements of the receiver are allocated to software and hardware. The software safety assurance is assured by developing the system adhering to the guidelines of DO-178B for Level A, B or C criticality depending upon the intended phases of application of the avionics receiver. The hardware safety assurance is assured by developing the system adhering to a host of guidelines including DO-254. In addition, the system failure probability is to be analyzed for satisfactory level of reliable performance. Further, the performance aspects of the avionics receiver is guided by the requirements specified in DO-229C in terms of receiver integrity, accuracy, availability, sensitivity and many other parameters.

Accord has developed a GPS-SBAS receiver, which is FAA TSO certifiable for en-route, terminal and non-precision approach. The receiver software and hardware is designed in such a way that it works in two different configuration, namely TSO-C145a and TSO-C129a. Accordingly, in the above two configurations the receiver meets the performance requirements of DO-229C and DO-208 respectively for the applicable phases of operation.

The receiver accuracy, acquisition and tracking sensitivity, dynamics, time-to-first-fix and other characteristics meet the required performance specifications outlined in DO-229C as well as DO-208 for en-route, terminal and non-precision approach of operation. The receiver software is engineered as per DO-178B, Level B. It has been subjected to environmental stress as per applicable sections of DO-160D as a host card in an avionics subsystem. The receiver is certifiable for TSO-C145a, Beta Class 1 as well as TSO-C129a Class B1, B2, C1 and C2 for en-route, terminal and non-precision phases of operation.

The receiver is to be used in conjunction with an antenna that is TSO certified and meets the requirements of DO-228. The receiver performance requirements are met when the RF link budget outlined in ARINC 743 is satisfied.

This paper gives a brief overview of the receiver highlighting its safety, reliability and integrity aspects. It discusses in detail how the safety and reliability are built into the system. In addition, this also briefly dwells on the noble software correlator architecture that is optimized for this application.

RECEIVER OVERVIEW

The GPS-SBAS receiver employs 12 GPS channels and 3 SBAS channels for parallel tracking of up to 15 satellite signals. The receiver has a simple two-block architecture and uses proprietary software correlator technology described in the next section. It employs an RF front-end that downconverts the GPS-SBAS L1 signal to a manageable IF frequency signal and sends it directly to the DSP through a serial port. The DSP processes the sampled IF frequency signal, runs the code tracking loops and carrier tracking loops to acquire and track the GPS-SBAS signal. Further, it performs the navigation data extraction, management and finally the user position, velocity and time computation. In addition it performs receiver autonomous integrity monitoring to detect outliers and satellite failure by using SBAS satellite messages or through Failure Detection (FD) and Exclusion (FDE) algorithm. Figure 1 shows a simple diagram of the receiver identifying some of the important input/output signals.

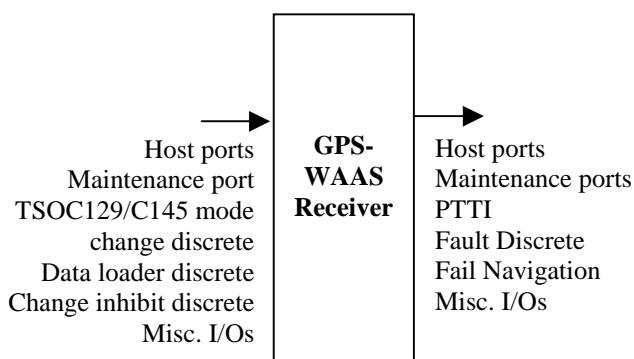


Figure 1: Receiver Input/output Diagram

The receiver performs exhaustive Receiver Autonomous Integrity Monitoring (RAIM), Predictive RAIM, Built In Test (BIT) and Fault monitoring as safety measures. These features are briefly described in the next sections.

The receiver employs a gas discharge tube for lightning protection for the electrical lines, such as antenna link that are to be exposed outside the host enclosure.

The receiver is connected to the external world through a host port and a maintenance port. The data protocol used in the host port is as per ARINC 743. The maintenance port is to be used for software upgrade, magnetic table download, servicing and maintenance. To prevent inadvertent writing in the boot memory during erroneous software upgrade, a comprehensive handshaking protocol involving hardware and software signaling is employed.

