SURVEILLANCE AND BROADCAST SERVICES PROGRAM
SEGMENT 1

SAFETY RISK MANAGEMENT DOCUMENT:
PRELIMINARY HAZARD ANALYSIS

DOCUMENT NO.: SBS-SRMD-062606-1

SEPTEMBER 18, 2006

VERSION 1.0

Submitted by: _____ Date: _____
Vincent Capezzuto, SBS Program Manager

Reviewed by: _____ Date: _____
Kathy D. Smith, ATO-E Senior Safety Engineer

Approved by: _____ Date: _____
Richard L. Day, Vice President, ATO-E

Reviewed by: _____ Date: _____
Alan Feinberg, ATO-T Senior Safety Engineer

Approved by: _____ Date: _____
Bruce Johnson, Vice President, ATO-T

Approved by: _____ Date: _____
Martino Dennis, ATO System Safety Working Group Chair
(ATO SSWG)

Approved by: _____ Date: _____
Huan Nguyen, Director, Safety Risk Management

Approved by: _____ Date: _____
Associate Administrator, AOV

FOREWORD

This Safety Risk Management Document (SRMD) describes the proposed changes to the National Airspace System (NAS) pertaining to the SBS Program and identifies system safety hazards and safety requirements needed to mitigate the risks associated with those hazards. As the program progresses, this SRMD will record the evidence to support that the changes to the NAS are acceptably safe.

Version 1.0 of the SRMD addresses the first segment of the SBS Program established via a final investment decision in June 2006. When additional program segments are defined or the scope of the SBS Program is modified, this SRMD will be revised as necessary and submitted to the ATO System Safety Work Group (SSWG).

One planned revision to the SBS SRMD involves the Capstone ADS-B system. In July 2006, the SBS and Capstone Programs entered into a Service Level Agreement to formally transfer responsibility and ownership of the Capstone ADS-B system and its related architecture to the SBS Program. The SBS Program will revise this SRMD to document Capstone ADS-B system hazards and submit the updated SRMD to the ATO SSWG. In the interim, the SBS Program accepts the Capstone Phase II safety hazards identified in the table below. These hazards were transferred from Capstone to SBS in accordance with the ATO SSWG meeting minutes from July 25, 2006. The SBS Program will track these hazards until formal closure.

Table 1: Capstone Phase II Safety Hazards Transferred to the SBS Program

Capstone Phase II Hazard # (Scenario #)	Capstone Phase II Hazard Description (Scenario)
99 (Ba43)	Deviations occur to safety-related data/information displayed between the controller and pilots and an inappropriate clearance is given resulting in collision.
106 (Ba59)	EnRoute IFR aircraft surveillance is lost due to malfunction. Situation is confined to a single target and it is not detected automatically. Event results in collision.
125 (Ba97)	Ground system alerts/warnings are LTA. Alert/warning does not provide notice when needed. Situation results in increased accident risk.
130 (Bb109)	Aircraft is EnRoute at minimums for VFR and weather deteriorates rapidly. HMI occurs associated with weather data/information. Pilot/Aircrew relying on displayed weather data/information for successful VFR navigation. HMI contributes to confusion and results in inadvertent exposure to adverse weather and CFIT.
131 (Bb112)	Aircraft is EnRoute at minimums for VFR and weather deteriorates rapidly. Weather data/information displayed in cockpit is inadequate. Pilot/Aircrew relying on displayed weather data/information for successful VFR navigation. Situation contributes to confusion and results in inadvertent exposure to adverse weather and CFIT.

EXECUTIVE SUMMARY

ADS-B is an advanced surveillance technology that enables equipped aircraft or surface vehicles to broadcast their identification, position, altitude, velocity, and other information. Since the position information is normally derived from the Global Positioning System (GPS) and broadcast approximately once per second, it provides improved accuracy and more timely information updates than conventional surveillance. The improved positional accuracy and the ability to provide additional aircraft-derived flight parameters (flight objects or flight data message elements) will result in enhanced surveillance in the NAS. ADS-B is automatic because no external stimulus is required; it is dependent because it relies on on-board navigation sources and onboard 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, aircraft or ground-based, are receiving its broadcast.

