



# Automatic Dependent Surveillance – Broadcast (ADS-B)

Final Draft

## Design Analysis Report: ADS-B Preliminary Hazard Analysis

Volume I

Findings and Recommended Safety Requirements

September 20, 2001

**Volume I - Design Analysis Report: ADS-B Preliminary Hazard Analysis**

**Final Draft**

**September 20, 2001**

Prepared For: Federal Aviation Administration  
1250 Maryland Avenue, SW  
Washington, DC 20024

Prepared By: Michael Allocco     FAA Office of System Safety, (ASY-300)  
Robert Thornburgh     Adsystem, Inc.  
1250 Maryland Avenue, SW  
Washington, DC 20024

Reviewed by: \_\_\_\_\_ Date \_\_\_\_\_  
Scott VanBuren  
Chief System Engineer

Approved by : \_\_\_\_\_ Date \_\_\_\_\_  
Mike Harrison, Chairman



# TABLE OF CONTENTS

## Volume I - Design Analysis Report: ADS-B Preliminary Hazard Analysis

1.0	Summary .....	1
2.0	Purpose.....	3
2.1	Purpose of Analysis .....	3
3.0	Background.....	4
4.0	System Description .....	4
4.1	Definition of Automatic Dependent Surveillance-Broadcast .....	4
4.2	Aircraft Equipment Overview.....	7
4.3	Ground Equipment Overview .....	9
4.4	Software .....	9
4.5	Transition from the Current Surveillance Architecture .....	9
5.0	Approach and Methodology .....	11
5.1	Scenario Model .....	12
5.2	Risk Determination .....	166
5.3	Scenario Descriptions .....	199
5.4	System Safety Order of Precedence.....	2222
6.0	Hazard Identification and Analysis.....	2222
6.1	Scenario Discussions .....	2222
6.1.1	AFXO – Aircraft –Fixed Object .....	2323
6.1.2	AFLO – Aircraft – Flying Object .....	233
6.1.3	AGV – Aircraft – Ground Vehicle.....	233
6.1.4	AOAA – Aircraft –Other Airborne Aircraft .....	233
6.1.5	ANAA - Aircraft – Non-airborne Aircraft.....	244
6.1.6	AADF Aircraft –Aircraft Display Failure.....	244
6.1.7	AGDF Aircraft – Ground Vehicle Display Failure.....	244
6.1.8	SSDF Surface Aircraft –Surface Aircraft Display Failure .....	244
6.1.9	AFOD Aircraft –Fixed Object – Display Failure .....	25
6.1.10	AAAL Aircraft – Aircraft –Approach and Landing .....	25
6.1.11	SR - Security Related.....	255
6.1.12	HF - Human Factors.....	255
6.1.13	SA - System Anomalies .....	265
6.1.14	LTAD – Less Than Adequate Design.....	266
6.1.15	EE – Environmental Effects.....	266
6.1.16	LTAD -NS – Less Than Adequate Design .....	277
6.1.17	SA –NS System Anomaly – NAS Context.....	277
6.1.18	CP – Contingency Planning.....	277
6.1.19	IS-A Basic Interactive Aircraft .....	288
6.1.20	IS-B Separation and Sequencing .....	288
6.1.21	IS-C Flight Path Deconfliction Planning .....	288
6.1.22	IS-D Aircraft Broadcast Only .....	299
6.1.23	IS-E ATS EnRoute and Terminal Area Operations.....	299
6.1.24	IS-F Ground Receive Systems, Parallel Runway and Surface Operation .....	299
6.1.25	IS-G Ground Receive Systems, Flight Following .....	30

6.1.26	IS-H Separation and Sequencing .....	3030
6.1.27	IS-I Flight Path Deconfliction Planning .....	3131
6.1.28	IS-J Flight Path Deconfliction Planning and Terrain Awareness Warning System.....	3131
6.1.29	ILIS Integration Specific NAS/World-Wide Risks - Increased Risks.....	32
6.1.30	IS-K Wide Area Augmentation System/Local Area Augmentation System/ FMS/ L1 Frequency.....	333
6.1.31	IS-L Integration Specific NAS/World-Wide Risks .....	344
6.2	Preliminary Hazard Analysis.....	366
6.2.1	Preliminary Hazard Analysis Tables .....	366
7.0	Preliminary Requirements Recommendations.....	53
7.1	Candidate Safety Requirements.....	5353
8.0	Preliminary Hazard Analysis Findings .....	71
8.1	Risk Assessment Ratings .....	71
9.0	Conclusions and Recommendations .....	7272
10.0	Security .....	744
11.0	References.....	755
12.0	Bibliography .....	75
Appendix A - Acronyms and Definitions .....		76

Volume II - Design Analysis Report: ADS-B Preliminary Hazard Analysis, Scenario Matrix

## 1.0 Summary

This Preliminary Hazard Analysis (PHA) was developed based upon an expansion of, the Initial Hazard Assessment (IHA) of ADS-B completed 21 January, 2000. The IHA was limited in scope in that it only considered the severity of consequences associated with a specifically developed hazard scenario. There was not sufficient information at that time to define the probability (or likelihood) of occurrence. Risk Ratings could not be developed without the development of the requisite associated probability of occurrence. As the ADS-B system has evolved over the last several months, with additional system clarification, this Preliminary Hazard Analysis has been completed which takes into account both factors.

The IHA analysis, contained in Volume 1 ADS-B Safety Engineering Report #1: Initial Hazard Analysis, produced controls and mitigations to eliminate or reduce the risks associated with identified hazards. The controls and mitigations were turned into Candidate Safety Requirements/Recommendations requirements statements for possible inclusion in an initial requirements document (IRD). The requirements covered the end-to-end operation of the system and may therefore impact the manufacturers of the on-board avionics, the operators of the aircraft or vehicle, the services to be supplied by the NAS, the builders of the ground system, and the applications user community. The IHA hazard scenario worksheets are contained in Volume 2 ADS-B Safety Engineering Report #1: Initial Hazard Analysis.

The PHA expanded on the IHA and generated a total of 878 hazard scenarios. A hazard scenario, as contained in scenario sets, shows the sequential events which must occur to culminate in an undesired outcome (harm). The harm (accident) is a combination of system state and contributors to a sequence of events that result in a postulated harm. The contributors are varied in combinations and permutations of system failures and inappropriate human action or response. Each variation in a scenario set may affect either severity or likelihood, or both and may identify a new or different control requirement.

The expanded PHA hazard scenario worksheets are contained in the PHA Volume 2 of the ADS-B Design Analysis report: ADS-B Preliminary Hazard Analysis Volume #1. The PHA was conducted using the FAA System Safety Management Program, dated 1 January, 2001 and the methodology defined in the FAA System Safety Handbook, dated 30 December, 2000. The new hazard scenarios included both an expansion of the initial scenarios, at a system level based on emerging system information, as well as new scenarios based primarily on potential equipage combinations within the National Airspace System (NAS). The equipage combinations are derived from equipment assumed to be operational through the year 2015. The equipage combinations are listed and discussed in more detail in section 4.2 Aircraft Equipment Overview, of this report and listed in section 5.0 Approach and Methodology.

The output of the PHA is used in: (1) further developing system safety requirements to be added to the Safety Requirements Verification Table (SRVT), (2) preparing performance/design specifications, and (3) initiating the hazard tracking and risk resolution process for the ADS-B system. The PHA produced a total of 125 Candidate Safety Requirements (CSRs). Thirty-eight (38) of the CSRs were identified as Existing requirements. The remaining eighty-seven (87) requirements were identified as Recommended Candidate Requirements. Existing requirements are those that can be referenced in current program documentation, i.e., Military Specifications, FAA

Orders and other governmental regulations, and consensus standards. Recommended CSRs are those control methods that are not referenced in current program documentation and are therefore, recommended. The CSRs are written as high-level "shall" statements that are postulated to control or mitigate hazardous outcomes as identified in the analysis.

The PHA findings from the analysis are summarized as follows:

- Recommendations that relate to “see and avoid” procedures, such as lighting and marking of aircraft, flying objects, ground vehicles, and fixed objects.
- Recommendations relating to alternate, independent means of validating the ADS-B provided information, such as call sign, ID, position, velocity, and altitude. These are generally requirements on the NAS to continue to provide current surveillance and communications systems until sufficient confidence is established in the reliability and availability of ADS-B. This approach is consistent with current ADS-B plans for a transition period in which ADS-B will be operated in parallel with existing systems.
- Design requirements for the ADS-B system to ensure reliable operation, high availability, and self-test features to detect malfunctions or loss of integrity.
- Requirements that cite existing FAA, DOD, or industry specifications or standards
- Recommendations for studies to determine human factors design requirements using pilots and controllers to determine the safest implementation of the system. Laboratory simulations, flight tests, and operational evaluations are included.
- Requirements for compatibility and integration of information from a wide range of input sources/types expected to be in use through the year 2015.
- Requirements for training associated with safety related to ADS-B design, maintenance, or operation.
- Requirements to prevent interface malfunctions between existing and legacy systems and ADS-B resulting in loss of ADS-B capabilities.
- Requirements to prevent system/subsystem malfunctions from propagating to other systems/subsystems or communications/avionics equipment.
- Requirements to prevent communication delays or losses as a result of LTA mixed equipage procedural integration.
- Requirements designed to prevent less than adequate integration of ADS-B with Airborne Conflict Management (ACM).
- Requirements to ensure integrated ADS-B System time source is synchronized for accurate position, velocity and time.
- Requirements for integration of national and international separation standards associated with ADS-B use.

While the 878 total hazard scenarios were identified and analysed in the ADS-B PHA, forty-one (41) were ranked as High Hazards. Of these 41 high hazards 40 were ranked as 1C (Catastrophic Severity and Extremely Improbable) and one (1) ranked as 2B (Hazardous Severity with a Remote Probability). The 41 high hazard scenarios consisted of the following:

24 - Human factors:

Excessive workload, language barriers/conflicts, input errors, conflicts between pilots & controllers,

9 - Mixed Equipage:

Confusion, conflicts, errors, system inaccuracies

7 - Security:

Jamming, spoofing, intentional intrusion

1 - Unidentified intruder

The high hazards were ranked relative to all of the hazards identified. All identified high and medium hazards will be placed into a Hazard Tracking System (HTS). The HTS will allow each hazard to be tracked throughout system lifecycle activities. As the system matures through design and build activities additional controls may be identified which may impact a hazards ranking.

The overriding conclusion of the Preliminary Hazard Analysis is the ADS-B system will have a tremendous impact on the structure of the NAS architecture from introduction through full planned applicability. It must interface with existing and legacy systems with reliability, which is both acceptable and measurable. The findings of the PHA demonstrate the prudence of a phased introduction into the NAS utilizing a closed-loop approach with continuous monitoring/testing feedback. System operability, reliability confidence must be obtained prior to planned expansion.

Although this analysis was performed based on the current state of knowledge of the requirements, an ADS-B design does not yet exist: therefore, all hazards may not have been identified. In order to assure a successful ADS-B System Safety Program, follow-on safety reviews must be conducted. Review and update of the hazard analysis, scenario by scenario, is required.

Future changes to the ADS-B baseline system or program must be evaluated from a system safety perspective. This PHA is based upon current system safety engineering practices as specified in the referenced applicable specifications and requirements documents. Subjective judgements and logic has been applied to the development of applicable scenarios, the identification of appropriate mitigation, and to ensure conservative estimations of risk.

## **2.0 Purpose**

### **2.1 Purpose of Analysis**

The Preliminary Hazard Analysis was conducted to identify safety related risks and develop controls to either eliminates or controls those risks to an acceptable level. The system-level PHA was conducted to evaluate the safety-related risks of ADS-B integrated within the NAS out to the year 2015.

This PHA was conducted as one of the safety analyses included in the ADS-B System Safety Assessments in support of the Safeflight 21 Product Team. The purpose of the PHA was to identify hazards and to assess the risk of these hazards applicable to the 27 applications addressed in the safe flight 21 Master Plan. The ADS-B System Safety Assessments were mandated by the U. S. Congress for completion in Fiscal Year 2001 to support decisions relative to initial certification of ADS-B for applications within the NAS. The logic associated with the PHA scenarios have also been defined along with associated potential effects and recommended precautions, controls, and procedures. Those precautions, controls and mitigations have been converted to high-level candidate safety requirements.

### **3.0 Background**

ADS-B is currently being considered for applications in the National Airspace System. One of the principal drivers from the user standpoint is to enable Free Flight, however, the Cargo Airline Association (CAA) is vitally interested in ADS-B to improve the safety and efficiency of their operations. In 1995, Radio Technical Commission for Aeronautics (RTCA) Task Force III was formed to develop a consensus regarding free flight implementation. They considered ADS-B as a key technology for free flight by enabling the common situational awareness necessary for air and ground shared responsibility.

RTCA SC-186 has developed Minimum Aviation System Performance Standards (MASPS) for ADS-B, DO-242<sup>(2)</sup>. The MASPS were published in January 1998. They serve as the basis for this Preliminary Hazard Analysis. DO-242 identifies both near term and far term applications of ADS-B. These applications cover air-to-air, air-to-ground, and airport surface operations. The near term applications of primary interest are: Aid to Visual Acquisition, Conflict Avoidance, Separation Assurance and Sequencing, Flight Path Deconfliction Planning, Simultaneous Approaches (to parallel runways), and Airport Surface. In addition, Table D-1 of RTCA/DO-242 lists 23 additional potential near term applications, and Table D-2 lists another 14. In addition to the MASPS, RTCA has also developed Minimum Operational Performance Standards (MOPS) for ADS-B.

Safeflight 21 is a joint FAA/CAA program to conduct research and development activities including Operational Evaluations of the 9 enhancements<sup>(3)</sup> identified by RTCA as having potential for improving safety, capacity and efficiency of air traffic operations. Seven of the 9 enhancements involve the use of ADS-B. Safeflight 21 conducted an operation evaluation, referred to as OpEval1, in the Ohio River Valley during July 1999, using several aircraft equipped with ADS-B and Cockpit Display of Traffic Information (CDTI). OpEval 2 was conducted at Louisville, KY, in FY 2000, and OpEval 3 is planned for Memphis in the Spring of 2002.

In addition to the US activities, the European aviation community is evaluating ADS-B for air traffic control applications. For areas not equipped with radar, as is the case many places in Europe, ADS-B might be a cost-effective solution to their need for increased capacity and efficiency.

### **4.0 System Description**

The descriptive material in this section has been excerpted and adapted from Reference 2.

#### **4.1 Definition of Automatic Dependent Surveillance-Broadcast**

ADS-B is a function on an aircraft or a surface vehicle operating within the surface movement area that periodically broadcasts its state vector (horizontal and vertical position, horizontal and vertical velocity) and other information. ADS-B is automatic because no external stimulus is required to elicit a transmission; it is dependent because it relies on on-board navigation sources and on-board broadcast transmission systems to provide surveillance information to other users. The aircraft or vehicle originating the broadcast may or may not have knowledge of which users are receiving its broadcast; any user, either aircraft or ground-based, within range of this broadcast, may choose to receive and process ADS-B surveillance information.

For the purpose of this PHA, the terms aircraft or airborne vehicle refers to a machine or device capable of atmospheric flight. The term ground vehicle refers to vehicles that operate on the airport surface movement area (i.e., runways and taxiways). In addition to aircraft and ground vehicles, ADS-B service may be extended to identify fixed objects (e.g., an uncharted tower not identified by a current NOTAM.)

ADS-B consists of the following components: message generation and transmission by the source aircraft/ground vehicle, propagation medium, and message reception/report assembly processing by the user (Figure 4-1). As described later, some ADS-B participants may be able to transmit but not receive. In addition, some ground-based users may be able to receive but not transmit.

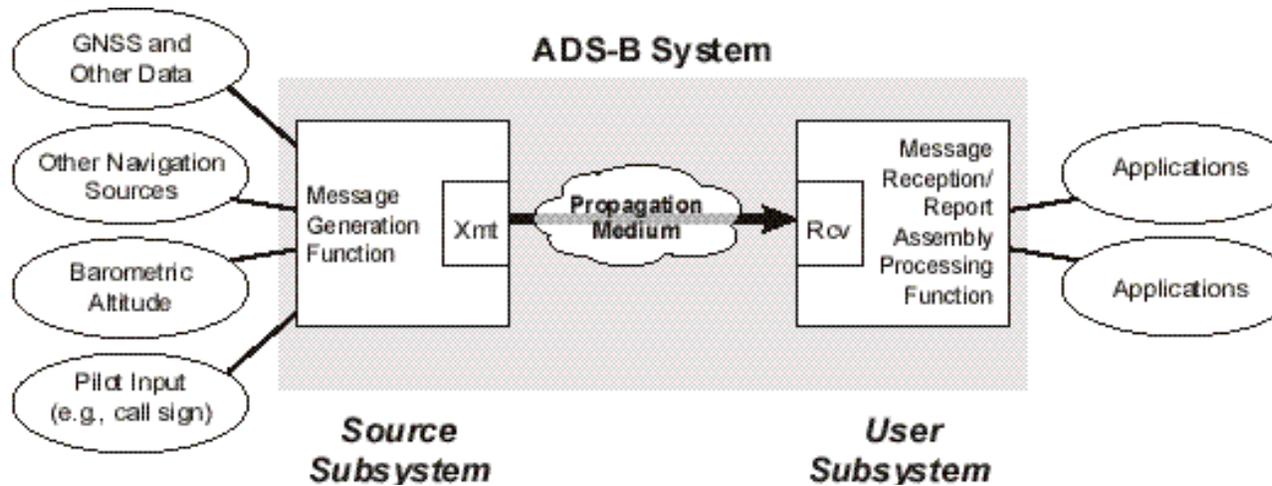


Figure 4-1. Functional Relationship between ADS-Band Surveillance Applications

The PHA is conducted at a system level. All human, hardware, software, and environmental interfaces within the NAS associated with ADS-B integration were evaluated.

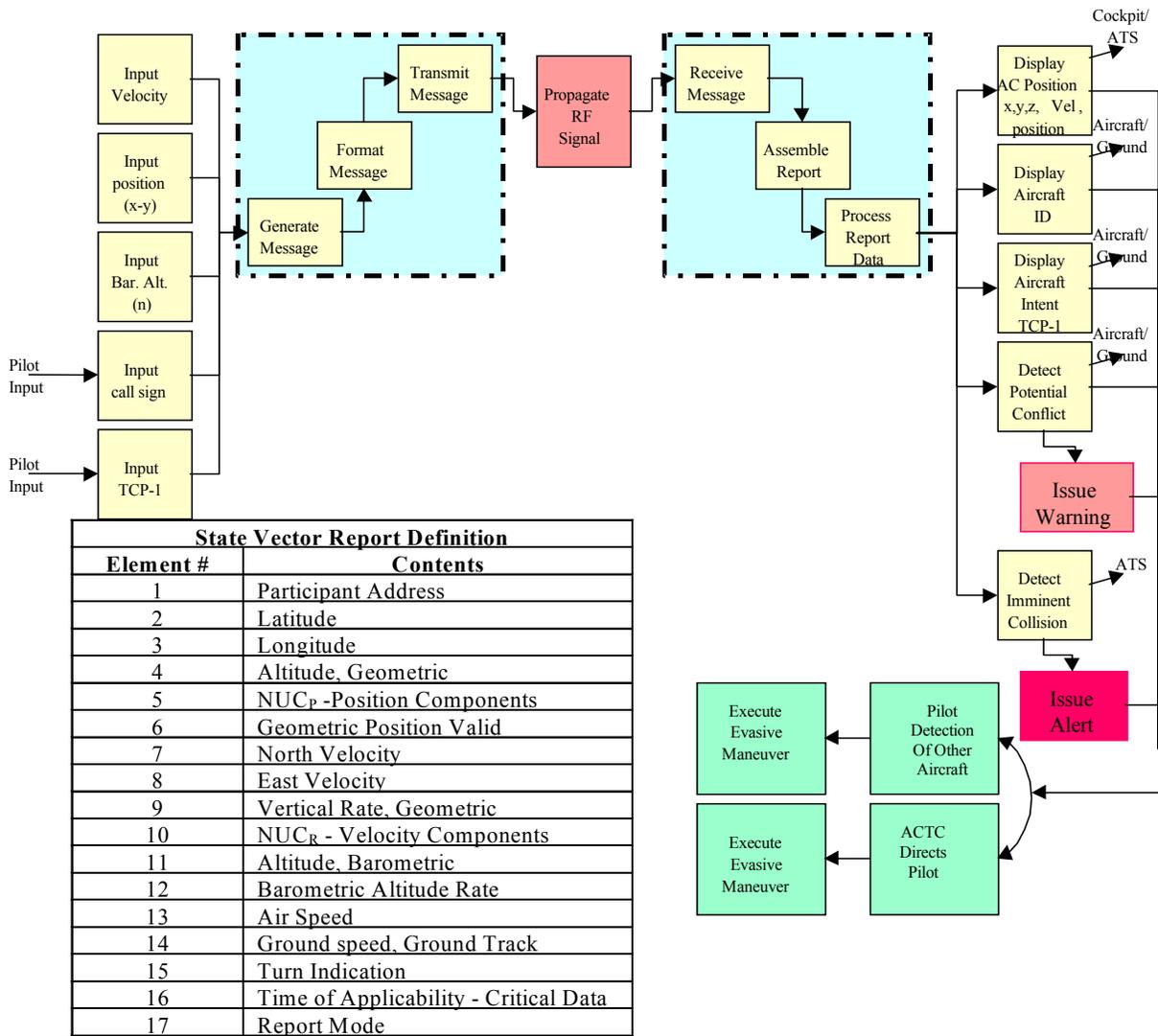


Figure 4-2 ADS-B Functional Flow Diagram Depicting Additional Capabilities of Conflict Detection and Conflict Resolution

It is assumed that the radio frequencies used for the ADS-B transmissions will operate in internationally allocated aeronautical radionavigation service band(s).