CORRELATOR

The receiver employs a proprietary software correlator engine (patent pending). In this technique, the receiver core is realized around a single programmable Digital Signal Processor (DSP) microcomputer. The receiver is based upon a unique architecture, which allows complete GPS-SBAS signal processing as well as navigation processing functions to be implemented on a single programmable DSP. Thereby it obviates the need for a separate hardware correlator, signal processor and navigation processor.

This type of architecture lends itself very well to flexible upgradation as well as programmability for variety of applications. The programmatic interface to the GPS core engine facilitates the developer to embed his/her own applications on the receiver core along with GPS function.

Figure 2 shows the two-block receiver architecture using a software correlator.

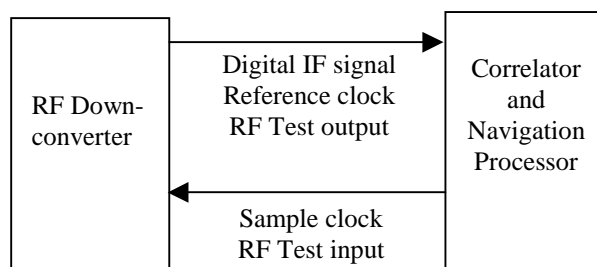


Figure 2: Receiver Architecture using Software Correlator

Some of the noble features of this correlator are:

- a) flexible software architecture with programmatic interface
- b) scalable architecture to translate the advances in the DSP core technology into performance benefits
- c) software architecture well suited to adapt to the advances in the GNSS programs
- d) optimized power consumption
- e) dynamic mobilization of computing resources to sustain receiver performance under adverse signal conditions
- f) sampling clock is directly connected from DSP to RF down converter, making it possible to change the sampling frequency in the software to interface with a variety of RF down converter.

BUILT IN TEST

The receiver performs Power-on Built-In-Test (PBIT) as well as Continues Built-In-Test (CBIT) to enhance the safety and reliability of the system. All major hardware

components are covered under the PBIT and CBIT, such that faulty components during power on and also during continues mode of operation are identified and notified to the host computer immediately for timely intervention.

Power-on BIT

Power on built in test is conducted as soon as the power is switched on. The receiver conducts an exhaustive test and checks the functionality of all the major components or functional blocks. The outcome of the self-test decides whether the receiver transits to initialization mode or fault mode as shown in Figure 3.

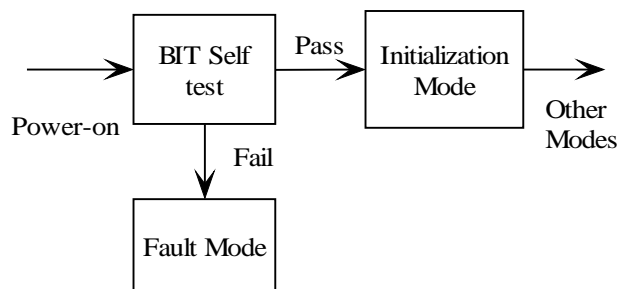


Figure 3 - BIT Mode transition diagram

Continues BIT

Following the Initialization mode, the receiver performs self-test in the background during all modes of operation of the receiver. These are called On-line BIT or Continues BIT (CBIT). These tests shall be performed in a staggered manner so that the computational resources can be utilized for the intended functions in each mode.