Outcomes of the ADS-B system include conflict detection and conflict resolution. Figure 4-2 shows the ADS-B Functional Flow Diagram that depicts the additional capabilities of conflict detection and conflict resolution.

## 4.2 Aircraft Equipment Overview

The aircraft equipment for ADS-B includes a message generation function, transmission function, a receiver with message receipt and report assembly processing function (these may be optional in some implementations), and a number of interfaces (see Figure 4-1). Based on the intended use for an aircraft, airborne vehicle, or ground vehicle, the ADS-B subsystem may be interactive, broadcast only or receive only. Depending on the implementation of the ADS-B avionics, some of the information may be constant (e.g., aircraft/vehicle category). For fixed objects, a message may be generated with no variable information.

Aircraft equipment may include:

- Backup sources of navigation data and interfaces (e.g., redundant GNSS, LORAN, FMS, or INS)
- Augmented GNSS processing (to increase the state vector accuracy and/or integrity)
- Barometric pressure altitude and interface as required
- Interface to applications that process ADS-B reports from other aircraft
- Pilot interface (e.g., to allow pilot entry of fields such as the flight identification or emergency status)
- Application equipment, such as processors and displays

The ADS-B system will be introduced into the NAS where it must interface with existing and legacy systems. Existing and legacy systems and equipage definitions include the following:

- 1) CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.
- 2) MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.
- 3) TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.
- 4) TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.
- 5) TIS are a Mode S Data Link service that delivers automatic traffic advisories to pilots.
- 6) FIS is currently a commercially available very high frequency (VHF) data link that provides weather and aeronautical information needed by pilots.
- 7) TAWS uses position data from a navigational system, like GPS, and a digital terrain database to display surrounding terrain.

8) WAAS enhances GPS signals to provide more precise location information to an accuracy of approximately 25 feet. WAAS is designed to use reference stations covering wide areas throughout the U.S. to cross check GPS signals and then relay integrity and correction information to aircraft via geostationary communication satellites. WAAS enhances availability by using these satellites to provide GPS-like navigation signal.

9) LAAS provides precise correction data to airborne and surface receivers that will result in navigation accuracy of less than 40 inches to distances of 20 miles or more from the airport.

Below is a table of ADS-B Aircraft System Classes (from RTCA/DO-242, Table 3-1) as used in the NAS and included in the assumptions developed for the hazard scenario system states within this PHA.

Class	Subsystem	Capabilities	Features	Comments
<b>Interactive Aircraft/Vehicle Participant Systems (Class A)</b>				
A <sub>0</sub>	Minimum Interactive Aircraft/Vehicle	Aid to Visual Acquisition.	Lower transmit power and less sensitive than Class A <sub>1</sub> .	Minimum interactive capability with CDTI.
A <sub>1</sub>	Basic Interactive Aircraft	A <sub>0</sub> Plus Conflict Avoidance.	Standard Tx and Rx.	Provides ADS-B based conflict avoidance and interface to current TCAS surveillance algorithms/displays.
A <sub>2</sub>	Enhanced Interactive Aircraft	A <sub>1</sub> Plus Separation Assurance and Sequencing.	Standard transmit power and more sensitive receiver. Interface with avionics source required for TCP data.	Baseline for separation management employing intent information.
A <sub>3</sub>	Extended Interactive Aircraft	A <sub>2</sub> Plus Flight Path Deconfliction Planning.	More sensitive receiver. Interface with avionics source required for TCP and TCP+1 data.	Extends planning horizon for strategic separation employing intent information.
<b>Broadcast-Only Participant Systems (Class B)</b>				
B <sub>1</sub>	Aircraft Broadcast Only	Supports visual acquisition and conflict avoidance for other participants.	Transmit power may be matched to coverage needs. Nav data input required.	Enables aircraft to be seen by Class A and Class C users.
B <sub>2</sub>	Ground Vehicle Broadcast Only	Supports visual acquisition and conflict avoidance on airport surface.	Transmit power matched to surface coverage needs. Nav data input required.	Enables vehicle to be seen by Class A and Class C users.

B <sub>3</sub>	Fixed Obstruction	Supports visual acquisition and conflict avoidance.	Fixed coordinates. No Nav data input required. Collection with obstruction not required with appropriate broadcast coverage.	Enables Nav hazard to be detected by Class C users.
<b>Ground Receive Systems (Class C)</b>				
C <sub>1</sub>	ATS EnRoute and Terminal Area Operations	Supports ATS cooperative surveillance.	Requires ATS certification and interface to ATS sensor fusion system.	EnRoute coverage out to 200 nmi. Terminal coverage out to 60 nmi.
C <sub>2</sub>	ATS Parallel Runway and Surface Operations	Supports ATS cooperative surveillance.	Requires ATS certification and interface to ATS sensor fusion system.	Approach coverage out to 10 nmi. Surface coverage out to 5 nmi.
C <sub>3</sub>	Flight Following Surveillance	Supports private user operations planning and flight following.	Does not require ATS interface. Certification requirements determined by user application.	Coverage determined by application.

Figure 4-3 ADS-B Aircraft System Classes

### 4.3 Ground Equipment Overview

Ground equipment will vary depending on the ground application. At a minimum, there will be equipment to receive ADS-B messages. Based on these messages, ADS-B reports will be provided to ground applications, and may be combined with other information (such as radar data).

### 4.4 Software

Although software has not been specifically identified, some of the functionality in ADS-B is software controlled. Some of the input data items will be either software or firmware generated.

### 4.5 Transition from the Current Surveillance Architecture

The introduction of ADS-B equipment into aircraft and ground stations will be into an existing system of surveillance, navigation, and communications. There will be a period of transition rather than an abrupt change. The transition period will serve several useful purposes. It will allow air and ground participant's time to make the equipment changes, which is in keeping with the traditions for such changes. Also it will allow experience to be gathered with ADS-B and the associated GNSS and other sources of navigation information. After a period of transition, which could extend over several years, it is possible that some of the existing systems may be discontinued.

For ATS providers, ADS-B is seen as supplementing and potentially replacing the current radar-based surveillance architecture. As ADS-B is increasingly used, there will be mixed coverage of ADS-B and radar surveillance. Airspace not currently having radar coverage (e.g., low altitude airspace or airport surface) may be the first locations to have ADS-B coverage. During the ADS-B transition period, as changes in ground based systems are introduced to make use of ADS-B information, a number of different changes will be required, involving antennas, receivers, and automation systems including displays. These changes may take several forms and may encompass

several intermediate conditions. For example, during one period a ground system may receive ADS-B information and also conduct SSR surveillance on a given aircraft, using a fusion function to merge the two forms of surveillance into a single track for that one aircraft. During a subsequent period, the ground system may receive ADS-B information from an aircraft and not conduct SSR surveillance on that aircraft, while using SSR for surveillance of other aircraft not equipped with ADS-B. For airborne collision avoidance systems, a similar evolution may be expected. To avoid unnecessary constraints during these changes, and to facilitate the acceptance of ADS-B, the ADS-B information may need to be backward compatible with existing capabilities.

Transitioning to coverage based on ADS-B will be done in incremental steps. In addition, ATS providers will need to update automation in order to utilize ADS-B coverage, along with other improvements aimed at increasing the level of service provided to users. Finally, ATS providers will need to deal with mixed equipage of users in these airspaces for the transition period. For airspace users, transition concerns will be based on the level of service available to a given airspace.

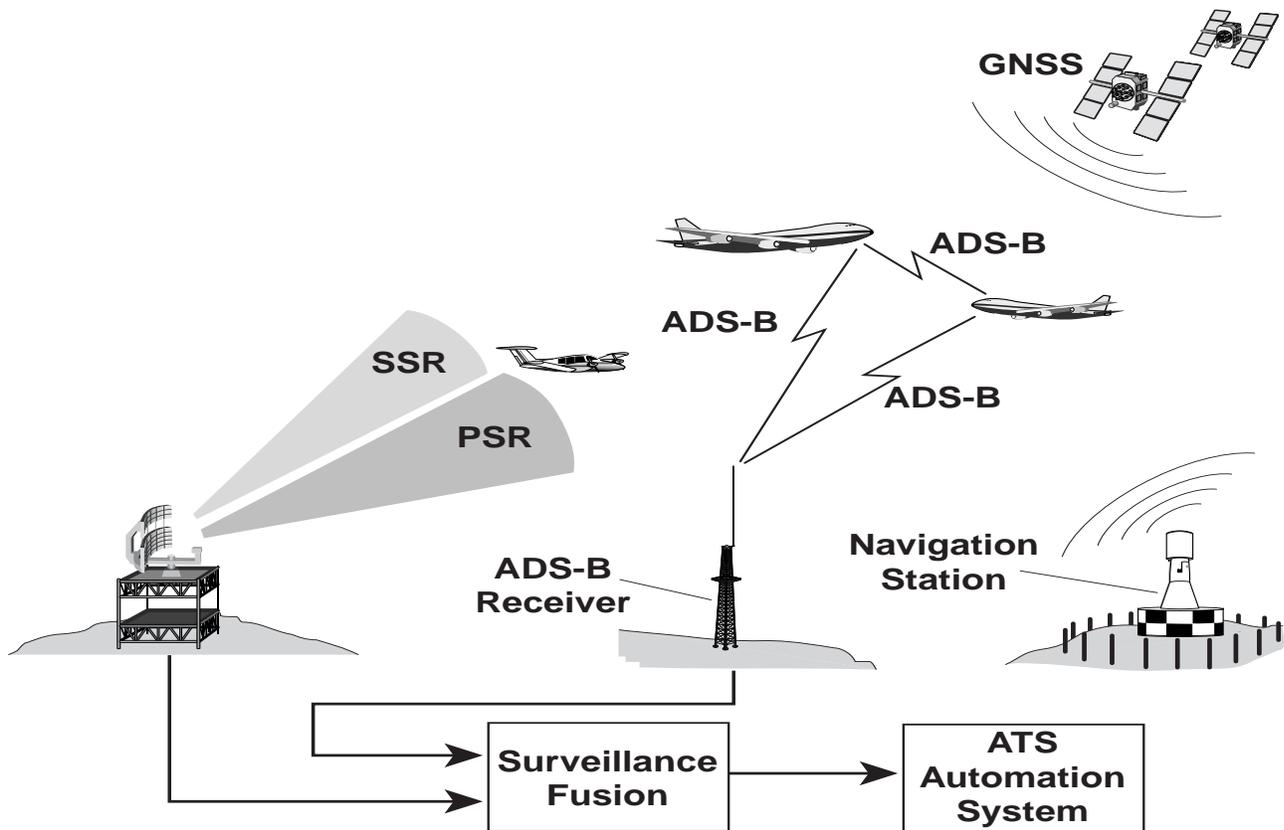


Figure 4-2. ATS Ground Surveillance Transition Configuration

These levels of service will depend not only on the individual user's equipage, but may also depend on ground infrastructure improvements and whether other users in the airspace are equipped. A potential ATS ground surveillance configuration is depicted in Figure 4-2.

The transition surveillance architecture may use multi-sensor data fusion at the ATS centers to transform multiple radar and aircraft ADS-B reports into aircraft track files and aircraft path intent files. Controller needs for greater track accuracy and improved maneuver response may first translate into multi-sensor radar data fusion to achieve improved surveillance compared with today's

legacy tracking systems. The data fusion codes will then be enhanced to blend ADS-B reports with radar and other remote sources to provide greatly enhanced surveillance capabilities for advanced applications such as surface surveillance and arrival fix metering. The need for more efficient and more weather-independent terminal operations will drive the transition to ADS-B equipage at busy hub airports. However, radar systems may remain to provide services for non-equipped users, and to provide backup capability in the event of ADS-B system failures.

## 5.0 Approach and Methodology

The PHA is based on the guidance provided in the System Safety Management Program and FAA System Safety Handbook. Given knowledge of the ADS-B concept of operations, potential accidents were hypothesized. The team identified the potential system accidents/incidents should failures, malfunctions, or human errors occur. The analysis was conducted using a tabular format as shown in Figure 5-1.

Seq # (1)	Scen # (2)	Scenario Description (3)	Contributors (4)	Subsequent Contributors (5)	Phase of Flight (6)	Possible Effect (7)	Risk (8)	Recommendations for Precautions, Controls & Mitigations (9)
856	ISL.04	LTA cross-checking of barometric altimetry with GPS fails to identify deviation in altitude, which results in increased collision risk.	LTA cross-checking of barometric altimetry due to: LTA design LTA procedure  Human error.  GPS fails to identify deviation in altitude due to:  SW malfunction HW malfunction System malfunction Electromagnetic environmental effects Inadvertent damage LTA design. Aircraft on collision course.	Pilot/flight crew loss of situational awareness.  Aircraft not identified via radar or other sources.  ATCT does not communicate warning in time.  See and avoid unsuccessful.	Takeoff, Approach Landing, Flight, Surface, Emergency	Collision	IIC	41 Design system to detect and indicate erroneous barometric altitude rate errors before transmitting through ADS-B. 42 Provide independent means of validating Barometric altitude rate changes. 3N ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude. 6N Require all flying objects that can become hazards to navigation be equipped with ADS-B transmitters, or other appropriate means of identification. 15N Assure that controller/pilot training and procedures are in place for ADS-B, to minimize human error and increase situational awareness. 16N Define criteria for determining threshold values for ADS-B coverage area to assure controller/pilot adequate situational awareness. 22N Design system to minimize the potential for failure of Conflict Avoidance function. 23N Design system to minimize the potential of loss of targets.

Figure 5-1 – Tabular Format for the PHA

The first column is the sequence identifying number. The second column is the Scenario-specific number. A description of the Scenario is in the 3<sup>rd</sup> column. The initial Contributors are in Column 4 and subsequent contributors in Column 5. The phase of flight is located in column 6 with the possible effect in column 7. The Risk Acceptance Code/Risk Rating is in Column 8. Controls are identified in Column 9. In addition, all scenario sequences are assumed to occur under adverse conditions (the system state) that are described in the assumptions section below.

The MS Word table is constructed to allow sorting on any of the columns. In fact, the Table in Volume II is sorted by the Risk Acceptance Code in order of decreasing risk.

The analysis team attempted to be as inclusive as possible in the identification of a potential system accident based on a system scenario. Factors considered were:

- what are the potential events?
- what are the particular tasks of aircrew and controllers?
- what are the risks associated with particular designs, latent design hazards, errors associated with fabrication, assembly, installation, removal, maintenance of the system, logistics, reliability, availability, specific computer-human considerations?

Assumptions:

- As identified in Safeflight 21, ADS-B is assumed to be paired with TIS-B

System State part of the scenario model used in this PHA analysis was based on "worst case" conditions. Worst cases condition, for the sake of this analysis are defined as:

- heavy traffic (maximum) conditions (peak operating times),
- weather deteriorated by severe condition, e.g., heavy rain/snow event accompanied by strong and varied winds (including shear conditions),
- at night, creating minimal visibility, and
- environmentally complex work areas (cockpits, towers).

Limitations:

- This was not an all inclusive system hazard analysis in that there are other scenarios to be addressed that equate to the total lifecycle of ADS-B as it will be integrated within the NAS.

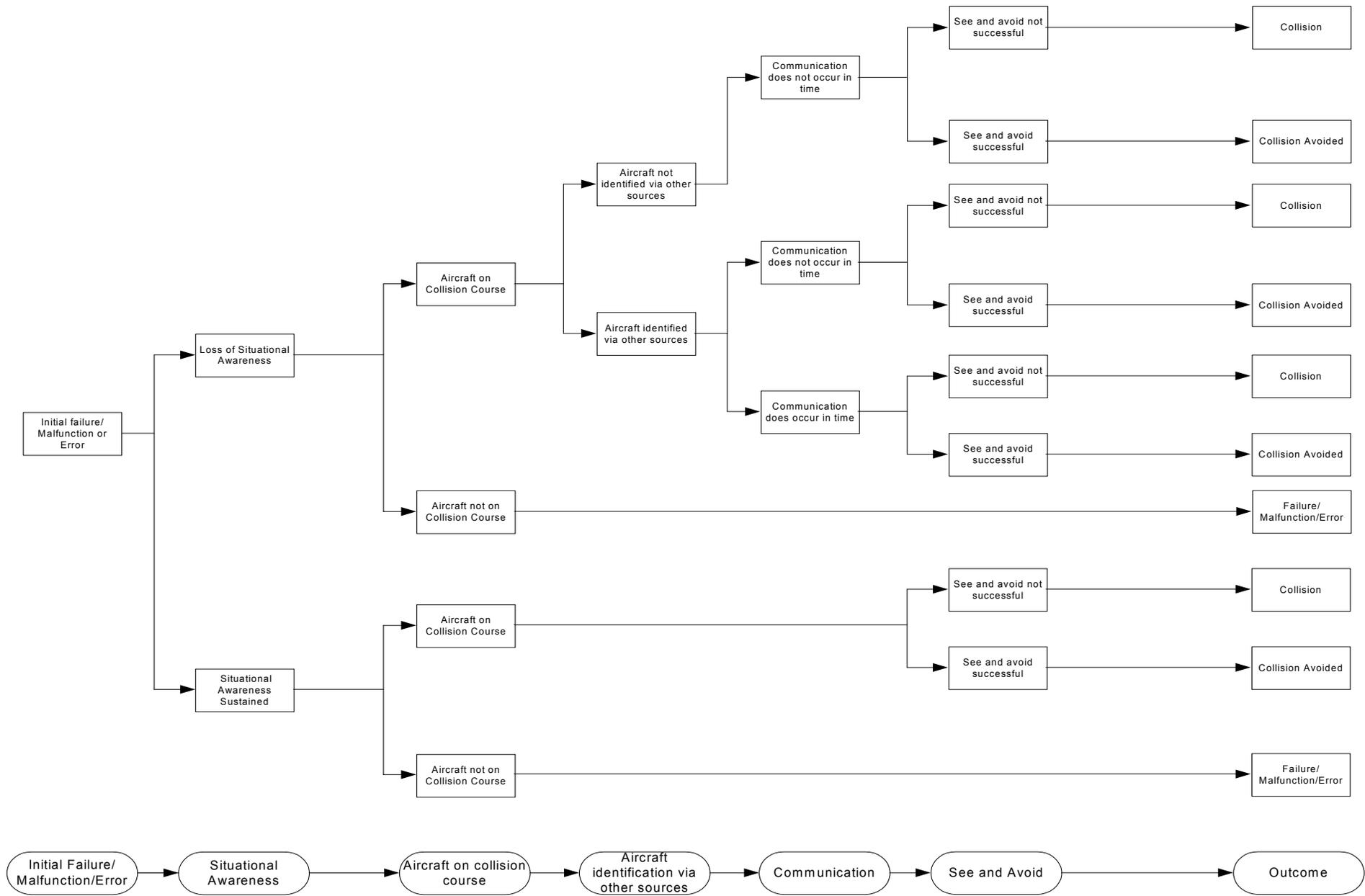
## **5.1 Scenario Model**

The SSH provides guidance on the use of a scenario to describe accidents that may cause harm, and therefore represent a hazardous situation. Two logic trees were developed, Visual Meteorological Conditions (VMC) and Instrument Meteorological Conditions (IMC). Figures 2 and 3 illustrate this concept.

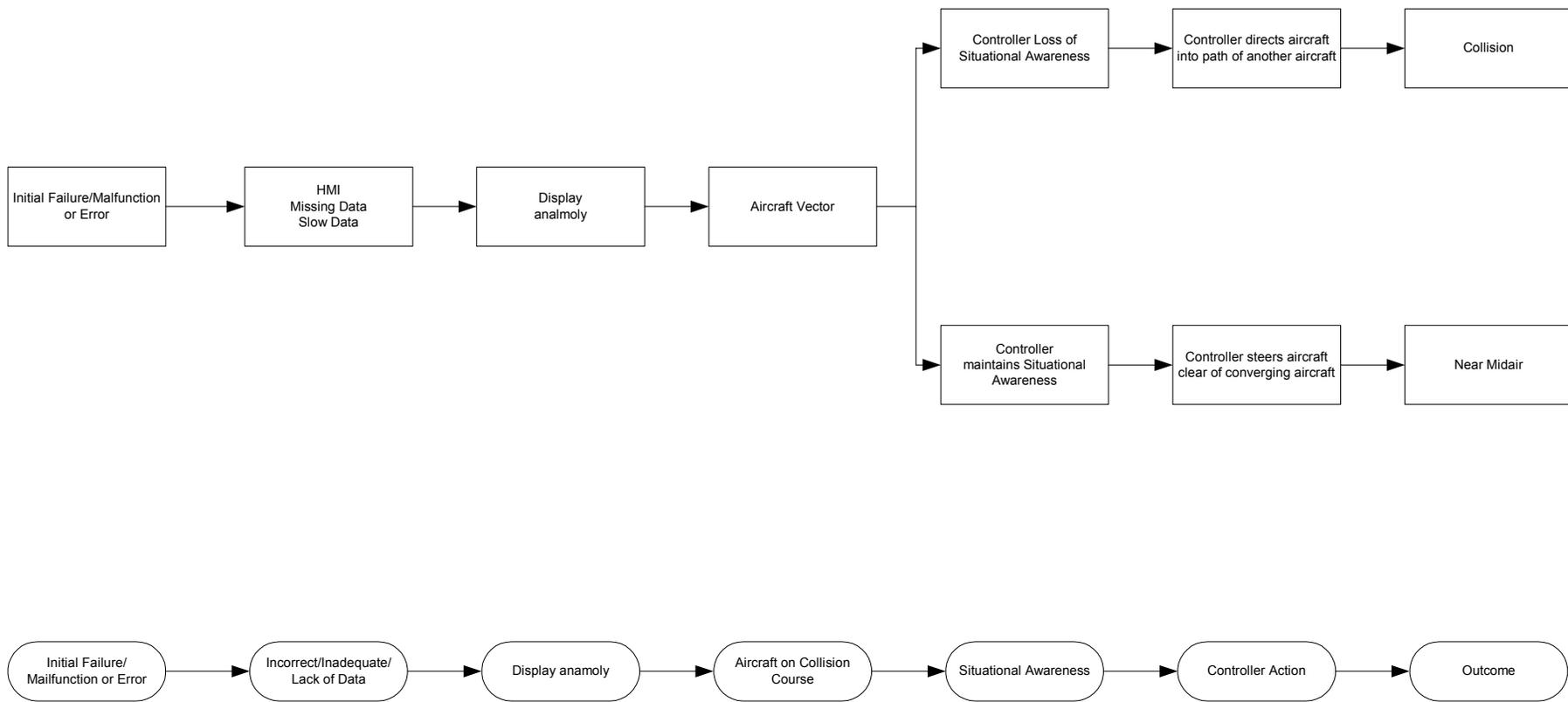
The models are based on the premise that an accident is usually not the result of a single cause. There may be an initial contributor, followed by subsequent contributors that lead to the possible effect. The possible effects can either be the best, middle, or worst-case credible potential effect.