Table 1 gives a list of built in tests conducted on the major hardware or functional blocks:

Sl.	Component	Tests
1	Processor ALU, MAC and Shifter	Predefined logical, arithmetic and shift operations and assembly language code execution
2	Processor cache	Run predefined piece of test code using the processor cache which is already profiled
3	Processor program sequencer	Run predefined piece of test code involving the program sequencer whose outcome is known
4	Processor data registers	Test for a) stuck at fault, b) inversion coupling fault, c) idem potent coupling fault, d) state coupling fault, e) data retention fault
5	Processor timers	Program the timer with a predefined number, and monitor the downcount

6	SDRAM	Test for a) stuck at fault, b) coupling fault, c) data retention fault, d) Address lines/ data lines/ SDRAM control signal lines from the DSP
7	SRAM	Test for a) stuck at fault, b) coupling fault, c) data retention fault
8	Real Time Clock	a) Data retention failure, b) Data Write/Read failure from internal RAM memory, c) Alarm failure
9	EEPROM	Data write error or data retention fault
10	FLASH Memory	a) Data retention fault, b) Address lines/ Data lines/ Control lines from the DSP to the Flash.
11	RF	a) Antenna short circuit, b) Antenna open circuit, c) PLL Lock
12	Input latch	Additional hardware logic gates to write and read back a) Lines shorted to ground or VCC, b) Lines shorted to the adjacent line, c) Unable to latch data from input onto the output lines, d) Data lines/control signal lines from the DSP
13	Output latch	Additional hardware logic gates to write and read back a) Lines shorted to ground or VCC, b) Lines shorted to the adjacent line, c) Unable to latch data from input onto the output lines, d) Data lines/control signal lines from the DSP
14	Serial communication modules	Additional hardware loop back path to write and read back

Table 1: Typical Built In Tests

FMEA AND FTA

The safety and reliability aspects of the receiver are adjudged through Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA).

FMEA is performed at the system level. The effects of each failure mode are determined at the system level for each operating mode of the equipment.

A parts count analysis is normally used early in a design and proposal formulation when detailed information is not

available, or a rough estimate of reliability is all that is required. This method requires less information, generally part quantities, quality level and the application environment.

A part stress analysis takes into account more detailed information regarding the components, and therefore offers a more accurate estimate of failure rate. This is applicable during the later design phase when actual hardware and circuits are being designed.

The MIL-HDBK-217F utilizes the Arrhenius relation for calculating the reliability, which illustrates the relationship between failure rate and temperature for components. The temperature-related failure rate, according to the Arrhenius relation, is:

$$\lambda_P = A e^{-\frac{E_a}{k} \left(\frac{1}{T} - \frac{1}{T_0} \right)}$$

where,

λ_P is the failure rate of the part expressed in failures/ 10^6 hours

T is the ambient temperature in degrees Kelvin.

T_0 is the reference temperature in degrees Kelvin

K is the Boltzmann's constant in eV/K

A is the normalizing rate constant, and

E_a is the activation energy in eV.

The Mean Time Between Failures (MTBF) for the receiver is obtained by inverting the total failure rate of the system multiplied by $1e^{+06}$ hours.

$$MTBF = \left(\frac{1}{\sum \lambda_p} \right) (1e^{+06}) \text{ hours}$$

The piece-part FMEA is done on the system where the failure mode of each individual component contained in the item or function is analyzed. The list is created for all the components and then the failure mode for each component is determined. When there is an ambiguity of the type of the failure mode, then the worst-case failure is assumed.

The failure is classified as a major or a minor severity class. A failure is classified as major, when there is a failure in the system and misleading information is derived from the system. A failure is classified as minor, when there is a failure in the system and failure indication is clearly conveyed out of the.

Functional FMEA is conducted for the software in the following steps:

- a) Identify the major functions
- b) Define the failure modes for each function
- c) Determine the phases of the flight where the function will have impact
- d) Identify the effect of the failure modes of the function
- e) Categorize the criticality of the failure modes of the function
- f) Identify methods to detect the failure

Table 2 shows a sample functional FMEA worksheet for one function. Similar worksheet is to be created for all the major functions of the equipment.

Table 2: Typical Built In Tests

Function Names	Function Code	Failure Mode	Flight Phase	Failure Effect	Criticality	Detection Method	Comments
Provide aircraft position, velocity and precise time	01	Does not provide PVT solution	E, T, NPA	No navigation information to the pilot	Minor	No display of PVT.	
	01	Provides incorrect PVT solution	E, T, NPA	Misleading navigation information to the pilot	Major	Is indicated by Integrity data.	

The Fault Tree Analysis is an important technique in the overall assessment of the safety critical system. A fault tree analysis is a deductive failure analysis, which focuses on one particular undesired event and provides a method for determining causes for the occurrence of this event. The fault tree analysis is a 'top-down' system evaluation procedure in which a quantitative model for a particular undesired event is formed and then evaluated. In this method to begin with all the top level undesired events are identified and is reduced or analyzed to sufficient detail

so as to satisfy the top level undesired event. The faults that will result in predefined undesired event include, component hardware failure, human error and other events.

The fault tree analysis focuses on one particular undesired event and which provides a method for determining the cause of the event. The list of undesired events are compiled first. Each undesired event would become the top-level event in a fault tree. Depending upon the system

indenture level, these top-level events can have different origins. Some major undesired events are:

- Loss or misleading position information
- Loss or misleading integrity information
- Loss or misleading ETA informatoin
- Loss or misleading Pseudorange and Doppler information
- Loss or misleading DOP information
- Loss or misleading PTTI information

In the fault tree analysis, the probability of failure is calculated at each branch level and hence the probability of the top level undesired event is calculated. The probability of the events is calculated using the formula

$$P_s = R = e^{-\lambda t}$$

where

- P_s = Probability of success
- R = Reliability
- e = Natural logarithm base
- λ = Base event failure rate, and
- t = Base event exposure or “ At risk” time.

In reliability terms, we know component survival and component failure are complementary and mutually exclusive. Hence

$$P_s + P_f = R + Q = 1,$$

OR,

$$P_f = Q = 1 - e^{-\lambda t}$$

where

- P_f = Probability of failure.
- Q = Unreliability

The probabilities of two events are added if they are branched using the OR Gate. If they are branched using the AND gate then the probability of two events are multiplied. That is because,

$$P(A + B) = P(A) + P(B)$$

$$P(A.B) = P(A) . P(B)$$

The Fault identifications starts with the basic blocks that can cause the stated failures, and then trace it down to the last dependent unit in the chain, and then sum up the probability of failures. This is performed as per the document SAE ARP4761

Figure 4 gives an example of a fault tree.