In figure 5-2, visual conditions, the initial event is an ADS-B failure/malfunction/error, followed by the controller, if involved, being given inaccurate position information about one or more aircraft, resulting in confusion about where the airplanes really are, this confusion may reduce or cause total loss of situational awareness, resulting in misdirection of an aircraft and collision. However, since visual conditions exist it may be possible for the flight crew to see and avoid the pending collision, resulting in a Near Mid-Air Collision.

In figure 5-3, instrument conditions, the initial event is an ADS-B failure/malfunction/error, followed by the controller being given inaccurate position information about one or more aircraft, resulting in confusion about where the airplanes really are. This confusion may reduce or cause total loss of situational awareness, resulting in misdirection of an aircraft and collision.



**Figure 5-2 Safety Risk Analysis Model - Visual Meteorological Conditions**



**Figure 5-3 Safety Risk Analysis Model - Instrument Meteorological Conditions**

Another model that was used in the analysis is termed the 5M model. It is predicated on the concept that the total system comprises the Mission (i.e., what is the system trying to accomplish, as defined in the operational concept), the Machine (i.e., the system hardware and software), the Man (potential for human error in following rules and executing procedures), Media ( the operational state of the system, as well as the physical environment such as fog, rain, wind, ice, snow, and other related weather phenomena), and Management (i.e., Rules, regulations, procedures such as FAA Order for Air Traffic Control 7110.65. For ADS-B, the analysis considered the total end-to-end system, including hardware (systems and subsystems) and software failures, as well as the controller and the actions of the flight crew. As the analysis considered legacy systems malfunctions that might give misleading or conflicting information, reliability and availability requirements were, in limited instances, imposed as controls on them.

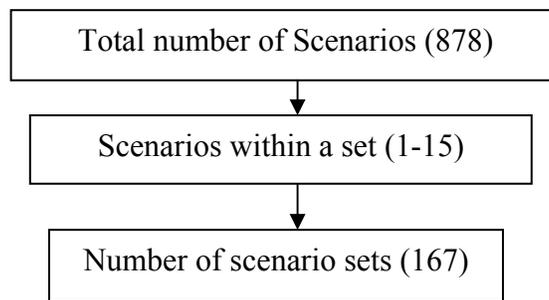


Figure 5-4 Scenario Set Logic Tree

Based on the above scenario set logic tree, eight hundred seventy eight scenarios (forty-one high risk scenarios/seven hundred ninety-eight medium risk scenarios/thirty-nine low risk scenarios) were generated. From there, the scenarios were further broken down into one hundred sixty-seven sets. See figure 5-2. In most cases, each set contains five to seven scenarios.

## 5.2 Risk Determination

Risk is determined by two factors: severity of consequence (i.e., what is the worst thing that can happen), and likelihood of occurrence (i.e., What is the probability or expected frequency that this series of contributors will result in the expected harm?). Risk is not determined by the likelihood that the hazard will occur, but that the worst credible effect (i.e., a collision of two aircraft) will occur.

The ADS-B PHA used the criteria contained in the SSMP for both severity and likelihood of occurrence. These are shown in Figures 5-5 and 5-6.

<b>Catastrophic</b>	Results in multiple fatalities.
<b>Hazardous</b>	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: (1) Large reduction in safety margin or functional capability (2) Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (3) Serious or fatal injury to small number of persons (other than flightcrew)
<b>Major</b>	Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – (1) Significant reduction in safety margin or functional capability (2) Significant increase in operator workload (3) Conditions impairing operator efficiency or creating significant discomfort (4) Physical distress to occupants of aircraft (except operator) including injuries Major occupational illness and/or major environmental damage, and/or major property damage
<b>Minor</b>	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Including - (1) Slight reduction in safety margin or functional capabilities (2) Slight increase in workload such as routine flight plan changes (3) Some physical discomfort to occupants or aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage
<b>No Safety Effect</b>	Has no effect on safety

**Table 5-5 - Severity of Consequence Criteria**

<b>Probable</b>	<b>Qualitative:</b> Anticipated to occur one or more times during the entire system/operational life of an item. <b>Quantitative:</b> Probability of occurrence per operational hour is equal to or greater than $1 \times 10^{-5}$
<b>Remote</b>	<b>Qualitative:</b> Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-5}$ , but greater than $1 \times 10^{-7}$
<b>Extremely Remote</b>	<b>Qualitative:</b> Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-7}$ but greater than $1 \times 10^{-9}$
<b>Extremely Improbable</b>	<b>Qualitative:</b> So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-9}$

**Table 5-6 - Likelihood of Occurrence Criteria**

Severity	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Likelihood					
Probable A	Low Risk	Medium Risk	High Risk	High Risk	High Risk
Remote B	Low Risk	Low Risk	Medium Risk	High Risk	High Risk
Extremely Remote C	Low Risk	Low Risk	Low Risk	Medium Risk	High Risk
Extremely Improbable D	Low Risk	Low Risk	Low Risk	Low Risk	Medium Risk

	<b>High Risk</b>
	<b>Medium Risk</b>
	<b>Low Risk</b>

**Table 5-7 – Risk Assessment Criteria**

Table 5-7 shows the criteria for risk acceptability. A high risk may be considered acceptable by the FAA, but in most cases all efforts must be made to mitigate or control the risk to a lower category. Medium and low risk acceptability are also defined in the figure.

The risk is then determined from the Risk Assessment Matrix shown in Table 5-7. Severity is shown in the top row, and likelihood in the left column. For a given scenario, the severity is first determined using the methodology above. In some cases the scenario postulated a collision of two aircraft, making it catastrophic by definition. The likelihood of occurrence was determined based on a qualitative judgment with input from experts familiar with the system and its operation. The intersection of Severity and Likelihood determines the level of risk acceptability on the matrix. For example, a “1 C” is of Catastrophic Severity (1), but Extremely Remote (C) Likelihood; Therefore, the risk is high.

### 5.3 Scenario Descriptions

The Preliminary Hazard Analysis matrix (models), as defined in Figure 5-1 above, has been designed to convey appropriate information related to a potential scenario, its worst case severity, flight phase in which the scenario can occur, and recommendations for precautions, controls and mitigations. The models are based on the premise that an accident is usually not the result of a single cause. Scenarios were further refined into sub-scenarios, with identifying hazard descriptions codes. The first 18 scenario codes in the PHA are based on the assumption aircraft are equipped with both ADS-B and CDTI. The ADS-B and CDTI equipped aircraft are defined below.

AFXO	Aircraft - Fixed Object
AFLO	Aircraft – Flying Object
AGV	Aircraft – Ground Vehicles
AOAA	Aircraft – Other Airborne Aircraft
ANAA	Aircraft – Non-Airborne Aircraft
AADF	Aircraft – Aircraft, Display Failure
AGDF	Aircraft – Ground Vehicle, Display Failure
SSDF	Surface Aircraft – Surface Aircraft, Display Failure
AFOD	Aircraft – Fixed Object, Display
AAAL	Aircraft – Aircraft, Approach and Landing
SR	Security Related
HF	Human Factors
SA	System Anomalies
LTAD	Less Than Adequate Design
EE	Environmental Effects
LTAD-NS	NAS Modernization Integrated System Hazards, Less Than Adequate Design
SA-NS	NAS Modernization Integrated System Hazards, System Anomaly
CP	Contingency Planning

The development of the PHA necessitated the development of new scenario set categories to cover additional risks associated with equipage combinations and the introduction of the ADS-B technology into the NAS. The remaining 13 scenario sets are based on the risks associated with the introduction of ADS-B technology/equipment into the existing NAS architecture with its legacy systems. The new scenario categories, labeled Integrated Systems (IS) and their sub-scenarios (scenario sets) A through L, present mixed equipage risks associated with various communication, phases of flight, and operations. In a number of scenarios either Cockpit Display of Traffic Information (CDTI) or Multi-Function Display (MFD) is identified. The CDTI provides information on the identification and location of all Mode A, C, and S equipped aircraft in system range. Based on the ADS-B assumptions described in Section 5.0 above, ADS-B equals ADS-B plus TIS-B, non-Mode A, C, and S equipped aircraft locations will also be provided from radar data from ground installations through TIS-B. The MFD provides all of the information found on the CDTI scope as well as displaying moving ground maps (terrain and identifying features) as well as weather-related information. The IS categories are provided below with their associated hazard descriptions.

## Basic Interactive Aircraft

IS-A1 Own Aircraft, ADS-B (Class A1), CDTI, TCAS – I, TIS  
IS-A2, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – I  
IS-A3, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – II, TIS  
IS-A4, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – II

## Separation and Sequencing

IS-B1, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – I, TIS  
IS-B2, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – I  
IS-B3, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – II, TIS  
IS-B4, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – II

## Flight Path Deconfliction Planning

IS-C1, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – I, TIS  
IS-C2, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – I  
IS-C3, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – II, TIS  
IS-C4, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – II

## Aircraft Broadcast Only

IS-D1, Own Aircraft, ADS-B (Class B1), CDTI  
IS-D2, Own Aircraft, ADS-B (Class B1), MFD  
IS-D3, Own Aircraft, ADS-B (Class B1), CDTI, TIS  
IS-D4, Own Aircraft, ADS-B (Class B1), MFD, TIS

## Ground Receive Systems, EnRoute and Terminal

IS-E1, ATS EnRoute and Terminal Area Operations, ADS-B  
(Class C1)

## Ground Receive Systems, Parallel Runway and Surface Operation

IS-F1, ATS Parallel Runway and Surface Operation, ADS-B  
(Class C2)

## Ground Receive Systems, Flight Following

IS-G1, Flight Following Surveillance, ADS-B (Class C3)

## Separation and Sequencing

IS-H1, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, TIS  
IS-H2, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I  
IS-H2, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I  
IS-H4, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II  
IS-H5, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, TIS,  
FIS  
IS-H6, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, FIS  
IS-H7, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II, TIS,  
FIS  
IS-H8, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II, FIS

## Flight Path Deconfliction Planning) ISI Series

IS-I1, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TIS  
IS-I2, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I  
IS-I3, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TIS  
IS-I4, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II

Flight Path Deconfliction Planning and Terrain Awareness Warning System), ISJ Series  
IS-J1, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TIS,  
TAWS  
IS-J2, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TAWS  
IS-J3, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TIS,  
TAWS  
IS-J4, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TAWS  
Wide Area Augmentation System / Local Area Augmentation System/ FMS/ L1  
Frequency) IS-K series  
Integration Specific NAS/World-Wide Risks IS-L Series

Integration Specific NAS/World-Wide Risks - Increased Risks - IL-IS Series

In most cases, scenarios are grouped into hazard scenario "sets," A set consists of a scenario theme, which is a combination of system state and contributors to a sequence of events that result in a postulated harm. The contributors are varied in combinations and permutations of system failures and inappropriate human action or response. Each variation in a scenario set may affect either severity or likelihood, or both and may identify a new or different control requirement.

Scenario descriptions are short concise statements that define the basic scenario (the circumstances and outcome expected from the full tabular scenario data). The severity is the worst-case severity or harm expected should the scenario occur. Risk is based upon Table 3.1-1, Operational Safety Assessment Hazard Classification Matrix the FAA System Safety Management Plan. The left-hand number refers to the "Effect on" column, the right-hand number refers to the Hazard Classification. Possible Effect indicates the worst case harm expected. Flight Phase defines when in the life cycle the event could occur, i.e. Takeoff, Landing, Approach, Terminal, Surface, EnRoute, Oceanic, etc.

It is expected that the associated hazards will be eliminated or controlled to an acceptable level should appropriate implementation of the Controls and Mitigation's occur. Since this is the case, high-level Safety Requirements have been defined from these Controls and Mitigation's.

In some situations, due to the maturity of the design, further analysis and study is required to refine the Controls and Mitigations. The related specifics and other considerations are discussed below.

## 5.4 System Safety Order of Precedence

The order of precedence for satisfying system safety requirements and resolving identified risks is as follows:

Description	Priority	Definition
<u>Design for minimum risk.</u>	1	From the first design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.
<u>Incorporate safety devices.</u>	2	If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.
<u>Provide warning devices.</u>	3	When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response.
<u>Develop procedures and training.</u>	4	Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic or critical severity.

Table 5-9 Safety Order of Precedence

## 6.0 Hazard Identification and Analysis

Within the scenario analysis technique, eighteen sub-scenario codes were defined. For each sub-scenario code there are a number of scenarios defined. This section discusses the worst case scenarios analyzed, and the rationale for the specific risk indicated.

### 6.1 Scenario Discussions

The thirty-one scenario set codes are listed below along with the worst-case scenario and associated risk rationale. The first 18 assume ADS-B only applications with CDTI or MFD. The remaining 12 treat ADS-B operating with other equipment such as TCAS, TIS-B, etc.

### **6.1.1 AFXO – Aircraft –Fixed Object**

There are three scenario sets (21 total scenarios) discussed, AFXO-01, 02, 03. These scenarios address collision of an aircraft with a fixed object. Either the fixed object is not equipped with ADS-B, or ADS-B has failed on the subject aircraft or on the fixed object. The worst case event considers collision of the subject aircraft with a fixed object assuming reliance on ADS-B only with minimal controls applied. The worst case also assumes low visibility weather conditions. The event can occur during take-off, or landing, during approach or on the airport surface. To control these risks, the following controls have been identified and recommended requirements have been indicated: The ADS-B system should be designed to automatically detect system failures or malfunctions and these should be communicated to the aircrew and to air traffic controllers. It is important that failures and/or malfunctions be reported as soon as possible to allow aircrews and ground controllers time to take appropriate action.

Safe operating procedures by the aircrew can reduce these risks using “see and avoid” procedures. Equipping fixed objects with lights and markings will enhance the “see and avoid” procedures.

### **6.1.2 AFLO – Aircraft – Flying Object**

Three scenario sets (20 total scenarios) are analyzed. In all three scenario sets, the worst case event is a collision of an ADS-B equipped aircraft with another flying object, such as launch vehicles, hot air balloons, ultralights, etc). The contributor to the collision is either the flying object which is not equipped with ADS-B, or it is equipped but ADS-B has failed, or ADS-B has failed on the subject aircraft. The operational environments include Oceanic, EnRoute, and Terminal domains.

The controls identified in 6.1.1 are applicable to this scenario. Additionally, an alternate means of detecting flying objects, such as ATC warnings is required to reduce the risks associated with this scenario.

### **6.1.3 AGV – Aircraft – Ground Vehicle**

Three scenario sets (20 total scenarios) are analyzed. In all three scenario sets, the worst case event is a collision of an ADS-B equipped aircraft with a ground vehicle. The cause of the collision is because the ground vehicle is not equipped with ADS-B, or it is equipped and has failed, or because the ADS-B on the subject aircraft has failed. The operational environment is the airport surface. Dense fog during darkness poses the worst case if the subject aircraft is relying on ADS-B only for surveillance.

Controls identified for these scenarios are similar to those previously identified, however, in this case an alternate means of detecting the aircraft and informing the ground vehicle operator is required, e.g., ASDE-X, ASDE-3, ASDE-3b, etc.

### **6.1.4 AOAA – Aircraft –Other Airborne Aircraft**

These two scenario sets (12 total scenarios) are a special case of 6.1.2 where the flying object is another airborne aircraft. The three inadvertent collision cases are due to failure of ADS-B on either aircraft, or because the other airborne aircraft is not equipped with ADS-B. Worst case is in severe meteorological conditions where there is reliance on ADS-B only for surveillance input.

Control for these risks require an alternate means of detecting the other airborne aircraft, such as TCAS, or ATC warnings based on surveillance radar.

#### **6.1.5 ANAA - Aircraft – Non-airborne Aircraft**

These three scenario sets (20 total scenarios) are similar to 6.1.3 AGV, where the surface vehicle is another aircraft. It is of significance because of the frequency and severity of runway incursion accidents. In this scenario, either ADS-B has failed on the subject aircraft, the other non-airborne aircraft, or the other aircraft lacks ADS-B equipage. During the transition to full equipage of all commercial and GA aircraft, this is a credible accident scenario. The worst case involves weather and darkness combinations that inhibit “see and avoid” procedures on the airport surface.

Control of these risks require an alternate means of detecting the non-airborne aircraft and informing the flight crews of its position.

#### **6.1.6 AADF Aircraft –Aircraft Display Failure**

In these four scenario sets (26 total scenarios) scenario, there are four failures that cause the inadvertent collision:

- Erroneous position data transmitted by the subject aircraft
- Erroneous position data transmitted by the other aircraft
- Failure of the subject aircraft’s cockpit display
- Failure of the other aircraft’s cockpit display

All four failures occur in worst case weather/darkness conditions where ADS-B is the only source of surveillance data.

Two controls are of particular significance in controlling these risks: Design ADS-B to detect and report malfunctions/erroneous data, and provide an alternate means of detecting aircraft position. Contingency procedures should also be exercised to reduce these risks.

#### **6.1.7 AGDF Aircraft – Ground Vehicle Display Failure**

There are only two variations on these scenario sets (12 total scenarios). First is that the Ground Vehicle is transmitting erroneous position information. Second is that the subject aircraft cockpit display fails. Again, worst case visibility conditions with ADS-B as sole surveillance input.

As indicated in AGV above, the most significant control identified is to have an alternate means of detecting the ground vehicle and informing the aircraft crew.

#### **6.1.8 SSDF Surface Aircraft –Surface Aircraft Display Failure**

This is a special case of runway incursion or airport surface collision on taxiways. There are four possible causes (12 total scenarios) analyzed:

- Erroneous position data transmitted by other surface aircraft
- Erroneous position data transmitted by the subject aircraft
- Failure of subject aircraft’s display
- Failure of other aircraft’s display

Controls are similar to the Aircraft to Aircraft Display failure case above. The two controls that are of particular significance in controlling these risks are (1). Design ADS-B to detect and report malfunctions/erroneous data, and (2) provide an alternate means of detecting aircraft position. Contingency procedures should also be exercised to reduce these risks.

#### **6.1.9 AFOD Aircraft –Fixed Object – Display Failure**

In these two scenario sets (12 total scenarios) display failure occurs either due to ADS-B transmitting erroneous position information, or the on-board CDTI fails.

Controls: Design ADS-B to assure that failures/malfunctions are detected and reported to automatically to affected aircrew.

#### **6.1.10 AAAL Aircraft – Aircraft –Approach and Landing**

This scenario set (7 total scenarios) involves the loss of separation assurance during terminal approach due to ADS-B failure. One application that is of particular importance is simultaneous approaches to parallel runways. The worst case assumes reliance on ADS-B-only for surveillance input, and worst case visibility conditions.

Controls for these risks require high availability of ADS-B and an alternate means of obtaining surveillance data due to the time-criticality of two aircraft in this situation. High availability of the ADS-B system is vital to minimize the risk associated with this scenario. Should the ADS-B system fail in this application, increased risk of loss of separation can occur. Also, ATC contingency procedures must be applied in the event that ADS-B fails. In addition, ATC and air crew training in contingency procedures is vital in reducing these risks.

#### **6.1.11 SR - Security Related**

These two scenario sets (14 total scenarios) discuss loss of separation during terminal approach due to intentional “jamming” of the ADS-B signal, or “spoofing” in which hackers breach system security.

The design of the ADS-B system requires physical and electronic security protection means such as intrusion detection, intrusion protection, e.g., message authority verification, and other mitigation to assure that intentional threats have been controlled.

#### **6.1.12 HF - Human Factors**

Six scenario sets (40 total scenarios) were analyzed that might result in increased collision risk. These are;

- Excessive controller workload resulting in loss of situational awareness due too excessive displays clutter.
- Excessive pilot workload resulting in loss of situational awareness due to excessive display clutter, i.e., too much information on the CDTI.
- Inappropriate or erroneous communication due to language barrier
- Loss of separation assurance due to erroneous “future intent” messages, due to pilot error
- Inadequate Computer Human Interface design causes inappropriate or erroneous communication.
- Inappropriate or erroneous communication due to language barrier results in loss of situational awareness and increased collision risk between aircraft and ground vehicle.

There are specific controls that affect Human Factors that are required.. They involve the following:

- The ADS design should accommodate international communications in accordance with acceptable human factors design practices and standardized ICAO agreements.
- Provide alternate means of communications, i.e., voice backup to minimize the potential for miscommunication.
- Potential loss of situational awareness can occur due to excessive aircrew and/or controller workload. Research effort is needed to understand and minimize the potential for loss of situational awareness.

#### **6.1.13 SA - System Anomalies**

There are 30 scenario sets (204 total scenarios) which illustrate system anomalies that were analyzed for their impact on safety of ATC operations using ADS-B only as the surveillance input. They cover a wide variety of possible causes that range from errors in one or more parts of the state vector transmission, e.g., latitude, longitude, heading, etc. to saturation of the frequency spectrum being used for transmission.  
involve:

The most appropriate controls to minimize the potential for system anomalies involve:

- The system shall be designed to insure that no single failure, common mode failure, human error, or design feature can cause a catastrophic event.
- The system shall be designed to ensure that dual independent component failure, dual human errors, or a combination of a component failure and human error cannot cause a catastrophic event.
- The system should be designed to assure that no single software anomaly, common software malfunction, or design feature shall result in a catastrophic event.

There are a number of other controls required which address specific anomaly scenarios that are listed in Appendix A

#### **6.1.14 LTAD – Less Than Adequate Design**

These three scenario sets (21 total scenarios) should properly be termed Latency Effects, because the three all consider the effects of latency errors in processing the input data, the communication link, and the application processing. The result is a loss of data integrity due to excessive elapsed time between the data acquisition and data display on the airborne or ground displays

In this case, the control is straight forward. Latency requirements for the transmitter, receiver and communications link are specified in NAS-SR-1000.

#### **6.1.15 EE – Environmental Effects**

Two scenario sets (8 total scenarios) were analyzed related to environmental effects. The first one concerned weather effects on ADS-B that would cause “blind spots”. These effects may be unique to a given technology being considered. The second sub-scenario concerned effects of the natural environment, such as solar flares, Gamma Rays, and other electromagnetic anomalies.

To minimize potential for adverse weather affecting communications, it is required that the appropriate frequency spectrum is selected, in that alternate frequency spectrum be made available as a redundancy. Ground stations should also be designed to minimize the effects of lightening or other adverse weather conditions.

The ADS-B system should be hardened against electromagnetic interference.

#### **6.1.16 LTAD -NS – Less Than Adequate Design**

These two scenario sets (8 total scenarios) changes the earlier assumption that the operation was based on ADS-B ONLY. In this case, ADS-B is assumed to be integrated with other NAS Modernization automation systems. Two sub-scenarios were identified that could result in a collision. First was less-than-adequate human factors design integration of ADS-B with other NAS Modernization automation systems, such as CPDLC, FIS, TCAS, TIS, etc. The concern is that too much information in the cockpit, if it is not properly integrated, may cause confusion, or loss of situational awareness.

The second concern was that redundant flight critical information could be conflicting. For example, if TCAS provides alarm information that is not consistent with information provided by ADS-B, the aircrew may become confused, or delay taking action to avoid a collision.

Mitigation of the risk for these scenario sets involve research activities such as analysis and simulation, or flight tests with teams of pilots and controllers to determine acceptable limits on the display of information and acceptable ways to display the information in an integrated system, to avoid confusion, or information overload. The results of these studies can then be translated into design requirements.

#### **6.1.17 SA –NS System Anomaly – NAS Context**

These two scenario sets (14 total scenarios) are similar to 6.1.16 LTAD, except the cause of conflicting information to the cockpit or air traffic controller is a system anomaly as opposed to inadequate design. The result is the same, however, redundant, conflicting flight critical information that leads to the wrong response, or a delayed response.

In this case, the design must eliminate the potential for system anomalies that would result in conflicting information. Adequate testing is also required to ensure that the design requirements have covered all known anomalies.

#### **6.1.18 CP – Contingency Planning**

Less than adequate contingency planning, as shown in this one scenario set (7 total scenarios) results in possible increased collision risk due to confusion over responsibility for separation assurance in a shared responsibility environment, e.g., Free Flight Phase One.

These procedures must be worked out in simulations or preferably, flight tests to cover all contingency situations that can be identified.

#### **6.1.19 IS-A Integrated Systems - Basic Interactive Aircraft**

These six scenario sets (35 total scenarios) deal with collision of subject aircraft with other aircraft due to ADS-B malfunction and TCAS-I or Conflict Avoidance malfunction, or conflicting information on CDTI, TCAS, or TIS.

The control of these scenario sets requires the ADS-B System, air and ground equipment, be designed to automatically report system failure/ malfunction to ATC and affected aircrews and to have contingency plans in the event of system loss. Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2) and ensure system will integrate with TIS and TCAS-I and/or other systems integrate with ADS-B system and provide redundant alert against collision risk. All ADS-B avionics need be certified, installed and an approval process established .

In addition, the ADS-B equipment shall be designed to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations.

#### **6.1.20 IS-B Integrated Systems - Separation and Sequencing**

These four scenario sets (24 total scenarios) examines loss of separation and sequencing assurance due to ADS-B malfunction, with TCAS-I, TCAS-II, TIS or CDTI malfunction contributing to loss of separation.

The controls for these scenarios require ADS-B system be designed to assure that system failures/malfunctions are detected and reported automatically to affected personnel in accordance with FAA CT-96/1. The system must be designed to prevent single point failures and require Avionics certification, installation, and approval process established for ADS-B with TCAS-II and CDTI. The design should also protect against interference. As in all cases where system failure is postulated there must be contingency procedures

#### **6.1.21 IS-C Integrated Systems - Flight Path Deconfliction Planning**

These four scenario sets (24 total scenarios) considers loss of separation assurance during flight path deconfliction planning due to ADS-B malfunction, TCAS-I, TCAS-II, TIS, or CDTI malfunction.

The controls for these scenarios are similar to those in ISA and ISB and require ADS-B system be designed to assure that system failures/malfunctions are detected and reported automatically to affected personnel in accordance with FAA CT-96/1. The system must be designed to prevent single point failures and require Avionics that a certification, installation, and approval process be established for ADS-B with TCAS-II and CDTI. The design should also protect against recognized forms of interference, such as EMI, jamming, and spoofing. As in all cases where system failure is postulated contingency procedures must be developed.

#### **6.1.22 IS- Integrated Systems - Aircraft Broadcast Only**

These four scenario sets (24 total scenarios) consider loss of separation assurance due to ADS-B malfunction, and a TCAS-II or CDTI malfunction. Loss of ability of own aircraft to be seen by Class A and Class C users due to ADS-B malfunction on own aircraft.

Mitigation of the risks identified in ISD scenario sets is accomplished through design requirements which ensure failure isolation of ADS-B hardware and that the system fails safe. In addition the system shall be designed to assure that dual independent component failure, dual human errors, or a combination of a component failure and a human error cannot cause a catastrophic event. In addition, as aircraft identification is essential to successful system operation, design the system to minimize the potential of loss of targets. It is prudent to require all airborne craft, identified as potentially hazards to navigation, be equipped with ADS-B transmitters, or other appropriate automated means of identification. As in all scenarios covering aircraft and ground installations, avionics equipment must meet the certification, installation, and approval process established for ADS-B. As in all cases where system failure is postulated contingency procedures must be developed.

#### **6.1.23 IS- Integrated Systems - ATS EnRoute and Terminal Area Operations**

This one scenario set (9 total scenarios) considers degraded surveillance due to ADS-B malfunction on single aircraft.

Control of the ATS EnRoute and Terminal Area Operations system is accomplished through engineering design to eliminate or reduce the potential of malfunction within sensor fusion system or interface and to assure that system failures/malfunctions are detected and reported automatically. . As in all scenarios covering aircraft and ground installations, avionics equipment must meet the certification, installation, and approval process established for ADS-B. As in all cases where system failure is postulated contingency procedures must be developed.

#### **6.1.24 IS-F Integrated Systems - Ground Receive Systems, Parallel Runway and Surface Operation**

This one scenario set (10 total scenarios) examines what happens when a collision occurs during parallel runway operations due to ADS-B malfunction. TCAS – I or II or TIS, not helpful.

Controls for the risks identified in Ground Receive Systems, Parallel Runway and Surface Operation is accomplished by designing the system to eliminate or reduce the likelihood of malfunction within the sensor fusion system or interface and assure that system failures/malfunctions are detected and reported automatically. In the event of a failure/malfunction, provide for appropriate ATC/Aircrew contingency procedures and ATCT use of applicable 7110.65 procedures for validating aircraft ID, position, and altitude and provide alternate means of identifying other aircraft/vehicle/fixed object

Design ADS-B System to conform to FAA CT-96/1 and to automatically report system failure/ malfunction to ATC and affected aircrews. Apply system reliability and availability requirements (TBD) to eliminate or control the risk of failures, system anomalies, and malfunctions.

Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations. Design TIS, TCAS-I and II, to integrate with ADS-B and provide redundant alert against collision risk. Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2).

#### **6.1.25 IS-G Integrated Systems - Ground Receive Systems, Flight Following**

This one scenario set (3 total scenarios) covers loss of private user flight following surveillance due to ADS-B malfunction.

Design ADS-B system to minimize the potential of loss of flight following surveillance to assure that system failures/malfunctions are detected and reported automatically to ATC and affected aircrews. Failure/malfunction indication shall be designed to conform to FAA CT-96/1. If a malfunction occurs the ATCT will use 7110.65 procedures for validating aircraft ID, position, and altitude. In the event of a malfunction/loss, ATC/Aircrew contingency procedures should be developed which include an alternate means of identifying other aircraft/vehicle/fixed object.

The system should be designed such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2), applying appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions. In addition, apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions.

#### **6.1.26 IS-H Integrated Systems - Separation and Sequencing**

These eight scenario sets (96 total scenarios) covers loss of separation assurance and sequencing due to ADS-B malfunction, TCAS-I, TCAS-II, or MFD or TIS malfunction contributes to collision. Loss of separation assurance due to ADS-B malfunction results in collision.

Design ADS-B to assure that system failures/malfunctions are detected and reported automatically to ATC and affected aircrews. Failure/malfunction indication shall be designed to conform to FAA CT-96/1. If a malfunction occurs than ATCT will use 7110.65 procedures for validating aircraft ID, position, and altitude.

Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2). Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions. Avionics certification and ground vehicle installation, and approval process established for ADS-B with TIS, MFD, TCAS-I, and TCAS-II, with TIS and TCAS-I to provide redundant alert against collision risk. As with all key electronics, design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations.

#### **6.1.27 IS- I Integrated Systems - Flight Path deconfliction Planning**

These four scenario sets (27 total scenarios) considers loss of separation assurance flight deconfliction planning due to ADS-B malfunction. TCAS-I, TCAS-II, TIS or MFD malfunction contributes to outcome.

Controls of the Flight Path deconfliction Planning scenarios are covered, as in 6.1.26, through the following control measures: Design ADS-B to assure that system failures/malfunctions are detected and reported automatically to ATC and affected aircrews. Failure/malfunction indication shall be designed to conform to FAA CT-96/1. If a malfunction occurs than ATCT will use 7110.65 procedures for validating aircraft ID, position, and altitude.

Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2). Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions. Avionics certification and ground vehicle installation, and approval process established for ADS-B with TIS, MFD, TCAS-I, and TCAS-II, with TIS and TCAS-I to provide redundant alert against collision risk. As with all key electronics, design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations.

#### **6.1.28 IS-J Integrated Systems - Flight Path Deconfliction Planning and Terrain Awareness Warning System**

These four scenario set (36 total scenarios) considers loss of separation assurance due to ADS-B malfunction impacting the flight path deconfliction planning and terrain awareness warning system. TCAS-I, TCAS-II, TIS or MFD malfunction contributes to outcome.

Design ADS-B System to automatically report system failure/ malfunction to ATC and affected aircrews with failure/malfunction indication designed to conform to FAA CT-96/1. Provide for appropriate ATC/Aircrew contingency procedures. In addition, require avionics and ground systems certification, installation, and approval process established for ADS-B with TIS, TCAS-I, TCAS-II, MFD, and TAWS.

Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions. Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2).Design ADS-B to assure that system failures/malfunctions are detected and reported automatically. Provide alternate means of identifying other aircraft/vehicle/fixed object.

MFD or CDTI, TAWS, and TCAS-I and II must be designed, where necessary, to integrate with ADS-B, provide redundancy, maximize system alert capability, redundant alert against collision, and minimize alert delay or masking of alert, and minimizes conflictive information communicated in cockpit. As with all communications function, design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations.

#### 6.1.29 IL-IS Integrated Systems - Integration Specific NAS/World-Wide Risks - Increased Risks

These eighteen scenario sets (23 total scenarios) covers one or two single scenario events which cover a wide-ranging group of unlinked hazards.

- The Unidentified aircraft intruder enters ADS-B airspace.
- Incremental risks not adequately addressed presents.
- Mixed-equipage airspace presents confusion and loss of situational awareness to controllers.
- LTA cross-checking of barometric altimeter with GPS (ADS-B) fails to identify deviation in altitude.
- Mixed-equipage airspace presents confusion and loss of situational awareness to controllers.
- LTA cross-checking of barometric altimeter with GPS (ADS-B) fails to identify deviation in altitude. .
- Unsuccessful conflict resolution between controllers and pilots.
- LTA visual identification of other aircraft by subject aircraft pilots/aircrew results in inappropriate communication with ATCT.
- Accuracy delta between ADS-B and TIS-B presents difficulty in target identification and increased accident risk.
- Inappropriate use of call sign or other language results in miss-communication.
- System inaccuracies between ADS-B and other subsystems result in inadvertent contact with wake vortex.
- Communication delay as a result of LTA mixed equipage procedural integration.
- Conflicts between subsystems (ADS-B, TCAS, TAWS, TIS) state data results in inaccurate assumptions associated with separation.
- LTA integration of audible alerts issued by ADS-B, TCAS, TAWS, TIS, and results in confusion.
- Pilot/flight crew enhanced traffic awareness results in increased go-around or rejected takeoffs.
- Time from when a hazardous situation develops to the time the pilot takes corrective action is insufficient due to ADS-B malfunction, failure, or anomaly. .
- System (Integrated System) time source is unsynchronized resulting in inaccurate position, velocity and time.
- Inadvertent access into SUA due to ADS-B malfunction, failure, or anomaly.
- LTA training associated with ADS-B design, maintenance, or operation.
- Collision with terrain or aircraft or fixed object or flying object, or vehicle during approach or landing or takeoff as a result of ADS-B malfunction, failure, or anomaly due to close proximity.

Design ADS-B to assure that system failures/malfunctions are detected and reported automatically to ATC and affected aircrews and that alternate means are provided for identifying other aircraft/vehicle/fixed object. Provide for appropriate ATC/Aircrew contingency procedures.

Failure/malfunction indication shall be designed to conform to FAA CT-96/1. The design of the system must insure that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2). The avionics and ground system certification, installation, and approval process must conform to that established for ADS-B and be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations

Design WAAS and LAAS, MFD or CDTI, TAWS, and TCAS to integrate with ADS-B, provide redundancy, maximize system alert capability, and minimize alert delay or masking of alert. Design system to minimize the potential for interface malfunction between FMS and ADS-B and select frequency spectrum to minimize adverse effects of weather on ADS-B transmissions and consider alternative frequency spectrum as backup.

Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions and to ensure failure isolation of hardware, firmware, and software.

#### **6.1.30 IS-K Integrated Systems - Wide Area Augmentation System / Local Area Augmentation System/ FMS/ L1 Frequency**

These twelve scenario sets (27 total scenarios) considers loss of separation assurance due to ADS-B malfunction as impacted through the Wide Area Augmentation System / Local Area Augmentation System/ FMS/ L1 Frequency.

- Interface malfunction between FMS and ADS-B results in loss of ADS-B.
- Degraded FMS input to ADS-B results in decreased accuracy.
- ADS-B malfunction propagates to FMS Failure of FMS results in loss of ADS-B.
- ADS-B malfunction propagates to other aircraft systems, effecting WAAS
- Loss of L1 frequency results in loss of: ADS-B, GPS, LAAS and WAAS. Event occurs during critical time, CAT IIIa, IIIb, or IIIc approaches.
- Interface malfunction between FMS and ADS-B results in loss of ADS-B.
- Degraded FMS input to ADS-B results in decreased accuracy.
- ADS-B malfunction propagates to FMS
- Failure of FMS results in loss of ADS-B.
- ADS-B malfunction propagates to other aircraft systems, effecting WAAS
- Loss of L1 frequency results in loss of: ADS-B, GPS, LAAS and WAAS.
- Interface malfunction between FMS and ADS-B results in loss of ADS-B.

Controls for these 12 sets require the protection of the system frequency spectrum to minimize adverse effects of weather on ADS-B transmissions and an alternative frequency spectrum as backup.

Design ADS-B System to automatically report system failure/ malfunction to ATC and affected aircrews with failure/malfunction indication designed to conform to FAA CT-96/1. The system must also provide for appropriate ATC/Aircrew contingency procedures and provide alternate means of identifying other aircraft/vehicle/fixed object. Controls must also ensure ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude.

Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2). Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions. Design ADS-B system architecture to ensure failure isolation of hardware, firmware, and software. Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations. Finally, controls must develop avionics certification and ground systems, installation, and approval process for ADS-B.

Design system to provide redundancy, minimize the potential for interface malfunction between WAAS and LAAS, FMS, MFD or CDTI, TAWS, and TCAS and ADS-B, maximize system alert capability, and minimize alert delay or masking and for the potential for degraded FMS input to ADS-B.

#### **6.1.31 IS-L Integrated Systems - Integration Specific NAS/World-Wide Risks**

These twenty-four scenario sets (28 total scenarios) considers the integration of ADS-B into the NAS and Foreign airspace

..

- Unidentified aircraft intruder enters ADS-B airspace and poses collision risk.
- Incremental risks not adequately addressed present increased risk of accident.
- Mixed-equipage airspace presents confusion and loss of situational awareness to controllers.
- LTA cross-checking of barometric altimetry with GPS fails to identify deviation in altitude, which results in increased collision risk.
- Unsuccessful conflict resolution between controllers and pilots results in increased collision risks.
- LTA visual identification of other aircraft by subject aircraft pilots/aircrew results in inappropriate communication with ATCT and increased collision risks.
- Accuracy delta between ADS-B and TIS-B presents difficulty in target identification and increased accident risk.
- Inappropriate use of call sign or other language results in miss-communication and increased collision risks.
- Inappropriate use of new terminology or phraseology results in miss-communication and increased collision risk.
- System inaccuracies between ADS-B and other subsystem results in inadvertent contact with wake vortex and increased accident risks.
- Communication delay as a result of LTA mixed equipage procedural integration results in increased collision risks.
- Conflicts between subsystems (ADS-B, TCAS, TAWS, TIS) state data results in inaccurate assumptions associated with separation and increased accident risks.
- LTA integration of audible alerts issued by ADS-B, TCAS, TAWS, TIS, and results in confusion and increased collision risks.
- LTA integration of Airborne Conflict Management (ACM) results in increased collision risks.

- Pilot/flight crew increase in traffic awareness results in increased go-around or rejected takeoffs.
- Time from when a hazardous situation develops to the time the pilot takes corrective action is insufficient
- System (Integrated ADS-B System) time source is unsynchronized resulting in inaccurate position, velocity and time.
- Malfunction within Data Fusion processing results in undetected corruption of safety-critical information and increased collision risks.
- LTA integration of national and international separation standards increases collision risks associated with ADS-B use.
- LTA airspace transition integration results in increased collision risks.
- LTA ADS-B equipage or site coverage results in inadequate coverage and increased collision risks..
- LTA integration of ADS-B coverage areas results in “blind spots” and increased collision risks.
- Corruption of ADS-B message formats data results in increased collision risks.
- Loss of safety-critical information/communication to pilot/aircrew as a result of ADS-B malfunction increases accident risk associated with SUA or weather.

Controls of scenarios covering Integration Specific NAS/World-Wide Risks are broad-based therefore the primary concerns/controls are listed below.

Controls require procedures for validating aircraft ID, position, and altitude and controller/pilot training and procedures are in place for ADS-B, to minimize human error and increase situational awareness.

Controls also need to determine the threshold values for ADS-B coverage area to assure controller/pilot adequate situational awareness, as well as require all flying objects that can become hazards to navigation be equipped with ADS-B transmitters, or other appropriate means of identification.

Design system to minimize the potential of loss of targets and failure of Conflict Avoidance function.

Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize the potential for LTA communication, maximize system alert capability, and integration of audible alerts, and minimize conflictive information communicated in cockpit.

Conduct analysis, studies, and simulations and/or flight-tests to develop engineering requirements and/or procedures to minimize the risks of unsuccessful conflict resolution between controllers and pilots. Conduct human factor analyses, evaluations, and/or simulations to identify safety-related risks associated with the integration of ADS-B system into the NAS.

Avionics ground system certification, installation, and approval process established for ADS-B.

Require all aircraft that can become hazards to navigation be equipped with ADS-B transmitters, or other appropriate automated means of identification.

Develop appropriate training materials and training programs to ensure that all participants in a shared responsibility environment understand their role and safe operation procedures.

Design ADS-B system architecture to ensure failure isolation of hardware, and ensure that hardware, firmware and software fail safe. Design the system to assure that dual independent component failure, dual human errors, or a combination of a component failure and a human error cannot cause a catastrophic event.

Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-G, MIL-STD-461D, MIL-STD-436D and FCC Regulations.

## 6.2 Preliminary Hazard Analysis

### 6.2.1 Preliminary Hazard Analysis Tables

Table 6-1 contains the Preliminary Hazard Analysis in a tabular format as prescribed in the System Safety Management Program, May 1, 2001. It is structured by Scenario and Sub-scenario. It contains a Scenario Description (the overall scenario theme), risks, Possible Effect, Flight Phase, Recommendations for Precautions, Controls and Mitigations, and a Comments column that helps explain the differences between some of the scenarios that sound very similar. Each recommended precaution, control or mitigation is given a unique control number. In many cases, the same control applies to several sub-scenarios. There are approximately 89 unique control numbers.