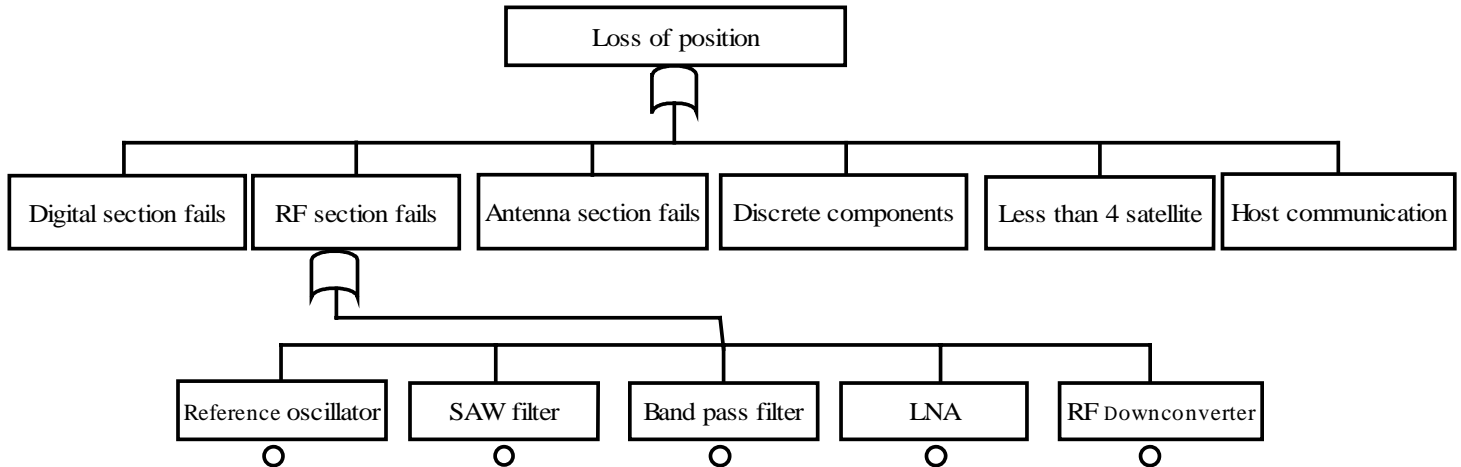


Figure 4: Example of a Fault Tree

Table 3 shows the definitions of the symbols used in the fault tree





Symbol	Name	Definition
	Description Box	Description of an output of a logic symbol or of an event.
	AND- Gate	Event can occur when all the next lower conditions are true.
	OR – Gate	Event can occur if any one or more of the next lower conditions are true.
	Basic Event	Event, which is internal to system under analysis, requires no further development.

Table 3: Fault Tree Symbols

RAIM

One of the most critical aspects of the GPS-SBAS receiver to be used in an aircraft for navigation purposes is to ensure that the receiver meets the integrity requirements in terms of detecting faults and if possible to make corrective actions in addition to generate timely alerts. The Fault Detection (FD) and Exclusion (FDE) algorithm, which is often known as FD/FDE is implemented in the receiver.

Even prior to the FD/FDE the receiver performs step error detection as per DO-229C. It monitors the quality of the signal before using it to generate the measurements data. The GNSSU monitors the quality of the ephemeris data, ionospheric data etc. by collecting two sets of data and comparing them before use.

The GNSSU performs cross-correlation error detection by comparing the ranges calculated using Ephemeris data and Almanac data. It has a watchdog timer to reset the system in case of accidental hang-up of the system.

An FD/FDE algorithm is developed and very detailed and extensive simulations have been carried out to validate the performance in terms of availability of fault detection and exclusion of the faulty satellite using GPS-SBAS Signal Simulator in the off-line as per the guidelines of DO-208, TSO-C129a and DO-229C. Simulations were carried out for the GPS orbit, to determine satellite visibility at over two thousands grid points on the earth surface and for 12 hours at 5 minutes time intervals. Then the FD/FDE algorithm that is developed is validated at each time-space points to determine the availability of fault detection and exclusion of the faulty satellite. The space-time points are arranged in terms of the Horizontal Protection Limit and Horizontal Exclusion Limit in presence and in absence of

SA. Then selected cases (different for DO-208/TSO-C129a and DO-229C) such as the most difficult to detect/exclude satellite is identified and Monte Carlo simulations are carried out at those selected space-time points to validate the False Alarm and Missed Alarm and other RAIM requirements.

The following receiver integrity aspects are addressed in the receiver:

1. Step error detection
2. Cross correlation error detection
3. Double ephemeris collection and usage
4. RAIM availability
5. Fault detection and exclusion with and without WAAS
6. Fault detection and exclusion in presence or absence of SA
7. Fault detection and exclusion with and without Baro altitude
8. Predictive RAIM
9. Figure of merit computation
10. Navigation data integrity monitor functions

Appendix A and B show flow chart for the RAIM logic and FD/FDE logic used in the receiver. The flowcharts are self explanatory