<b>AFXO Aircraft - Fixed Object</b>			
<p>There are three scenarios discussed, AFXO-01, 02, 03. These scenarios address inadvertent collision of an aircraft with a fixed object. Either the fixed object is not equipped with ADS-B, or ADS-B has failed on the subject aircraft or on the fixed object.</p> <p>The worst case event considers inadvertent collision of the subject aircraft with a fixed object; assuming reliance on ADS-B only with minimal controls applied. The worst case also assumes low visibility weather conditions. The event can occur during take-off, or landing, during approach or on the airport surface.</p> <p>To control these hazards, the following controls have been identified and recommended requirements have been indicated: The ADS-B system should be designed to automatically detect system failures or malfunctions and these should be communicated to the aircrew and to air traffic controllers. It is important that failures and/or malfunctions be reported as soon as possible to allow aircrews and ground controllers' time to take appropriate action.</p> <p>Safe operating procedures by the aircrew can reduce these risks using "see and avoid" procedures. Equipping fixed objects with lights and markings will enhance the "see and avoid" procedures.</p>			
<b>Scenario Set Sequential Number</b>	<b>Scenario Set Identification Number</b>	<b>Scenario Set Descriptions and Scenario Sub-set Descriptions</b>	<b>Total number of scenarios in the Set</b>
1	<b>AFXO-01</b>	Collision of subject aircraft with fixed object due to failure to identify fixed object. Fixed object not equipped with ADS-B.	7

2	<b>AFXO-02</b>	Collision of subject aircraft with fixed object due to failure of ADS-B on fixed object.	7
3	<b>AFXO-03</b>	Collision of subject aircraft with fixed object due to failure of ADS-B on aircraft.  Fixed object is equipped with ADS-B.	7
<p><b>AFLO Aircraft – Flying Object</b></p> <p>Three sub-scenarios are analyzed. In all three scenarios, the worst case event is a collision of an ADS-B equipped aircraft with another flying object, such as launch vehicles, hot air balloons, ultralights, etc). The cause of the collision is either because the flying object is not equipped with ADS-B, or it is equipped but ADS-B has failed, or because ADS-B has failed on the subject aircraft. The operational environments include Oceanic, EnRoute, and Terminal domains.</p> <p>The controls identified in 6.1.1 are applicable to this scenario. Additionally, an alternate means of detecting flying objects, such as TCAS, or ATC warnings is required to reduce the risks associated with this scenario.</p>			
4	<b>AFLO-01</b>	Collision of subject aircraft with flying object due to failure to identify flying object. Flying object not equipped with ADS-B.	7
5	<b>AFLO-02</b>	Collision of subject aircraft with flying object due to failure of ADS-B on flying object.	7
6	<b>AFLO-03</b>	Collision of subject aircraft with flying object due to failure of ADS-B on subject aircraft.	6
<p><b>AGV Aircraft – Ground Vehicles</b></p> <p>Three sub-scenarios are analyzed. In all three scenarios, the worst case event is a collision of an ADS-B equipped aircraft with a ground vehicle. The cause of the collision is because the ground vehicle is not equipped with ADS-B, or it is equipped and has failed, or because the ADS-B on the subject aircraft has failed. The operational environment is the airport surface. Dense fog during darkness poses the worst case if the subject aircraft is relying on ADS-B only for surveillance.</p> <p>Controls identified for these hazards are similar to those previously identified, however, in this case an alternate means of detecting the aircraft and informing the ground vehicle operator is required, e.g., AMASS.</p>			
7	<b>AGV-01</b>	Collision of subject aircraft with ground vehicle due to failure to identify ground vehicle. Ground vehicle not equipped with ADS-B.	6
8	<b>AGV-02</b>	Collision of subject aircraft with ground vehicles due to failure of ADS-B on ground vehicles.	7
9	<b>AGV-03</b>	Collision of subject aircraft with ground vehicles due to failure of ADS-B on own aircraft	7
<p><b>AOAA Aircraft – Other Airborne Aircraft</b></p> <p>These sub- scenarios are a special case of 6.1.2 where the flying object is another airborne aircraft. The three inadvertent collision cases are due to failure of ADS-B on either aircraft, or because the other airborne aircraft is not equipped with ADS-B. Worst case is in severe meteorological conditions where there is reliance on ADS-B only for surveillance input.</p> <p>Control for these hazards require an alternate means of detecting the other airborne aircraft, such as TCAS, or ATC warnings based on surveillance radar.</p>			
10	<b>AOAA-01</b>	Collision of subject aircraft with other airborne aircraft due to failure to identify other airborne aircraft, via ADS-B. Other airborne aircraft not equipped with ADS-B.	6
11	<b>AOAA-02</b>	Collision of subject aircraft with other airborne aircraft due to failure of ADS-B on other airborne aircraft	6

<b>ANAA Aircraft – Non-Airborne Aircraft</b>			
This is a scenario similar to 6.1.3 AGV, where the surface vehicle is another aircraft. It is of significance because of the frequency and severity of runway incursion accidents. In this scenario, either ADS-B has failed on the subject aircraft, the other non-airborne aircraft, or the other aircraft lacks ADS-B equipage. During the transition to full equipage of all commercial and GA aircraft, this is a credible accident scenario. The worst case involves weather and darkness combinations that inhibit “see and avoid” procedures on the airport surface.			
<b>Control of these hazards requires an alternate means of detecting the non-airborne aircraft and informing the flight crews of its position.</b>			
12	<b>ANAA-01</b>	Collision of subject aircraft with non-airborne aircraft due to failure to identify non-airborne aircraft. Other aircraft not equipped with ADS-B.	7
13	<b>ANAA-02</b>	Collision of subject aircraft with non-airborne aircraft due to failure of ADS-B on non-airborne aircraft	7
14	<b>ANAA-03</b>	Collision of subject aircraft with non-airborne aircraft due to failure of ADS-B on subject aircraft.	6
<b>AADF Aircraft – Aircraft, Display Failure</b>			
In this scenario, there are four failures that cause the inadvertent collision:			
<ul style="list-style-type: none"> <li>• Erroneous position data transmitted by the subject aircraft</li> <li>• Erroneous position data transmitted by the other aircraft</li> <li>• Failure of the subject aircraft’s cockpit display</li> <li>• Failure of the other aircraft’s cockpit display</li> </ul>			
All four failures occur in worst case weather/darkness conditions where ADS-B is the only source of surveillance data.			
Two controls are of particular significance in controlling these hazards: Design ADS-B to detect and report malfunctions/erroneous data, and provide an alternate means of detecting aircraft position. Contingency procedures should also be exercised to reduce these risks.			
15	<b>AADF-01</b>	Collision of subject aircraft with other aircraft due to erroneous position information on subject aircraft cockpit display. Other aircraft transmits erroneous position information.	6
16	<b>AADF-02</b>	Collision of subject aircraft with other aircraft due to erroneous position information on subject aircraft cockpit display. Subject aircraft displays erroneous position information. Source of erroneous information on display is due to failure of on-board display.	7
17	<b>AADF-03</b>	Collision of other aircraft with subject aircraft due to erroneous position information on other aircraft cockpit display. Subject aircraft transmits erroneous position information.	7
18	<b>AADF-04</b>	Collision of other aircraft with subject aircraft due to erroneous position information on other aircraft cockpit display. Other aircraft displays erroneous position information. Source of erroneous information on display is due to failure of on-board display.	6
<b>AGDF Aircraft – Ground Vehicle, Display Failure</b>			
There are only two variations on this scenario. First is that the Ground Vehicle is transmitting erroneous position information. Second is that the subject aircraft cockpit display fails. Again, worst case visibility conditions with ADS-B as sole surveillance input.			
As indicated in AGV above, the most significant control identified is to have an alternate means of detecting the ground vehicle and informing the aircraft crew.			
19	<b>AGDF-01</b>	Collision of subject aircraft with ground vehicle due to erroneous position information on subject aircraft cockpit display. Ground vehicle transmits erroneous position information.	6
20	<b>AGDF-02</b>	Collision of subject aircraft with ground vehicle due to erroneous position information on subject aircraft cockpit display. Subject aircraft displays erroneous position information. Source of erroneous information on display is due to failure of on-board display.	6

<p><b>SSDF Surface Aircraft – Surface Aircraft, Display Failure</b></p> <p>This special case of runway incursion or airport surface collision on taxiways. There are four possible causes analyzed:</p> <ul style="list-style-type: none"> <li>• Erroneous position data transmitted by other surface aircraft</li> <li>• Erroneous position data transmitted by the subject aircraft</li> <li>• Failure of subject aircraft’s display</li> <li>• Failure of other aircraft’s display</li> </ul> <p>Controls are similar to the Aircraft to Aircraft Display failure case above. The two controls that are of particular significance in controlling these risks are (1). Design ADS-B to detect and report malfunctions/erroneous data, and (2) provide an alternate means of detecting aircraft position. Contingency procedures should also be exercised to reduce these risks.</p>			
21	<b>SSDF-01</b>	Collision of subject surface aircraft with other surface aircraft due to erroneous position information on subject aircraft cockpit display. Other surface aircraft transmits erroneous position information.	7
22	<b>SSDF-02</b>	Collision of subject surface aircraft with other surface aircraft due to erroneous position information on subject aircraft cockpit display. Subject aircraft displays erroneous position information. Source of erroneous information on display is due to failure of on-board display.	7
23	<b>SSDF-03</b>	Collision of other surface aircraft with subject surface aircraft due to erroneous position information on other surface aircraft’s display due to failure of other surface aircraft’s display.	7
24	<b>SSDF-04</b>	Collision of other surface aircraft with subject aircraft due to erroneous position information on other surface aircraft display. Source of erroneous information on other surface aircraft display is due to erroneous position data from subject aircraft.	7
<p><b>AFOD Aircraft – Fixed Object, Display</b></p> <p>Display failure occurs either due to ADS-B transmitting erroneous position information, or the on-board CDTI fails.</p> <p>Controls: Design ADS-B to assure that failures/malfunctions are detected and reported to automatically to affected aircrew.</p>			
25	<b>AFOD-01</b>	Collision of subject aircraft with fixed object due to display failure on subject aircraft.	7
26	<b>AFOD-02</b>	Collision of subject aircraft with fixed object due to erroneous position information on subject aircraft’s display due to fixed object transmitting erroneous position data.	7
<p><b>AAAL Aircraft – Aircraft, Approach and Landing</b></p> <p>This scenario involves the loss of separation assurance during terminal approach due to ADS-B failure. One application that is of particular importance is simultaneous approaches to parallel runways. The worst case assumes reliance on ADS-B-only for surveillance input, and worst case visibility conditions.</p> <p>Controls for these risks require high availability of ADS-B and an alternate means of obtaining surveillance data due to the time-criticality of two aircraft in this situation. High availability of the ADS-B system is vital to minimize the risk associated with this scenario. Should the ADS-B system fail in this application, increased risk of loss of separation can occur. Also, ATC contingency procedures must be applied in the event that ADS-B fails. In addition, ATC and air crew training in contingency procedures is vital in reducing these risks.</p>			
27	<b>AAAL-01</b>	Loss of separation assurance and collision during terminal approach due to ADS-B failure. (No other surveillance information available, i.e., no backup)	7
<p><b>SR Security Related</b></p> <p>Loss of separation during terminal approach due to intentional “jamming” of the ADS-B signal, or “spoofing” in which hackers breach system security.</p> <p>The design of the ADS-B system requires physical and electronic security protection means such as intrusion detection, intrusion protection, e.g., message authority verification, and other mitigation to assure that intentional threats have been controlled.</p>			

28	<b>SR-01</b>	Loss of separation assurance and collision during terminal approach due to intentional security intrusion, i.e., intentional “jamming” of ADS-B signal.	7
29	<b>SR-02</b>	Loss of separation assurance and collision due to “spoofing”, i.e., hackers breach system security.	7
<p><b>HF Human Factors</b></p> <p>Five sub-scenarios were analyzed that might result in increased collision risk. These are;</p> <ul style="list-style-type: none"> <li>Excessive controller workload resulting in loss of situational awareness due too excessive displays clutter.</li> <li>Excessive pilot workload resulting in loss of situational awareness due to excessive display clutter, i.e., too much information on the CDTI.</li> <li>Inappropriate or erroneous communication due to language barrier</li> <li>Loss of separation assurance due to erroneous “future intent” messages, due to pilot error</li> <li>Inadequate Computer Human Interface design causes inappropriate or erroneous communication.</li> </ul> <p>There are specific controls that affect Human Factors that are required.. They involve the following:</p> <ul style="list-style-type: none"> <li>The ADS design should accommodate international communications in accordance with acceptable human factors design practices and standardized ICAO agreements.</li> <li>Provide alternate means of communications, i.e., voice backup to minimize the potential for miscommunication.</li> </ul> <p>Potential loss of situational awareness can occur due to excessive aircrew and/or controller workload. Research effort is needed to understand and minimize the potential for loss of situational awareness.</p>			
30	<b>HF-01</b>	Possible increased collision risk due to excessive controller workload, loss of situation awareness associated with excessive display clutter.	7
31	<b>HF-02</b>	Increased collision risk due to pilot workload, loss of situation awareness associated with excessive display clutter, i.e., and too much information.	7
32	<b>HF-03</b>	Loss of separation assurance and collision due to erroneous “future intent” messages, due pilot input error.	6
33	<b>HF-04</b>	Inappropriate or erroneous communication due to language barrier results in loss of situational awareness and increased collision risk.	7
34	<b>HF-05</b>	Inappropriate or erroneous communication due to language barrier results in loss of situational awareness and increased collision risk between aircraft and ground vehicle.	6
35	<b>HF-06</b>	Inappropriate or erroneous communication due to less than adequate CHI design results in loss of situational awareness and increased collision risk between aircraft.	7
36	<b>HF.07</b>	Inappropriate or erroneous communication due to less than adequate CHI design results in loss of situational awareness and increased collision risk between aircraft and ground vehicle.	7
<p><b>SA System Anomalies</b></p> <p>There are 28 system anomalies that were analyzed for their impact on safety of ATC operations using ADS-B only as the surveillance input. They cover a wide variety of possible causes that range from errors in one or more parts of the state vector transmission, e.g., latitude, longitude, heading, etc. to saturation of the frequency spectrum being used for transmission.</p> <p>The most appropriate controls to minimize the potential for system anomalies involve:</p> <ul style="list-style-type: none"> <li>The system shall be designed to insure that no single failure, common mode failure, human error, or design feature can cause a catastrophic event.</li> <li>The system shall be designed to ensure that dual independent component failure, dual human errors, or a combination of a component failure and human error cannot cause a catastrophic event.</li> <li>The system should be designed to assure that no single software anomaly, common software malfunction, or design feature shall result in a catastrophic event.</li> </ul> <p>There are a number of other controls required which address specific anomaly scenarios that are listed in Appendix A</p>			
37	<b>SA-01</b>	Inappropriate clearance given as a result of erroneous flight data in Data Block, i.e., ACID, ALTITUDE, POSITION, HEADING, etc caused by loss of data integrity.  Scenario results in collision.	7

38	<b>SA-02</b>	Loss of separation assurance and collision during terminal approach due to frequency saturation i.e., is their sufficient bandwidth to accommodate all aircraft in a terminal environment?	7
39	<b>SA-03</b>	Loss of separation assurance and collision due to insufficient range of ADS-B on approaching aircraft.	7
40	<b>SA-04</b>	Possible increased collision risk due to ADS-B system calibration deviation.  Scenario addresses many aircraft.	6
41	<b>SA-05</b>	Common Mode failures in ADS-B that could result in loss of separation assurance and collision.	7
42	<b>SA-06</b>	Loss of separation and collision due to common software anomaly.	7
43	<b>SA-07</b>	Common cause failure in ADS-B results in loss of transmission and consequent collision.	7
44	<b>SA-08</b>	Loss of separation integrity due to delay in transmitting data results in collision.	7
45	<b>SA-09</b>	Possible increased collision risk due to ADS-B system calibration error.	7
46	<b>SA-10</b>	ADS-B system malfunction occurs and the ground controller does not detect it.  Scenario results in collision.	7
47	<b>SA-11</b>	ADS-B system malfunction occurs and the pilot does not detect it.  Scenario results in collision.	7
48	<b>SA-12</b>	Erroneous malfunction indication to pilot.  Scenario results in collision.	7
49	<b>SA-13</b>	Erroneous malfunction indication to controller.  Scenario results in collision.	7
50	<b>SA-14</b>	Erroneous turn indication due to ADS-B system forecast error.  Scenario results in collision.  Aircraft initially not on collision course.	6
51	<b>SA-15</b>	Erroneous turn indication due to ADS-B system forecast error.  Scenario results in collision.  Aircraft initially on collision course.	7
52	<b>SA-16</b>	Erroneous turn indication due to ADS-B system malfunction.  Scenario results in collision.  Aircraft initially not on collision course.	7
53	<b>SA-17</b>	Erroneous turn indication due to ADS-B system malfunction.  Scenario results in collision.  Aircraft initially on collision course.	6
54	<b>SA-18</b>	Loss of separation assurance results in collision due to erroneous “future intent” messages, due to system malfunction.	7
55	<b>SA-19</b>	Display information conflict between ground displays and airborne displays due to ADS-B system malfunction results in collision.	7
56	<b>SA-20</b>	Erroneous position data (latitude-longitude) due to system malfunction resulting in loss of separation and collision.	7

57	<b>SA-21</b>	Erroneous position data (latitude-longitude) due to system malfunction resulting in loss of separation and collision.	6
58	<b>SA-22</b>	Data conflict between airspeed and velocity data results in erroneous data to be transmitted, (i.e., which one do you believe?), as a result of system malfunction. Scenario results in collision.	6
59	<b>SA-23</b>	Barometric Altitude Rate error causes loss of separation in terminal approach sequencing.  Scenario results in collision.	6
60	<b>SA-24</b>	Barometric Altitude Rate error on own aircraft causes false alarm on receiving aircraft.  Scenario results in collision.	7
61	<b>SA-25</b>	Barometric Altitude error on own aircraft causes false alarm on receiving aircraft.  Scenario results in collision.	7
62	<b>SA-26</b>	Position error on own aircraft causes false alarm on receiving aircraft.  Scenario results in collision.	7
63	<b>SA-27</b>	ADS-B malfunction caused by COTS or NDI results in system anomaly.  Scenario results in collision.	6
64	<b>SA-28</b>	Failure propagation results in loss of ADS-B.  Scenario results in collision.	9
65	<b>SA-29</b>	Failure propagation results in erroneous message indication.  Scenario results in collision.	6
66	<b>SA-30</b>  Also see SA-04.	Possible increased collision risk due to ADS-B system calibration deviation. Miscalibration is on single aircraft. Scenario results in collision.	7
<p><b>LTAD Less Than Adequate Design</b></p> <p>This scenario should properly be termed Latency Effects, because the three sub-scenarios all consider the effects of latency errors in processing the input data, the communication link, and the application processing. The result is a loss of data integrity due to excessive elapsed time between the data acquisition and data display on the airborne or ground displays</p> <p>In this case, the control is straightforward. Latency requirements for the transmitter, receiver and communications link are specified in NAS-SR-1000.</p>			
67	<b>LTAD-01</b>	Loss of data integrity due to delay in transmitting data due to LTA design.  Scenario addresses Transmitter Latency.  Scenario results in collision.	7
68	<b>LTAD-02</b>	Loss of data integrity due to communication link latency errors between the airborne and ground receiving/processing systems.  Scenario results in collision.	7
69	<b>LTAD-03</b>	Loss of separation due to time delay in ground processing system. (UPDATE RATE).  Scenario results in collision.	7

<b>EE Environmental Effects</b>			
Two sub-scenarios were analyzed related to environmental effects. The first one concerned weather effects on ADS-B that would cause “blind spots”. These effects may be unique to a given technology being considered. The second sub-scenario concerned effects of the natural environment, such as solar flares, Gamma Rays, and other electromagnetic anomalies.			
To minimize potential for adverse weather affecting communications, it is required that the appropriate frequency spectrum be selected, in that alternate frequency spectrum be made available as a redundancy. Ground stations should also be designed to minimize the effects of lightening or other adverse weather conditions.			
The ADS-B system should be hardened against electromagnetic interference.			
70	<b>EE-01</b>	Reduced safety margins due to weather effects on ADS-B which cause temporary “blind spots”.  Scenario results in collision.	7
71	<b>EE-02</b>	Loss of ADS-B Ground Station due to natural environmental effects such as solar flares, Gamma Rays, and/ or other related electromagnetic anomalies, such as EMI/EMC).	1
<b>LTAD-NS NAS Modernization Integrated System Hazards, Less Than Adequate Design</b>			
This scenario changes the earlier assumption that the operation was based on ADS-B ONLY. In this case, ADS-B is assumed to be integrated with other NAS Modernization automation systems. Two sub-scenarios were identified that could result in a collision. First was less-than-adequate human factors design integration of ADS-B with other NAS Modernization automation systems, such as CPDLC, FIS, TCAS, TIS, etc. The concern is that too much information in the cockpit, if it is not properly integrated, may cause confusion, or loss of situational awareness.			
The second concern was that redundant flight critical information could be conflicting. For example, if TCAS provides alarm information that is not consistent with information provided by ADS-B, the aircrew may become confused, or delay taking action to avoid a collision.			
Mitigation of the risk for these sub-scenarios involve research activities such as analysis and simulation, or flight tests with teams of pilots and controllers to determine acceptable limits on the display of information and acceptable ways to display the information in an integrated system, to avoid confusion, or information overload. The results of these studies can then be translated into design requirements.			
72	<b>LTAD-01 NS</b>	Less than adequate human factors design integration of NAS Modernization systems, i.e., ADS-B, CPDLC, FIS, etc. results in loss of situation awareness of flight crew and possible increased collision risk.	1
73	<b>LTAD-02 NS</b>	Due to less than adequate design, there is conflicting information communicated to the aircrew. This information addresses redundant flight critical information that is associated with an emergency. This can possibly lead to confusion, delayed response to the emergency situation and possible increased collision risk.	7
<b>SA-NS NAS Modernization Integrated System Hazards, System Anomaly</b>			
These two sub-scenarios are similar to 6.1.16 LTAD, except the cause of conflicting information to the cockpit or air traffic controller is a system anomaly as opposed to inadequate design. The result is the same, however, redundant, conflicting flight critical information that leads to the wrong response, or a delayed response.			
In this case, the design must eliminate the potential for system anomalies that would result in conflicting information. Adequate testing is also required to ensure that the design requirements have covered all known anomalies.			
74	<b>SA-01 NS</b>	Due to system anomaly, there is conflicting information communicated to the aircrew. This information addresses redundant flight critical information that is associated with an emergency. This can possibly lead to confusion, delayed response to the emergency situation and possible increased collision risk.	7

75	<b>SA-02 NS</b>	Due to system anomaly, there is conflicting information communicated to the air traffic controller. This information addresses redundant flight critical information that is associated with an emergency. This can possibly lead to confusion, delayed response to the emergency situation and possible increased collision risk.	7
<p><b>CP Contingency Planning</b></p> <p>Less than adequate contingency planning results in possible increased collision risk due to confusion over responsibility for separation assurance in a shared responsibility environment, e.g., Free Flight Phase One.</p> <p>These procedures must be worked out in simulations or preferably, flight tests to cover all contingency situations that can be identified.</p>			
76	<b>CP-01</b>	Less than adequate contingency planning results in possible increased collision risk due to confusion over responsibility for separation assurance in a shared responsibility environment.	7
<p><b>Basic Interactive Aircraft</b></p> <p><b>IS-A1, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – I, TIS</b></p> <p>CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.</p> <p>TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.</p> <p>TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
77	<b>IS-A1-01</b>	Collision of subject aircraft due to ADS-B malfunction and TCAS-I malfunction.	3
		TIS not helpful.	
78	<b>IS-A1-02</b>	Collision of subject aircraft due to ADS-B malfunction and conflicting information on CDTI, TCAS, or TIS.	3
79	<b>IS-A1-03</b>	Collision of subject aircraft due to malfunction of Conflict Avoidance.	3
<p><b>IS-A2, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – I</b></p> <p>CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.</p> <p>TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.</p>			
80	<b>IS-A2.01</b>	Collision of subject aircraft due to ADS-B malfunction and TCAS-I malfunction.	5
<p><b>IS-A3, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – II, TIS</b></p> <p>CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.</p> <p>TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.</p> <p>TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
81	<b>IS-A3.01</b>	Collision of subject aircraft due to ADS-B malfunction and TCAS-II malfunction, causing error in recommended vertical escape maneuver indication.	9
<p><b>IS-A4, Own Aircraft, ADS-B (Class A1), CDTI, TCAS – II</b></p> <p>CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.</p> <p>TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.</p>			
82	<b>IS-A4.01</b>	Collision of subject aircraft due to ADS-B malfunction and TCAS-II malfunction.	6

<b>Separation and Sequencing</b>			
<p><b>IS-B1, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – I, TIS</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.            TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
83	<b>IS-B1.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or TIS or CDTI malfunction contributes to loss of separation.	6
<p><b>IS-B2, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – I</b></p>			
84	<b>IS-B2.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or CDTI malfunction contributes to collision.	6
<p><b>IS-B3, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – II, TIS</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.            TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
85	<b>IS-B3.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or TIS or CDTI malfunction contributes to collision.	6
<p><b>IS-B4, Own Aircraft, ADS-B (Class A2), CDTI, TCAS – II</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.</p>			
86	<b>IS-B4.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or CDTI malfunction contributes to collision.	6
<p><b><u>Flight Path Deconfliction Planning</u></b></p>			
<p><b>IS-C1, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – I, TIS</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.            TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
87	<b>IS-C1.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or TIS or CDTI malfunction contributes to collision.	6
<p><b>IS-C2, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – I</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.</p>			
88	<b>IS-C2.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or CDTI malfunction contributes to collision.	6
<p><b>IS-C3, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – II, TIS</b>            CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.            TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.            TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			

89	<b>IS-C3.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or TIS or CDTI malfunction contributes to collision.	6
<b>IS-C4, Own Aircraft, ADS-B (Class A3), CDTI, TCAS – II</b> CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information. TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.			
90	<b>IS-C4.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or CDTI malfunction contributes to collision.	6
<b><u>Aircraft Broadcast Only</u></b> <b>IS-D1, Own Aircraft, ADS-B (Class B1), CDTI</b> CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information.			
91	<b>IS-D1.01</b>	Loss of ability of own aircraft to be seen by Class A and Class C users due to ADS-B malfunction on own aircraft. Scenario results in collision with vehicle.	6
<b>IS-D2, Own Aircraft, ADS-B (Class B1), MFD</b> MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.			
92	<b>IS-D2.01</b>	Loss of ability of own aircraft to be seen by Class A and Class C users due to ADS-B malfunction on own aircraft. Scenario results in collision with vehicle. MFD not helpful	6
<b>IS-D3, Own Aircraft, ADS-B (Class B1), CDTI, TIS</b> CDTI is a feature in the aircraft cockpit that will display automatic dependent surveillance broadcast (ADS-B) information. TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.			
93	<b>IS-D3.01</b>	Loss of ability of own aircraft to be seen by Class A and Class C users due to ADS-B malfunction on own aircraft. Scenario results in collision with vehicle if TIS is not useful.	6
<b>IS-D4, Own Aircraft, ADS-B (Class B1), MFD, TIS</b> MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.			
94	<b>IS-D4.01</b>	Loss of ability of own aircraft to be seen by Class A and Class C users due to ADS-B malfunction on own aircraft. Scenario results in collision with vehicle if TIS is not useful.	6
<b><u>Ground Receive Systems, EnRoute and Terminal</u></b> <b>IS-E1, ATS EnRoute and Terminal Area Operations, ADS-B (Class C1)</b>			
95	<b>IS-E1.01</b>	Degraded surveillance due to ADS-B malfunction on single aircraft.	9
<b><u>Ground Receive Systems, Parallel Runway and Surface Operation</u></b> <b>IS-F1, ATS Parallel Runway and Surface Operation, ADS-B (Class C2)</b>			
96	<b>IS-F1.01</b>	Collision occurs during parallel runway operations due to ADS-B malfunction. TCAS – I or II or TIS, not helpful.	10
<b><u>Ground Receive Systems, Flight Following</u></b> <b>IS-G1, Flight Following Surveillance, ADS-B (Class C3)</b>			

97	<b>IS-G1.01</b>	Loss of private user flight following surveillance due to ADS-B malfunction.	3
<p><b><u>Separation and Sequencing</u></b>  <b>IS-H1, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, TIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
98	<b>IS-H1.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-I or MFD or TIS malfunction contributes to collision.	9
<p><b>IS-H2, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.</p>			
99	<b>IS-H2.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-I or MFD malfunction contributes to collision.	9
<p><b>IS-H3, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II, TIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
100	<b>IS-H3.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-II or MFD or TIS malfunction contributes to collision.	9
<p><b>IS-H4, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.</p>			
101	<b>IS-H4.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-II or MFD malfunction contributes to collision.	9
<p><b>IS-H5, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, TIS, FIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.  FIS is currently a commercially available very high frequency (VHF) data link that provides weather and aeronautical information needed by pilots.</p>			

102	<b>IS-H5.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or MFD or TIS malfunction contributes to collision.	15
<p><b>IS-H6, Own Aircraft, ADS-B (Class A2), MFD, TCAS – I, FIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.  FIS is currently a commercially available very high frequency (VHF) data link that provides weather and aeronautical information needed by pilots.</p>			
103	<b>IS-H6.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or MFD malfunction contributes to collision.	15
<p><b>IS-H7, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II, TIS, FIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.  FIS is currently a commercially available very high frequency (VHF) data link that provides weather and aeronautical information needed by pilots.</p>			
104	<b>IS-H7.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or MFD or TIS malfunction contributes to collision.	15
<p><b>IS-H8, Own Aircraft, ADS-B (Class A2), MFD, TCAS – II, FIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.  FIS is currently a commercially available very high frequency (VHF) data link that provides weather and aeronautical information needed by pilots.</p>			
105	<b>IS-H8.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or MFD malfunction contributes to collision.	15
<p><b><u>Flight Path Deconfliction Planning</u></b>  <b>IS-II, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TIS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.</p>			
106	<b>IS-II.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-I or TIS or MFD malfunction contributes to collision.	9

<b>IS-I2, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I</b>			
MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats.			
107	<b>IS-I2.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-I or MFD malfunction contributes to collision.	6
<b>IS-I3, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TIS</b>			
MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions. TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.			
108	<b>IS-I3.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision. TCAS-II or TIS or MFD malfunction contributes to collision.	6
<b>IS-I4, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II</b>			
MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TCAS-II in addition to TCAS-I capabilities, provides recommended vertical maneuvers to the crew to avert potential near midair collisions.			
109	<b>IS-I4.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-II or MFD malfunction contributes to collision.	6
<b><u>Flight Path Deconfliction Planning and Terrain Awareness Warning System</u></b>			
<b>IS-J1, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TIS, TAWS</b>			
MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats. TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots. TAWS uses position data from a navigational system, like GPS, and a digital terrain database to display surrounding terrain.			
110	<b>IS-J1.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-I or TIS or MFD malfunction contributes to collision.	12
<b>IS-J2, Own Aircraft, ADS-B (Class A3), MFD, TCAS – I, TAWS</b>			
MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning. TCAS-I is a pilot warning indicator that displays proximate traffic and alerts the crew to other aircraft that may become potential near midair collision threats. TAWS uses position data from a navigational system, like GPS, and a digital terrain database to display surrounding terrain.			
111	<b>IS-J2.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.	12

		TCAS-I or MFD malfunction contributes to collision.	
<p><b>IS-J3, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TIS, TAWS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.  TIS is a Mode S Data Link service that delivers automatic traffic advisories to pilots.  TAWS uses position data from a navigational system, like GPS, and a digital terrain database to display surrounding terrain.</p>			
112	<b>IS-J3.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-II or TIS or MFD malfunction contributes to collision.	12
<p><b>IS-J4, Own Aircraft, ADS-B (Class A3), MFD, TCAS – II, TAWS</b>  MFD is a multi-function display that is a high-resolution color VGA, sunlight-readable display developed for general aviation applications. The display is capable of displaying ADS-B traffic, flight information service, moving map, terrain awareness information, and VFR/IFR charting functions. Some displays have internal GPS receivers to provide timing and positioning.  TCAS-II in addition to TCAS-I capabilities provides recommended vertical maneuvers to the crew to avert potential near midair collisions.  TAWS uses position data from a navigational system, like GPS, and a digital terrain database to display surrounding terrain.</p>			
113	<b>IS-J4.01</b>	Loss of separation assurance due to ADS-B malfunction results in collision.  TCAS-II or MFD malfunction contributes to collision.	12
<p><b>IL-IS, Integrated Systems - Integration Specific NAS/World-Wide Risks - Increased Risks</b>  Scenario events which cover a wide-ranging group of unlinked hazards.</p>			
114	<b>IL-IS.01</b>	Unidentified aircraft intruder enters ADS-B airspace and poses collision risk.	2
115	<b>IL-IS.02</b>	Incremental risks not adequately addressed presents increased risk of accident.	1
116	<b>IL-IS.03</b>	Mixed-equipage airspace presents confusion and loss of situational awareness to controllers.	2
117	<b>IL-IS.04</b>	LTA cross-checking of barometric altimetry with GPS (ADS-B) fails to identify deviation in altitude, which results in increased collision risk.	1
118	<b>IL-IS.05</b>	Unsuccessful conflict resolution between controllers and pilots results in increased collision risks.	1
119	<b>IL-IS.06</b>	LTA visual identification of other aircraft by subject aircraft pilots/aircrew results in inappropriate communication with ATCT and increased collision risks.	2
120	<b>IL-IS.07</b>	Accuracy delta between ADS-B and TIS-B presents difficulty in target identification and increased accident risk.	1
121	<b>IL-IS.08</b>	Inappropriate use of call sign or other language results in miscommunication and increased collision risks.	2
122	<b>IL-IS.09</b>	System inaccuracies between ADS-B and other subsystem results in inadvertent contact with wake vortex and increased accident risks.	1
123	<b>IL-IS.10</b>	Communication delay as a result of LTA mixed equipage procedural integration results in increased collision risks.	1
124	<b>IL-IS.11</b>	Conflicts between subsystems (ADS_B, TCAS, TAWS, TIS) state data results in inaccurate assumptions associated with separation and increased accident risks.	1
125	<b>IL-IS.12</b>	LTA integration of audible alerts issued by ADS-B, TCAS, TAWS, TIS, and results in confusion and increased collision risks.	2
126	<b>IL-IS.13</b>	Pilot/flight crew enhanced traffic awareness results in increased go-around or	1

		rejected takeoffs.	
127	<b>IL-IS.14</b>	Time from when a hazardous situation develops to the time the pilot takes corrective action is insufficient due to ADS-B malfunction, failure, or anomaly.	1
128	<b>IL-IS.15</b>	System (Integrated System) time source is unsynchronized resulting in inaccurate position, velocity and time.	1
129	<b>IL-IS.16</b>	Inadvertent access into SUA due to ADS-B malfunction, failure, or anomaly results in collision.	1
130	<b>IL-IS.17</b>	LTA training associated with ADS-B design, maintenance, or operation results in increased collision risk.	2
131	<b>IL-IS.18</b>	Collision with terrain or aircraft or fixed object or flying object, or vehicle during approach or landing or takeoff as a result of ADS-B malfunction, failure, or anomaly due to close proximity.	1
<p><b><u>Wide Area Augmentation System / Local Area Augmentation System/ FMS/ L1 Frequency</u></b>  <b>IS-K series</b>  WAAS enhances GPS signals to provide more precise location information to an accuracy of approximately 25 feet. WAAS is designed to use reference stations covering wide areas throughout the U.S. to cross check GPS signals and then relay integrity and correction information to aircraft via geostationary communication satellites. WAAS enhances availability by using these satellites to provide GPS-like navigation signal.  LAAS provides precise correction data to airborne and surface receivers that will result in navigation accuracy of less than 40 inches to distances of 20 miles or more from the airport.</p>			
132	<b>IS-K.01</b>	Interface malfunction between FMS and ADS-B results in loss of ADS-B. Event occurs during non-critical time.	2
133	<b>IS-K.02</b>	Degraded FMS input to ADS-B results in decreased accuracy. Event occurs during non-critical time.	2
134	<b>IS-K.03</b>	ADS-B malfunction propagates to FMS. Event occurs during non-critical time.	2
135	<b>IS-K.04</b>	Failure of FMS results in loss of ADS-B. Event occurs during non-critical time.	1
136	<b>IS-K.05</b>	ADS-B malfunction propagates to other aircraft systems, effecting WAAS. Event occurs during non-critical time.	4
137	<b>IS-K.06</b>	Loss of L1 frequency results in loss of: ADS-B, GPS, LAAS and WAAS. Event occurs during non-critical time.	2
138	<b>IS-K.07</b>	Interface malfunction between FMS and ADS-B results in loss of ADS-B. Event occurs during non-critical time.	3
139	<b>IS-K.08</b>	Degraded FMS input to ADS-B results in decreased accuracy. Event occurs during non-critical time.	2
140	<b>IS-K.09</b>	ADS-B malfunction propagates to FMS. Event occurs during non-critical time.	2
141	<b>IS-K.10</b>	Failure of FMS results in loss of ADS-B.	1

		Event occurs during non-critical time.	
142	<b>IS-K.11</b>	ADS-B malfunction propagates to other aircraft systems, effecting WAAS.	4
		Event occurs during non-critical time.	
143	<b>IS-K.12</b>	Loss of L1 frequency results in loss of:  ADS-B, GPS, LAAS and WAAS.	2
		Event occurs during non-critical time.	
<b><u>Integration Specific NAS/World-Wide Risks</u></b>			
<b>IS-L series</b>			
144	<b>IS-L.01</b>	Unidentified aircraft intruder enters ADS-B airspace and poses collision risk.	2
145	<b>IS-L.02</b>	Incremental risks not adequately addressed presents increased risk of accident.	1
146	<b>IS-L.03</b>	Mixed-equipage airspace presents confusion and loss of situational awareness to controllers.	2
147	<b>IS-L.04</b>	LTA cross-checking of barometric altimetry with GPS fails to identify deviation in altitude, which results in increased collision risk.	1
148	<b>IS-L.05</b>	Unsuccessful conflict resolution between controllers and pilots results in increased collision risks.	1
149	<b>IS-L.06</b>	LTA visual identification of other aircraft by subject aircraft pilots/aircrew results in inappropriate communication with ATCT and increased collision risks.	2
150	<b>IS-L.07</b>	Accuracy delta between ADS-B and TIS-B presents difficulty in target identification and increased accident risk.	1
151	<b>IS-L.08</b>	Inappropriate use of call sign or other language results in miss-communication and increased collision risks.	1
152	<b>IS-L.09</b>	Inappropriate use of new terminology or phraseology results in miss-communication and increased collision risk.	1
153	<b>IS-L.10</b>	System inaccuracies between ADS-B and other subsystem results in inadvertent contact with wake vortex and increased accident risks.	1
154	<b>IS-L.11</b>	Communication delay as a result of LTA mixed equipage procedural integration results in increased collision risks.	1
155	<b>IS-L.12</b>	Conflicts between subsystems (ADS-B, TCAS, TAWS, TIS) state data results in inaccurate assumptions associated with separation and increased accident risks.	1
156	<b>IS-L.13</b>	LTA integration of audible alerts issued by ADS-B, TCAS, TAWS, TIS, and results in confusion and increased collision risks.	1
157	<b>IS-L.14</b>	LTA integration of Airborne Conflict Management (ACM) results in increased collision risks.	1
158	<b>IS-L.15</b>	Pilot/flight crew increase in traffic awareness results in increased go-around or rejected takeoffs.	2
159	<b>IS-L.16</b>	Time from when a hazardous situation develops to the time the pilot takes corrective action is insufficient	1
160	<b>IS-L.17</b>	System (Integrated ADS-B System) time source is unsynchronized resulting in inaccurate position, velocity and time.	1
161	<b>IS-L.18</b>	Malfunction within Data Fusion processing results in undetected corruption of safety-critical information and increased collision risks.	1
162	<b>IS-L.19</b>	LTA integration of national and international separation standards increases collision risks associated with ADS-B use.	1
163	<b>IS-L.20</b>	LTA airspace transition integration results in increased collision risks.	1
164	<b>IS-L.21</b>	LTA ADS-B equipage or site coverage results in inadequate coverage and increased collision risks.	1

165	<b>IS-L.22</b>	LTA integration of ADS-B coverage areas results in “blind spots” and increased collision risks.	1
166	<b>IS-L.23</b>	Corruption of ADS-B message formats data results in increased collision risks.	1
167	<b>IS-L.24</b>	Loss of safety-critical information/communication to pilot/aircrew as a result of ADS-B malfunction increases accident risk associated with SUA or weather.	1

The below listed Precision Approach categories are only applicable to a few specific scenario sub-sets under the hazard scenarios contained in the above table. Precision approaches are categorized in terms of decision ceilings and minimum capabilities.

A Category (CAT) I approach provides accurate guidance information in visibility as low as one-half mile and a ceiling as low as 200 feet. A CAT II approach involves a runway visibility range of 1,200 feet and a decision height of 100 feet.

CAT III approaches are divided into three levels: CAT IIIa, IIIb, and IIIc. CAT IIIa requires visibility of 700 feet at a decision height as low as zero feet; CAT IIIb requires a runway visibility range of 150 feet at a decision height of zero feet; and CAT IIIc relies completely on instrumentation and has no ceiling or runway visibility range minima.

## **7.0 Preliminary Requirements Recommendations**

### **7.1 Candidate Safety Requirements**

The controls listed in Table 7-1 have been, in most cases, converted to a recommended “shall” statement that can be considered for inclusion in the Requirement Document. The controls were either taken from the IHA or created as new controls through the PHA process. In either case, additional controls were developed, combined, and/or expanded as necessary through the review process. It may be premature to put this level of detail in the IRD, however, the candidate requirements may be of significant benefit during the Investment Analysis process to evaluate potential solutions in arriving at a Final Requirements Document (FRD). Subsequently, they can be incorporated into the System Specification.

The Table is set up in a tabular format contain divided into six (6) columns. The first column (CR. No.) shows the sequential numeric listing of all Recommended Candidate Requirements. The sequential numeric listings start with the number one (1) and proceeds through number one hundred-sixteen (116). Only those rows, which contain functional Candidate Safety Requirements/Recommendations, are listed. Additional Controls and Recommended Safety Requirements/Recommendations are listed but were either combined into a higher-level “shall” statement or was captured in another functional Candidate Safety Requirements/Recommendations statement. Column two (2) (Con. No.) contains the original IHA and/or PHA control numbers. The control numbers are provided to facilitate a cross-reference from Table 7 to the original Hazard Scenario for which it was developed. Column three (3) contains the original Control language and assists in providing clarification for the language found in the associated Controls and Recommended Safety Requirements/Recommendations. Column four (4) contains the Candidate Requirements language presented in a “shall” statement, which is verifiable. The last columns, five (5) and six (6) allow identification of the Candidate Safety Requirements/Recommendations statements

as either “Existing” or “Recommended.” An Existing Requirement is one that can be traced to current FAA, other governmental, or consensus requirements documentation.

In total 141 controls are listed. Of these, 116 were formatted into Candidate Safety Requirements/Recommendations. A review of the Candidate Safety Requirements/Recommendations identified 43 as Existing and 73 as Recommended.