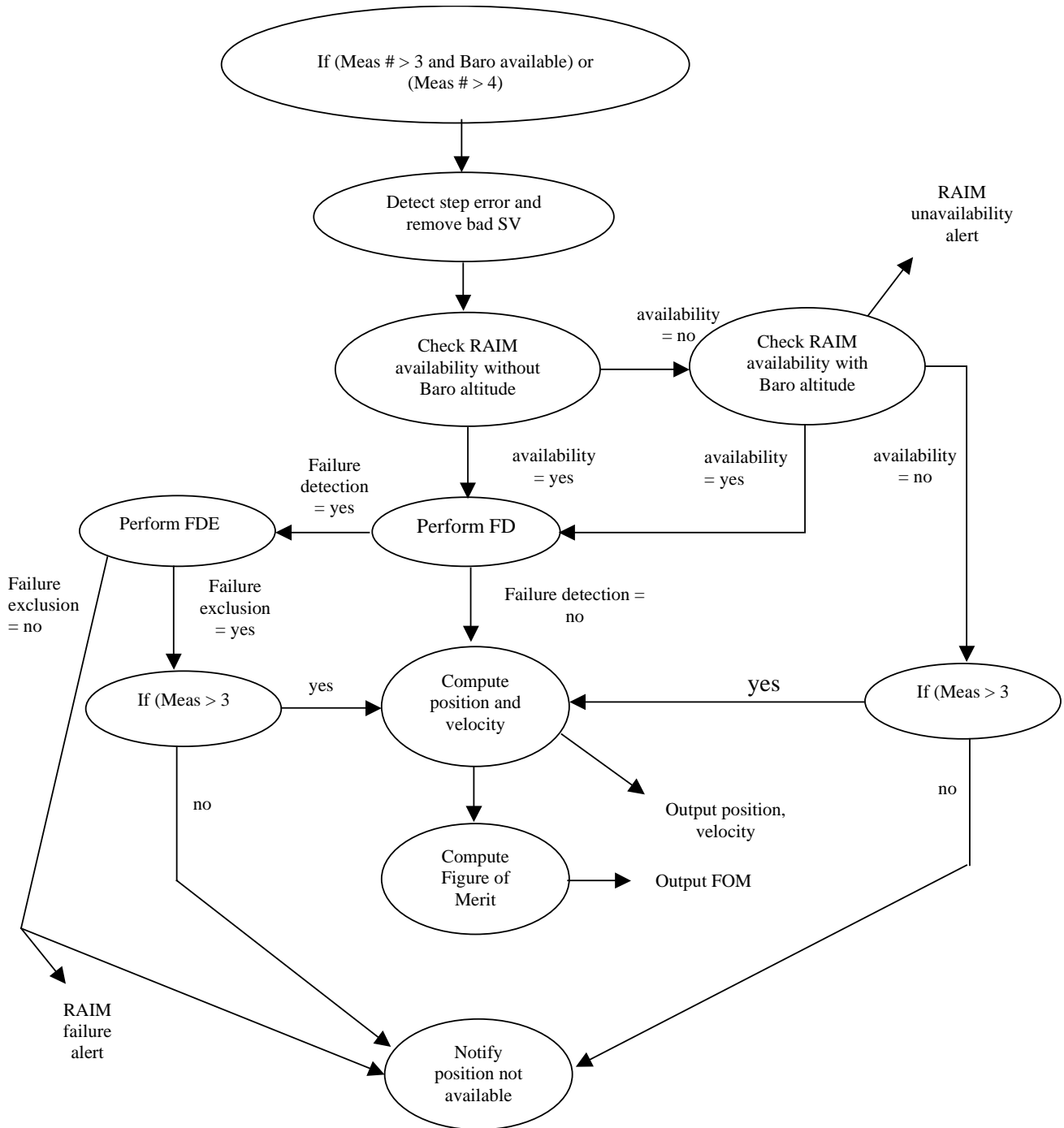
CONCLUSIONS

Accord’s GPS-SBAS receiver built around a DSP has a unique architecture and has all the required safety and reliability checks. It meets all the relevant requirements specified in DO-229C, DO-208, DO-160D, ARINC-743 and was developed as per DO-178B.

REFERENCES

1. RTCA/DO-160D, Environmental Conditions and Test Procedures for Airborne Electronic/Electrical Equipment and Instruments, Change No. 1, July 29,1997
2. RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certifications, December 1, 1992
3. RTCA/DO-208, Minimum Operational Performance Standards (MOPS) for the Global Positioning System, July 12, 1991
4. RTCA/DO-229C, Wide Area Augmentation System (WAAS) for Satellite Navigation, October 6, 1999
5. ARINC 743A-3 Airborne Global Positioning System Receiver, February 4, 1998
6. GPS-SBAS Receiver development documentation

APPENDIX A: RAIM Flowchart



APPENDIX B: Satellite Failure Detection (FD) Flowchart

After step detection