**Table 7-1: Summary of Existing and Recommended Candidate Requirements and Controls**

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
1	1	Develop ADS-B ATC/Aircrew procedures to accommodate transitional risks.	FAA shall develop ADS-B ATC and flightcrew procedures to accommodate transition from secondary surveillance radar domain to ADS-B surveillance domain.		X
2	1N	Require all fixed objects that are evaluated as hazardous to be equipped with ADS-B transmitters.	Fixed objects defined under 14 CFR Part 77 shall be equipped with ADS-B transmitter.	X	
3	2	Require all aircraft to be equipped with appropriate lighting to enhance “see and avoid” separation.	FAA [AVR] shall institute rulemaking to require improved aircraft lighting to enhance "see and avoid". Reference: Advisory Circular 90-48C		X
4	2a	Require all aircraft to be equipped with appropriate lighting to enhance “see and avoid” separation.	Aircraft shall be equipped with enhanced lighting to aid in “see and avoid” in accordance with 14 CFR, Parts 23, 25, 27, and 29.		X
3	2b	Aircrew “see and avoid” procedures.	FAA shall determine the need for developing enhanced see and avoid and lighting procedures for ADS-B operations. Reference: Advisory Circular 90-48C.		
5	2d	2d Require fixed objects to be equipped with appropriate lighting, i.e., “see and avoid”.	All fixed objects that can become hazards to flight navigation shall be required to be equipped with appropriate lighting to enhance "see and avoid" separation.		X
6	2N	Provide updated information on fixed objects in appropriate data sources.	Fixed object database shall conform to the requirements of RTCA/DO-200.	X	
4	3	Aircrew “see and avoid” procedures.	FAA shall determine the need for developing enhanced see and avoid and lighting procedures for ADS-B operations.		
7	3N	ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude.	ATCT shall use procedures in 7110.65 for validating aircraft ID, position, and altitude.	X	

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
8	4	Design ADS-B airborne system to automatically report system failure/malfunction to ATC and affected aircrews.	The ADS-B system shall automatically report detected system failure/malfunction (loss or corruption of critical data) to ATC and affected aircrews. (Need another requirement that specifies detection of TBD percentage of failures with a probability of error of TBD.,)		X
9	4a	Design ADS-B airborne system to assure that system failures/ malfunctions are detected and reported automatically-	ADS-B airborne equipment shall meet design assurance levels consistent with application in ARP 4754 or equivalent.	X	
10	4N	Design ADS-B external equipment for physical protection and security to minimize the potential for damage as a result of vandalism.	ADS-B external ground-based equipment shall be designed for physical protection and security in accordance with FAA Order 1600.46 (Physical Security Review of New Facilities, Offices Space and Operating Areas) to preclude damage as a result of vandalism.	X	
11	5a	The ADS-B system shall be designed to automatically report system failure/ malfunction to ATC and affected aircrews.	ADS-B airborne equipment shall meet design assurance for display of alarms and other flags as prescribed by Advisory Circular 25.1309-1BX or equivalent.	X	
12	5N	Avionics certification, installation, and approval process established for ADS-B.	FAA shall develop AC 20-XX to establish installation and operational approval criteria for ADS-B and ancillary equipment.		X
13	5Na	Avionics certification, installation, and approval process established for ADS-B with TIS.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and TIS-B for separation assurance services		X
14	5Nb	Avionics certification, installation, and approval process established for ADS-B with TCAS-I.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and TCAS-I for separation assurance and collision avoidance services		X
15	5Nc	Avionics certification, installation, and approval process established for ADS-B with CDTI.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and CDTI for separation assurance and collision avoidance services		X
16	5Nd	Avionics certification, installation, and approval process established for ADS-B with MFD.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and MFD for separation assurance services		X
17	5Ne	Avionics certification, installation, and approval process established for ADS-B with TCAS-II.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and TIS-B for separation assurance and collision avoidance services		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
18	5Nf	Avionics certification, installation, and approval process established for ADS-B with TAWS.	The FAA shall establish a process for certification of airborne and ground systems that use ADS-B and TAWS for separation assurance services		X
19	6	The failure/malfunction indication shall be designed to conform to FAA CT-96/1.	ADS-B equipment and systems shall meet requirements for failure/malfunction indications consistent with the application in 14 CFR parts 23, 25, 27, and 29 in reference to Advisory Circulars 23.1309-1C and 25.1309-1BX.	X	
20	6a	Design in accordance with FAA CT-96/1	Computer Human Interfaces with ADS-B shall meet requirements in FAA Visual Requirements for Ground Display Systems, Version 1.		X
21	6N	Require all flying objects that can become hazards to navigation be equipped with ADS-B transmitters, or other appropriate means of identification.	Controlled flight objects in the NAS) shall be equipped with and required to use ADS-B transmitters to provide means for positive identification to ensure separation and surveillance.		X
22	7	Provide for appropriate ATC/Aircrew contingency procedures in the event of ADS-B failure/malfunction.	FAA shall develop procedures for the operational use of ADS-B in accordance with the disciplines established in the ADS-B Operational Concepts, Addendums 3 and 3.1, August 16, 2001.		X
23	7N	All ground vehicles that can become hazards to ground navigation shall be required to be equipped with ADS-B transmitters, or other appropriate means of identification.	Ground vehicles that operate in airport surface movement areas shall be equipped with and required to use ADS-B transmitters as the means of identification and position reporting.		X
24	8	ADS-B shall be designed to assure that system failures/malfunctions are detected and reported automatically. Note: Original IHA stated: "Require fixed objects to be equipped with appropriate lighting, i.e., "see and avoid"."	ADS-B airborne equipment shall incorporate a hardware monitor to detect and alert failure condition to flight crew. (use same language as we used earlier)		X
25	8a	Design ADS-B airborne system to assure that system failures/malfunctions are detected and reported automatically.	The ADS-B system shall automatically report system failure/malfunction (loss or corruption of critical data) to ATC and affected aircrews. Same		X
8	8b	Design ADS-B to assure that system failures/malfunctions are detected and reported automatically.	The ADS-B system shall automatically report system failure/malfunction (loss or corruption of critical data) to ATC and affected aircrews. Same as above		

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
26	8N	Require alternate means of detecting ground vehicles, i.e. ASDE-X.	Alternate means shall be provided to detect the location, velocity and ID and track ground vehicles		X
27	9a	Require alternate means of detecting flying object, e.g., TCAS, ATC warning, etc.	Alternate means shall be provided to detect controlled flight vehicles		X
28	9b	Require alternate means of detecting other airborne aircraft, e.g., TCAS, ATC warning, etc.	An alternate means to detect and avoid collision with other airborne aircraft shall be provided,		X
29	9c	Require alternate means of detecting other aircraft, e.g., TCAS, ATC warning, etc.	An alternate means to detect and avoid collision with other aircraft shall be provided.		X
30	9N	Require certification, installation, and approval process established for ADS-B equipped ground vehicles.	FAA shall establish a process for installation, and certification of ADS-B equipped ground vehicles.		X
31	10	Require ground vehicles to be equipped with appropriate lighting and color indication to enhance "see and avoid" separation.	Ground vehicles shall be required to be equipped with lighting and color indication iaw TBD FARXXX to enhance "see and avoid" separation.		X
32	10N	Require all aircraft that can become hazards to navigation be equipped with ADS-B transmitters, or other appropriate automated means of identification.	Aircraft shall be equipped with ADS-B transmitters to provide means for positive identification to ensure separation and provide surveillance.		X
4	11	Aircrew and ground personnel "see and avoid" procedures.	FAA shall determine the need for developing enhanced see and avoid and lighting procedures for ADS-B operations.		
4	11a	Aircrew/ground operator "see and avoid" procedures.	FAA shall determine the need for developing enhanced see and avoid and lighting procedures for ADS-B operations.		
33	11N	Require certification, installation, and approval process established for ADS-B ground system.	The FAA shall establish a process for certification of the ADS-B ground system.		X
34	12a	System operational modes shall be clearly displayed to the operators in accordance with MIL Handbook - 760 and similar requirement FAA-G- 2100g.	System operational modes shall be clearly displayed to the operators in accordance with MIL Handbook - 760 and similar requirement FAA-G- 2100g.	X	
35	12b	Require alternate means of detecting aircraft and informing air crew of position, e.g., AMASS	FAA shall provide an alternate method to detect LOCATION VELOCITY, ID AND TRACK other airborne aircraft for flight crews and ATC		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
36	12c	Require alternate means of detecting aircraft and informing non-airborne aircraft crew of position, e.g., AMASS, ATC controllers.	FAA shall provide an alternate method to detect LOCATION VELOCITY, ID AND TRACK airborne/taxiing aircraft, ground vehicles, and fixed objects identified by FAA as navigational hazards, for taxiing aircraft flightcrews and ATC,		X
37	12d	Provide alternate means of identifying other aircraft/vehicle/fixed object.	FAA shall provide an alternate method to detect LOCATION VELOCITY, ID AND TRACK other airborne aircraft, taxiing aircraft, ground vehicles, and fixed objects identified by FAA as navigational hazards, for approaching and departing aircraft flightcrews and ATC		X
38	12N	System operational modes shall be clearly displayed to the operators in accordance with MIL Handbook - 760 and similar requirement FAA-G- 2100g.	ADS-B system operational display modes shall be clearly visible to ATC and labeled per SAE ARP-4289 for airborne equipment and in accordance with NAS SR-1000, paragraph 3.8.4.C.1, for ground equipment.	X	
	13N	Design display symbology and coding to minimize the potential for confusion, HMI, and to enhance situational awareness.			
39	14	Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failures, system anomalies, and malfunctions.	The ADS-B system shall comply with reliability and availability requirements for risk of failures, system anomalies, and malfunctions and critical, essential, and routine services per NAS – SR-1000, Paragraph 3.8.1.b, c, d., and e.	X	
40	14N	Conduct human factor analyses, evaluations, and/or simulations to identify safety-related risks associated with the integration of ADS-B system into the NAS.	ADS-B airborne equipment shall be designed to meet applicable requirements of HRR-510 and General Aviation Development and Assessment of Cockpit Display Innovations.	X	
41	15N	Assure that controller/pilot training and procedures are in place for ADS-B, to minimize human error and increase situational awareness.	FAA shall develop controller/pilot training and procedures for ADS-B applications.		X
42	15Na	Assure that controller/pilot training and procedures are in place for ADS-B, to minimize human error and inappropriate use of new terminology or phraseology.	FAA shall develop controller/pilot training and procedures for ADS-B applications that include common phraseology.		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
43	16N	Define criteria for determining threshold values for ADS-B coverage area to assure controller/pilot adequate situational awareness.	FAA shall define criteria for determining threshold values for ADS-B coverage area to ensure controller/pilot adequate situational awareness.		X
44	17N	Conduct controller/pilot workload assessments to evaluate the potential for excessive workload associated with ADS-B system.	FAA shall conduct controller/pilot assessments to benchmark acceptable workload criteria associated with ADS-B system introduction, integration, and operation in accordance with Appendix D, RTCA/DO-242, and HRR-150.		X
45	17Na	Conduct controller/pilot workload assessments to evaluate the potential for informational overload associated with ADS-B and related subsystems MFD or CDTI, TAWS, TCAS, and TIS.	Controller/pilot workload criteria associated with ADS-B and legacy systems combinations shall be developed to ensure safe workload operations are not exceeded. Note: Subsystems include MFD or CDTI, TAWS, TCAS, and TIS.  Human factors related simulations shall be conducted to assure flightcrew compatibility and interoperability using ADS-B with CPDLC, FIS, FMS, etc.		X
46	18N	Design Software in accordance with Advisory Circular 20-115B.	Airborne software included as part of the equipment shall be developed in compliance with the appropriate software level as defined in RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification. Ground station software shall meet requirements of NAS SR-1000, paragraph 3.7.1.	X	
47	19	Allocate appropriate bandwidth to accommodate current and projected traffic growth.	FAA shall ensure adequate spectral bandwidth to accommodate current and projected traffic growth. Get APO-120 reference		X
48	19N	Design TIS to integrate with ADS-B and provide redundant alert against collision risk.	FAA shall ensure ADS-B system information, as displayed in the cockpit be compatible and integrated with TIS. Note: Integrated system shall provide redundant alert against collision risk.		X
49	19Na	Design TCAS-I to integrate with ADS-B and provide redundant alert against collision risk.	FAA shall revise TSO-C118 and RTCA/DO-197 to include TCAS I integration with ADS-B airborne equipment for coherent alert functionality for redundancy in collision detection and alerting.		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
50	19Nb	Design TCAS-II to integrate with ADS-B and provide redundant alert against collision risk.	FAA shall revise TSO-C119b and RTCA/DO-185A to ensure that TCAS II integrates into ADS-B airborne equipment for coherent alert functionality.		X
51	19Nc	19Nc Design TAWS to integrate with ADS-B and provide redundant alert against collision risk.	FAA shall revise TSO-C151a to ensure that TCAS II integrates into ADS-B airborne equipment for coherent alert functionality.		X
52	20	Select transmission frequencies with enough bandwidth to accommodate the allocation.	FAA shall assign datalink frequencies for ADS-B to ensure sufficient spectral bandwidth to accommodate all functionality, availability, and integrity for both ground and airborne applications.		X
49 50 51 52	20N	Design CDTI, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize conflicting information communicated in cockpit.			
49 50 51 52	20Na	Design CDTI to integrate with ADS-B, provide redundancy, and minimize conflicting information communicated in cockpit.	Design CDTI to integrate with ADS-B, provide redundancy, and control conflicting information communicated in cockpit in accordance with TBD (Jerry Anderson has action to identify source.)		
49 50 51 52	20Nb	Design MFD to integrate with ADS-B, provides redundancy, and minimizes conflictive information communicated in cockpit.	Design MFD to integrate with ADS-B, provides redundancy, and minimizes conflictive information communicated in cockpit. Same as 20NA		
53	21	Alternate means of separation assurance must be provided.	FAA shall provide alternate means of separation assurance when ADS-B is employed.		X
54	21N	Provide updated information on fixed objects in appropriate data sources.	FAA shall provide reliable updated information on permanent fixed objects in appropriate data sources, such as moving map databases and sectional maps.		
55	21Na	Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of failure of, or error in, recommended vertical escape maneuver indication.	FAA shall ensure that system reliability and availability requirements are established to minimize the risk of failure of, or error in, recommended vertical escape maneuver indication in accordance with NAS SR-1000. Section 3.	X	
56	21Nb	Apply appropriate system reliability and availability requirements (TBD) to minimize the risk of erroneous sequencing of aircraft.	FAA shall ensure that system reliability and availability requirements are established to minimize the risk of erroneous sequencing of aircraft in accordance with NAS SR-1000. Section 3.	X	

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
57	22a	Require periodic recalibration of ADS-B inputs, processing system and displays.	ADS-B inputs, processing system and displays shall be required to execute periodic accuracy checks.		X
58	22b	Require periodic recalibration of all airborne ADS-B systems.	All airborne ADS-B systems shall be required to execute periodic accuracy checks.		X
59	22N	Design system to minimize the potential for failure of Conflict Avoidance function.	ADS-B system shall be designed to ensure Conflict Avoidance. Need requirements for accuracy, integrity and continuity per NAS SR-1000. Section 3		X
55	22Na	Design system to minimize the potential for failure of, or error in, recommended vertical escape maneuver indication.	FAA shall ensure that system reliability and availability requirements are established to minimize the risk of failure of, or error in, recommended vertical escape maneuver indication in accordance with NAS SR-1000. Section 3		X
56	22Nb	Design system to minimize the potential of erroneous sequencing of aircraft.	FAA shall ensure that system reliability and availability requirements are established to minimize the risk of erroneous sequencing of aircraft in accordance with NAS SR-1000. Section 3.	X	
60	22Nc	Design system to minimize the potential of erroneous flight path.	The system shall be designed to ensure flight path accuracy.		X
61	22Nd	Design system to minimize the potential for interface malfunction between FMS and ADS-B	ADS-B system shall interface with FMS when available.		X
62	22Ne	Design system to minimize the potential for degraded FMS input to ADS-B	Design system to ensure accurate FMS WHEN input to ADS-B		X
63	22Nf	Design system to minimize the potential for visual identification of wrong aircraft by pilot/aircrew.	Design system to ensure visual identification accuracy of referenced aircraft by ATC and dependent pilot/aircrew.		X
64	23	Consider automated system for recalibration of ADS-B systems.	An automated system for recalibration of ADS-B systems shall be considered.		X
65	23N	Design system to minimize the potential of loss of targets.	ADS-B system shall ensure that potential loss of targets be less than $1E \times 10^{-9}$ It shall be shown that the likelihood of catastrophic mishaps due to ADS-B failures/malfunctions is less than $1E \times 10^{-9}$		X
66	24	Provide a design requirement for system-wide calibration of ADS-B.	A design requirement for system-wide calibration of ADS-B shall be provided.		X
67	24N	Design system to minimize the potential of malfunction within sensor fusion system or interface.	The system shall be designed to preclude malfunction within sensor fusion system or interface.		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
68	25	Provide built-in test capability in the system to identify and report when the system is out of calibration.	A built-in test capability in the system to identify and report when the system is out of calibration shall be provided.		X
69	25N	Design system to minimize the potential of loss of flight following surveillance.	The system shall be designed to ensure flight following surveillance. Put requirements for integrity accuracy and continuity		X
70	26	Design the system such that no single failure, common mode failure, human error or design feature shall result in a catastrophic event, (severity 1 or 2).	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2		X
71	26N	ADS-B displays shall meet the requirements of applicable Minimum Operational Performance Standards (MOPS) for minimizing clutter and other display congestion.	ADS-B displays shall meet the requirements of applicable Minimum Operational Performance Standards (MOPS). Note: This minimizes clutter and other display congestion.	X	
72	27	Design system to minimize the potential of excessive display congestion as a result of FIS integration with ADS-B and cockpit displays.	ADS-B and FIS display integration shall meet the requirements of applicable Minimum Operational Performance Standards (MOPS). Note: This eliminates or controls visual confusion.	X	
73	27N	Design MFD, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize conflicting information communicated in cockpit.	ADS-B system integration with MFD, CDTI, TAWS, TCAS, and TIS shall meet requirements of 14 CFR Sections 23, 25, 27, 29.1309 for airborne applications. The ADS-B ground system shall meet the requirements for surveillance under NAS SR-1000. Note: Systems integration must provide redundancy and eliminate or control	X	
74	28	Provide for appropriate latency budget for ADS-B system.	ADS-B system shall meet or exceed surveillance services requirement specified in NAS SR-1000.	X	
75	28a	ADS-B system shall meet or exceed traffic display requirement specified in NAS SR-1000.	ADS-B system shall meet or exceed traffic display requirement specified in NAS SR-1000.	X	

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
76	28N	Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize conflictive information communicated in cockpit.	ADS-B system integration with MFD, CDTI, TAWS, TCAS, and TIS shall meet requirements of 14 CFR Sections 23, 25, 27, 29.1309 for airborne applications. The ADS-B ground system shall meet the requirements for surveillance under NAS SR-1000 Section 3. Note: Systems integration must provide redundancy and eliminate or control conflicting information.	X	
77	28Na	Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, maximize system alert capability, and minimize alert delay or malfunction.	The airborne and ground displays of ADS-B information shall be compatible with TCAS.		X
78	28Nb	Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, maximize system alert capability, and minimize alert delay or masking of alert.	The ADS-B system information output shall provide integration and compatible with, and redundancy for TCAS, TIS, TAWS and display systems and equipment.		X
79	28Nc	Design MFD or CDTI, TAWS, and TCAS to integrate with ADS-B, provide redundancy, and minimize conflictive information communicated in cockpit.	MFD or CDTI, TAWS, TCAS, and TIS shall integrate ADS-B data to provide display of traffic alert at least equal to ATC alerting functional requirements specified in NAS SR-1000, paragraph 3.2.5.C.	X	
80	28Nd	28Nd Design MFD or CDTI, TAWS, and TCAS to integrate with ADS-B, provide redundancy, maximize system alert capability, and minimize alert delay or masking of alert.	MFD or CDTI, TAWS, TCAS, and TIS shall integrate ADS-B data to provide display of traffic alert at least equal to ATC alerting functional requirements specified in NAS SR-1000, paragraph 3.2.5.C.		
81	29	Design the system to assure that potential for delay is minimized.	Display of ADS-B data shall meet the requirements of CDTI MOPS Version 25-V2.	X	
82	29N	Ensure terrain/airfield map accuracy, associated with ADS-B, i.e. fixed object location, data base integrity, runway hold short lines, construction, helipads, etc.	ADS-B shall use, where applicable, the digital terrain data files developed and certificated to DTED requirements established by NIMA, e.g. fixed object location, terrain integrity, towers, construction.	X	
83	29Na	ADS-B shall use geodetic data developed under NOS standards and disseminated through NFDC meeting requirements of RTCA/DO-200.	ADS-B shall use, where applicable, geodetic data developed under NOS standards and disseminated through NFDC meeting requirements of RTCA/DO-200.	X	

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
84	30	Design the system to monitor time delays and eliminate bad data.	ADS-B shall meet or exceed data latency requirements for the navigation uncertainty category (NUC) as specified within RTCA/DO-242 (reference R3.16 in Section 4.0).	X	
85	30N	Establish database update revision cycle requirements for ADS-B, including changes between revision cycles, and annunciation to pilot if outdated.	FAA shall establish a database to update revision cycle requirements for ADS-B, including changes between revision cycles, and annunciation to pilot.		X
86	31	Provide design to identify latency delays and indicate those anomaly.	The ADS-B system shall inform operators when target data latency has exceeded TBD.		X
87	31	Provide design to identify latency delays and indicate those anomaly.	FAA shall conduct an analysis to determine target data latency requirements.		X
88	32	Provide alternate means of providing functionality.	An alternate means (to ADS-B) of providing functionality shall be provided.		
89	33a	Design the system to minimize false alarms.	ADS-B shall meet or exceed false alarm limits requirements specified within the flight scenarios described within RTCA/DO-242, Appendix J.	X	
89	33b	Design the system to minimize the potential for false alarms.	ADS-B shall meet or exceed false alarm limits requirements specified within the flight scenarios described within RTCA/DO-242, Appendix J.		
90	34	Design forecasting algorithms with sufficient margins of safety.	ADS-B conflict detection functions shall meet the requirements of RTCA/DO-242.	X	
91	34a		ADS-B transmissions shall indicate the ability of the transmitting participant to engage in path monitoring and de-confliction operations (reference R2.31 in Section 4.0).		X
91	34N	Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize the potential for miscommunication.	ADS-B transmissions shall indicate the ability of the transmitting participant to engage in path monitoring and de-confliction operations (reference R2.31 in Section 4.0).		
91	34Na	Design MFD or CDTI, TAWS, TCAS, and TIS to integrate with ADS-B, provide redundancy, and minimize the potential for LTA communication.	ADS-B transmissions shall indicate the ability of the transmitting participant to engage in path monitoring and de-confliction operations (reference R2.31 in Section 4.0).		

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
92	35	Design the system to minimize the potential for conflict between the ground displays and airborne displays.	ADS-B display data shall be presented to operators in a manner to assure accuracy and integrity of the target information at least equal to data displayed to ATC controller in accordance with NAS SR-1000, Section 3 for ground systems and 14 CFR Sections 23, 25, 27, 29.1309 for airborne applications.		
93	36	Design the system to detect and report conflicts in information between ground and airborne displays.	ADS-B data shall be displayed to the flightcrew in a manner to assure accuracy and integrity of the target information at least equal to data displayed to ATC controller in accordance with NAS SR-1000 Section 3.		
94	37	Require independent method of validating position data.	A source of geodetic position and altitude shall be provided to ADS-B to meet requirements of RTCA/DO-242 paragraph 3.5.2.1.2.	X	
95	38	An alternate means of velocity data shall be provided to ADS-B shall be provided.	An independent method (from ADS-B) of validating velocity data shall be required.		X
96	39	Design the system to minimize the potential for conflict between airspeed and velocity data.	ADS-B system shall provide display and alarms of impending collision to meet requirements of RTCA/DO-242 as referenced within Appendices D and J.	X	
97	40	Design the system to detect and indicate a discrepancy between airspeed and calculated velocity.	ADS-B system shall ensure displayed aircraft airspeed availability, integrity, and reliability, with discrepancy indication function		X
98	40a		ADS-B system shall ensure indicated airspeed data is accurately processed and displayed.		X
99	41	Design system to detect and indicate erroneous barometric altitude rate errors before transmitting through ADS-B.	ADS-B system shall verify accurate barometric altitude broadcast data.		X
100	42	Provide independent means of validating Barometric altitude rate changes.	ADS-B system shall verify accurate barometric altitude rate change broadcast data.		X
101	43	Provide contingency training to assure situational awareness and acclimation of ADS-B during terminal phase descent.	Training shall be provided to controllers and pilots for contingency procedures to assure situational awareness while using ADS-B during all flight phases.		X
102	46	Provide alternate means of collision avoidance such as TCAS or MSAW.	An alternate means (to ADS-B) of collision avoidance such as TCAS, or MSAW shall be provided.		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
103	47	ADS-B system architecture to ensure failure isolation of COTS and NDI hardware, firmware, and software.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2	X	
103	48a	Design ADS-B system architecture to ensure that COTS and NDI hardware, firmware and software fails safe.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2		
103	48b	48b Design ADS-B system architecture to ensure that hardware, firmware and software fails safe.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2		
103	49	49 Provide COTS and NDI hardware, firmware, and software discriminators TBD.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2		
103	50	50 Design ADS-B system architecture to ensure failure isolation of hardware.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2		
103	52	The ADS-B system architecture shall be designed to ensure failure isolation of hardware, firmware, and software.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2	X	

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
104	54	Design Transmitter/Receiver to meet Latency Requirements of NAS-SR-1000.	ADS-B system shall meet or exceed latency requirements as specified within RTCA/DO-242 (reference R3.16 in Section 4.0).	X	
104	55	Design Communication link to meet latency Requirements of NAS-SR-1000..	ADS-B system shall meet or exceed latency requirements as specified within RTCA/DO-242 (reference R3.16 in Section 4.0).	X	
104	56	Design application-processing system to meet Latency Requirements of NAS-SR –1000.	ADS-B system shall meet or exceed latency requirements as specified within RTCA/DO-242 (reference R3.16 in Section 4.0).	X	
105	57		FAA shall select frequency spectrum to ensure uninterrupted operation in all defined environmental conditions.		X
103	58	Consider alternative frequency spectrum as backup.	The ADS-B system design for safety; critical command and control functions shall require failure tolerance for three independent failures, or three human errors, or a combination of three independent failures and human errors per MIL-STD-882C, APPENDIX C, Paragraphs 70.1.1 and 70.1.2	X	
106	59	Design ground stations to minimize damage due to lightning or other adverse weather effect.	ADS-B system shall meet the requirements for protection against RF emissions, lightning, rain, snow, ice, extreme temperatures, extreme and humidity to the standards in FAA-G-2100g, MIL-STD-461D, MIL-STD-436D and FAA Requirements.		
106	60	Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D AND FCC Regulations.	ADS-B system shall meet the requirements for protection against RF emissions, lightning, rain, snow, ice, extreme temperatures, extreme and humidity to the standards in FAA-G-2100g, MIL-STD-461D, MIL-STD-436D and FAA Requirements.		
106	60a		ADS-B system shall meet the requirements for protection against RF emissions, lightning, rain, snow, ice, extreme temperatures, extreme and humidity to the standards in FAA-G-2100g, MIL-STD-461D, MIL-STD-436D and FAA Requirements.		

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
106	60b		ADS-B system shall meet the requirements for protection against RF emissions, lightning, rain, snow, ice, extreme temperatures, extreme and humidity to the standards in FAA-G-2100g, MIL-STD-461D, MIL-STD-436D and FAA Requirements.		
106	60c		ADS-B system shall meet the requirements for protection against RF emissions, lightning, rain, snow, ice, extreme temperatures, extreme and humidity to the standards in FAA-G-2100g, MIL-STD-461D, MIL-STD-436D and FAA Requirements.		
107	61		Human interfaces analysis shall be conducted using requirements for airborne displays, found in MFD or CDTI, using standards found in CDTI MOPS, Version 25-V2.		X
108	61a	Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with human factors in the integration of NAS Modernization systems, i.e., ADS-B, CPDLC, FIS, etc.	Human interfaces shall be observed using requirements for ground controller displays found in Visual Specification for Ground Display Systems, Version 1.1.		X
109	61b	Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with human factors related to possible conflicting communication.	Human factors safety related hazards shall be analyzed for identifying risks and developing controls for airborne ADS-B equipment using requirements of HRR-510		X
110	61c		Human factors safety related hazards shall be analyzed for ground ADS-B equipment using requirements of HRR-510		X
111	61d		Human factors related simulations shall be conducted to assure flightcrew compatibility and interoperability using ADS-B with CPDLC, FIS, FMS.		X
112	62	Conduct analysis, studies, simulations and/or flight tests to develop engineering requirements to eliminate or control the system risks to an acceptable level.	System hazards shall be identified through appropriate analysis and controlled to a risk level acceptable to the ADS-B Program and FAA management authorities as documented in the SSMP and SSPP.		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
112	63	Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with system anomalies that could cause conflicting flight critical information to be communicated.	System hazards shall be identified through appropriate analysis and controlled to a risk level acceptable to the ADS-B Program and FAA management authorities as documented in the SSMP and SSPP.		X
112	64	Conduct analysis, studies, simulations and/or flight tests to develop engineering requirements to minimize system anomalies that result from conflicting information.	System hazards shall be identified through appropriate analysis and controlled to a risk level acceptable to the ADS-B Program and FAA management authorities as documented in the SSMP and SSPP.		X
113	65	Develop "rules of the road"	FAA shall develop new procedures, as required, for changes to existing VFR and IFR operational requirements for separation, control, conflict resolution, and document in 7110.65 and the AIM.		X
114	66	Develop appropriate aircrew procedures to accommodate any possible contingency situation.	FAA shall develop new procedures for flightcrews to be followed during known emergency or other contingency situations and document in AIM and 7110.65.		X
115	67	.	FAA shall modify 7110.65 to include new controller known emergency or other contingency procedures, to be verified by the ADS-B		X
116	68	Develop appropriate training materials and training programs to ensure that all participants in a shared responsibility environment understand their role and safe operation procedures	FAA shall develop training materials and training programs to ensure that flightcrews and controllers are certificated to execute their roles and procedures to ensure safe operations.		X
117	69	Design ADS-B CHI to minimize the potential for human error.	The ADS-B CHI shall be designed to control or eliminate human error.		X
118	70	Design ADS-B for use in international communication in accordance with acceptable human factors design practices (e.g., IACO standard symbology).	FAA shall designate responsible delegate to coordinate with ICAO to develop standard symbology for display of ADS-B information.		X
2	70	Design ADS-B for use in international communication in accordance with acceptable human factors design practices			
119	72	Design reliable built-in test capability.	ADS-B system shall ensure that data is "reported" with integrity at least equal to or better than 1E x 10-6. (Reference RTCA/DO-242, Paragraph 3.3.6.5)		X

CR. No.	Con. No.	Controls	Candidate Safety Requirements/ Recommendations	Existing Requirement	Recommended Requirement
120	73	Design system to determine data validity.	ADS-B system shall ensure that source data which is processed and broadcast meets or exceeds detectable error of not less than $1E \times 10^{-9}$ .		X
121	74	Ensure that both aircraft are equipped for the application. This control recommendation deals with a scenario in which the aircraft have insufficient range for the application. This may be a problem during transition in mixed equipage environments.	FAA shall develop procedures to instruct controllers to authenticate minimum equipage for operations under certain separation assurance applications.		X
122	75	Provide alternate means of communication, i.e., Voice backup. This control recommendation deals with miscommunication due to a "language barrier". This may result from international aircraft equipped with different technology operating in U.S. airspace, or U.S. aircraft operating in foreign airspace.	Voice backup shall be provided to support ADS-B surveillance application in accordance with NAS SR-1000-3.6.1.	X	
119	76	Design ADS-B system to include end-to-end data integrity check functionality and provide proper notification if data corruption is detected	ADS-B system shall ensure that data is "reported" with integrity at least equal to or better than $1E \times 10^{-6}$ . (Reference RTCA/DO-242, Paragraph 3.3.6.5)		
123	77	Require warning lights on flying object to enhance "see and avoid" separation.	FAA [AVR] shall institute rulemaking to require improved aircraft lighting to enhance "see and avoid". Reference: Advisory Circular 90-48C		

It should be noted here that not all safety requirements would be included in the system specification, because some of the requirements fall on other FAA organizations to implement and verify. For example, ATC procedures are found in FAA 7110.65. Modifications to these procedures, or development of new procedures are not a hardware manufacturer's responsibility. Likewise, training may be the responsibility of a FAA organization, while the contractor may develop the training manuals and curricula.

## 8.0 Preliminary Hazard Analysis Findings

### 8.1 Risk Assessment Ratings

Forty (40) **High Risk** rating scenarios were identified. Seven hundred ninety-nine (799) fell in the **Medium Risk** region of the matrix, and 39 (39) scenarios were in the **Low Risk** region. The PHA in Volume 2 is sorted in the order of decreasing risk, i.e., 1C/High, 1D, 2C, 3B/Medium, 2D, 3C, 4B, 3D, and 4C/Low.

The results of the PHA are summarized in Figure 8-1 (below).

Severity \ Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A					
Remote B		3	313	1	
Extremely Remote C		1	18	157	40
Extremely Improbable D			10	7	328

High Risk
Medium Risk
Low Risk

Figure 8-1 - Assessment of Risk Associated with PHA Scenarios

Note that there are scenarios given a severity level of “I Catastrophic”. At this high level of analysis, a collision between two aircraft is considered catastrophic regardless of the number of occupants. The definition of Catastrophic is: Results in multiple fatalities. The definition of Hazardous is: Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be:

- (4) Large reduction in safety margin or functional capability
- (5) Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely
- (6) Serious or fatal injury to small number of persons (other than flightcrew)

Severity differentiates between multiple fatalities and a small number of fatalities. It was not possible at this level of analysis to create scenarios in which the number of occupants was a variable. To do so would have at least doubled the collision scenarios, without resulting in any new or different controls/safety requirements. The hazardous category is useful to organizations in FAA that deal with certification and regulation of aircraft.

## **9.0 Conclusions and Recommendations**

This Preliminary Hazard Analysis (PHA) was developed based upon an expansion of, the Initial Hazard Assessment (IHA) of ADS-B completed 21 January, 2000. The IHA was limited in scope in that it only considered the severity of consequences associated with a specifically developed hazard scenario. There was not sufficient information at that time to define the probability (or likelihood) of occurrence. Risk Ratings could not be developed without the development of the requisite associated probability of occurrence. As the ADS-B system has evolved over the last several months, with additional system clarification, this Preliminary Hazard Analysis has been completed which takes into account both factors.

The IHA analysis, contained in Volume 1 ADS-B Safety Engineering Report #1: Initial Hazard Analysis, produced controls and mitigations to eliminate or reduce the risks associated with identified hazards. The controls and mitigations were turned into Candidate Safety Requirements/Recommendations requirements statements for possible inclusion in an initial requirements document (IRD). The requirements covered the end-to-end operation of the system and may therefore impact the manufacturers of the on-board avionics, the operators of the aircraft or vehicle, the services to be supplied by the NAS, the builders of the ground system, and the applications user community. The IHA hazard scenario worksheets are contained in Volume 2 ADS-B Safety Engineering Report #1: Initial Hazard Analysis.

The PHA expanded on the IHA and generated a total of 878 hazard scenarios. A hazard scenario, as contained in scenario sets, shows the sequential events which must occur to culminate in an undesired outcome (harm). The harm (accident) is a combination of system state and contributors to a sequence of events that result in a postulated harm. The contributors are varied in combinations and permutations of system failures and inappropriate human action or response. Each variation in a scenario set may affect either severity or likelihood, or both and may identify a new or different control requirement.

The expanded PHA hazard scenario worksheets are contained in the PHA Volume 2 of the ADS-B Design Analysis report: ADS-B Preliminary Hazard Analysis Volume #1. The PHA was conducted using the FAA System Safety Management Program, dated 1 January, 2001 and the methodology defined in the FAA System Safety Handbook, dated 30 December, 2000. The new hazard scenarios included both an expansion of the initial scenarios, at a system level based on emerging system information, as well as new scenarios based primarily on potential equipage combinations within the National Airspace System (NAS). The equipage combinations are

derived from equipment assumed to be operational through the year 2015. The equipage combinations are listed and discussed in more detail in section 4.2 Aircraft Equipment Overview, of this report and listed in section 5.0 Approach and Methodology.

The output of the PHA is used in: (1) further developing system safety requirements to be added to the Safety Requirements Verification Table (SRVT), (2) preparing performance/design specifications, and (3) initiating the hazard tracking and risk resolution process for the ADS-B system. The PHA produced a total of 125 Candidate Safety Requirements (CSRs). Thirty-eight (38) of the CSRs were identified as Existing requirements. The remaining eighty-seven (87) requirements were identified as Recommended Candidate Requirements. Existing requirements are those that can be referenced in current program documentation, i.e., Military Specifications, FAA Orders and other governmental regulations, and consensus standards. Recommended CSRs are those control methods that are not referenced in current program documentation and are therefore, recommended. The CSRs are written as high-level "shall" statements that are postulated to control or mitigate hazardous outcomes as identified in the analysis.

The PHA findings from the analysis are summarized as follows:

- Recommendations that relate to “see and avoid” procedures, such as lighting and marking of aircraft, flying objects, ground vehicles, and fixed objects.
- Recommendations relating to alternate, independent means of validating the ADS-B provided information, such as call sign, ID, position, velocity, and altitude. These are generally requirements on the NAS to continue to provide current surveillance and communications systems until sufficient confidence is established in the reliability and availability of ADS-B. This approach is consistent with current ADS-B plans for a transition period in which ADS-B will be operated in parallel with existing systems.
- Design requirements for the ADS-B system to ensure reliable operation, high availability, and self-test features to detect malfunctions or loss of integrity.
- Requirements that cite existing FAA, DOD, or industry specifications or standards
- Recommendations for studies to determine human factors design requirements using pilots and controllers to determine the safest implementation of the system. Laboratory simulations, flight tests, and operational evaluations are included.
- Requirements for compatibility and integration of information from a wide range of input sources/types expected to be in use through the year 2015.
- Requirements for training associated with safety related to ADS-B design, maintenance, or operation.
- Requirements to prevent interface malfunctions between existing and legacy systems and ADS-B resulting in loss of ADS-B capabilities.
- Requirements to prevent system/subsystem malfunctions from propagating to other systems/subsystems or communications/avionics equipment.
- Requirements to prevent communication delays or losses as a result of LTA mixed equipage procedural integration.
- Requirements designed to prevent less than adequate integration of ADS-B with Airborne Conflict Management (ACM).
- Requirements to ensure integrated ADS-B System time source is synchronized for accurate position, velocity and time.

- Requirements for integration of national and international separation standards associated with ADS-B use.

While the 878 total hazard scenarios were identified and analysed in the ADS-B PHA, forty-one (41) were ranked as High Hazards. Of these 41 high hazards 40 were ranked as 1C (Catastrophic Severity and Extremely Improbable) and one (1) ranked as 2B (Hazardous Severity with a Remote Probability). The 41 high hazard scenarios consisted of the following:

24 - Human factors:

Excessive workload, language barriers/conflicts, input errors, conflicts between pilots & controllers,

9 - Mixed Equipage:

Confusion, conflicts, errors, system inaccuracies

7 - Security:

Jamming, spoofing, intentional intrusion

1 - Unidentified intruder

The high hazards were ranked relative to all of the hazards identified. All identified high and medium hazards will be placed into a Hazard Tracking System (HTS). The HTS will allow each hazard to be tracked throughout system lifecycle activities. As the system matures through design and build activities additional controls may be identified which may impact a hazards ranking.

The overriding conclusion of the Preliminary Hazard Analysis is the ADS-B system will have a tremendous impact on the structure of the NAS architecture from introduction through full planned applicability. It must interface with existing and legacy systems with reliability, which is both acceptable and measurable. The findings of the PHA demonstrate the prudence of a phased introduction into the NAS utilizing a closed-loop approach with continuous monitoring/testing feedback. System operability, reliability confidence must be obtained prior to planned expansion.

Although this analysis was performed based on the current state of knowledge of the requirements, an ADS-B design does not yet exist: therefore, all hazards may not have been identified. In order to assure a successful ADS-B System Safety Program, follow-on safety reviews must be conducted. Review and update of the hazard analysis, scenario by scenario, is required.

Future changes to the ADS-B baseline system or program must be evaluated from a system safety perspective. This PHA is based upon current system safety engineering practices as specified in the referenced applicable specifications and requirements documents. Subjective judgements and logic has been applied to the development of applicable scenarios, the identification of appropriate mitigation, and to ensure conservative estimations of risk.

## **10.0 Security**

Several information security hazard scenarios are identified in this PHA, however, this report does not meet the requirements of a formal and complete information security analysis.

## 11.0 References

- (1) FAA, *Research Evaluation Plan for ADS-B, Phase 1: Identification of Research Needs*, September 30, 1999
- (2). *NAS Modernization System Safety Management Plan, FAA Acquisition Management System*, January 1 2001
- (3). FAA-APO-99-1 FAA Long Range Aerospace Forecasts Fiscal Years 2015,2020 & 2025, June 1999.
- (4). MIL-STD-882C System Safety Program Requirements, 19 Jan 1993
- (5) FAA System Safety Management Program, May 1, 2000
- (6) FAA System Safety Handbook, January 2001
- (7) ADS-B High-Level Concept of Operations, status Summary, 12 January 2001.

## 12.0 Bibliography

1. NAS –SR-1000, *System Requirements Specification*, November 1991
2. FAA Order 8040.4 *Safety Risk Assessment*, June 26, 1998
3. MIL-STD-882C *System Safety Program Requirements*, 19 Jan 1993
4. FAA, *National Airspace System Architecture, Version 4.0*, January 1999
5. FAA CT96/1 *Human Factors Design Guide*
6. FAA G-2100-F, *Electronic Equipment General Requirements*
7. MIL-STD-461D, *Requirement for the Control of Electromagnetic Interference Emissions and Susceptibility*
8. MIL-STD-462D, *Measurement of Electromagnetic Interference*.
9. FAA ADS-B Plan, June 29, 1999
10. SC-186 WG4 Paper No. 1198-1, *Development of Technical Requirements for Automatic Dependent Surveillance-Broadcast (ADS-B) Applications*, November, 1998
11. Mission Need Statement (MNS) 326, *Automatic Dependent Surveillance-Broadcast (ADS-B)*
12. *ADS-B 1090 MHz Minimum Operational Performance Standards (MOPS)*, February 1, 1998
13. *ATS Concept of Operations for the National Airspace System*, September 30, 1997

## Appendix A Acronyms and Definitions

<b>Acronym</b>	<b>Definition</b>
AMASS	Airport Movement Automation System??
AMS	Acquisition Management System
ARS	Air Traffic System Requirements Service
ATC	Air Traffic Control
ATS	Air Traffic Services
BITE	Built-in Test Equipment
CAA	Cargo Airline Association
CDTI	Cockpit Display of Traffic Information
Corrupted Data	Input data that has been intentionally changed to make it invalid
COTS	Commercial Off-the-Shelf
CPDLC	Controller-Pilot Data Link Communication
FFP1	Free Flight Phase One
FIS	Flight Information System
FMS	Flight Management System
FRD	Final Requirements Document
GNSS	Global Navigation System
ICAO	International Civil Aviation Organization
IHA	Initial Hazard Analysis
INS	Inertial Navigation System
IRT	Integrated Requirements team
ISA	Integrated Systems Configurations
LTA	Less Than Adequate
LORAN	Long Range Radar Aid to Navigation
MASPS	Minimum Aviation System Performance Standards
MTR	Military Training Route
NAS	National Airspace System
NDI	Non-Developmental Item
NOTAM	Notice to Airmen
RTCA	RTCA, Inc. (formerly Radio Technical Commission for Aeronautics)
SSR	Secondary Surveillance Radar
SUA	Special Use Airspace
TBD	To Be Determined
TCAS	Traffic Collision Avoidance System
TIS	Traffic Information System