ADS-B technology also enables the implementation of Traffic Information Service-Broadcast (TIS-B), ADS-B Rebroadcast (ADS-R), and Flight Information Service-Broadcast (FIS-B) to support enhanced situational awareness and other applications intended for air crews. TIS-B service provides traffic information to receiver-equipped aircraft and surface vehicles based on the conventional radar returns received for non-ADS-B equipped aircraft. ADS-R provides traffic information to equipped aircraft based on ADS-B transmission from aircraft on independent data links. FIS-B provides weather and NAS Status information to equipped aircraft.

Per the FAA's ADS-B Link Decision, two data link technologies, the 1090 MHz extended squitter (1090ES) and the 978 MHz Universal Access Transceiver (UAT) have been approved for use in the NAS. It is anticipated that air transport category aircraft will equip with the 1090ES link and general aviation will equip with the UAT link. Both the UAT and 1090ES links support TIS-B and ADS-R services. Only UAT supports FIS-B service.

The Surveillance and Broadcast Services Safety Risk Management Panel prepared and conducted the Preliminary Hazard Analysis (PHA) for seven applications selected for the near-term NAS implementation:

- ATC Surveillance
- Weather and NAS Status Situational Awareness
- Enhanced Visual Acquisition
- Enhanced Visual Approaches
- Final Approach and Runway Occupancy Awareness
- Airport Surface Situational Awareness
- Conflict Detection

Rulemaking is planned to require aircraft equipage with ADS-B transmit capability to support the ATC Surveillance application. On the other hand, equipping with avionics necessary to support the remaining applications is voluntary.

Proposed locations for deploying or updating ADS-B and TIS-B/FIS-B ground infrastructure include the Gulf of Mexico, Louisville, and Juneau. These locations are subject to change based on the refinement of the SBS Program business case.

Preliminary hazards were identified based on the loss of functionality and malfunctions associated with the ADS-B related services. Hazard effect severities were characterized according to ADS-B application and worst-case system state.

Based on the results of the PHA, 80 hazards were identified, including 8 high-risk hazards, 15 medium-risk hazards, and 57 low-risk hazards. Many of these hazards are repeated across the different in-cockpit applications, but assessed risk may differ by application.

With the verification of the following recommended safety requirements, the assessed risk level for all hazards is expected to be medium to low risk. It should be noted that if the recommended requirements are not implemented, high risks may be realized.

- The FAA shall define and implement requirements for an independent automated safety monitoring capability that monitors inputs and outputs at interfaces between SBS subsystems and provides fault diagnostics, failure control and correction, and configurable status monitoring and alarm annunciation. Software for the automated safety monitoring capability shall satisfy the objectives for Assurance Level 2 defined in RTCA DO-278 or an equivalent software design assurance standard.
- The SBS Contractor shall adhere to industry best practices for software development.
- The ADS-B system shall be designed to meet Mil-STD-461 requirements for electromagnetic susceptibility and interference.
- The combined probability that ADS-B primary and backup surveillance fails shall be no more than extremely remote (i.e., 10^{-7})
- The FAA shall develop and implement certification procedures to verify that SBS ground equipment performance is within tolerance.
- The FAA shall perform an analysis of 1090 MHz spectrum utilization impacts given peak ADS-B, Mode S, and Mode A/C target loads and densities and the worst-case potential combination of ATC surveillance systems which utilize the 1090 MHz spectrum in the same service area. The spectrum analysis shall evaluate the impacts to aircraft transponder occupancy, TCAS performance, and the probability of target detection for each ATC surveillance system considered above. If deemed necessary based on the results of the spectrum analysis, the FAA shall develop a mitigation strategy to minimize the risk to maintaining required ATC surveillance systems' performance and required TCAS performance.
- The system shall provide a notification to maintenance operators prior to reaching a computer processing utilization threshold at which target data may be lost or dropped.
- The system shall provide a notification to maintenance operators prior to reaching a telecommunications loading threshold at which target data may be lost or dropped.
- The system shall provide a notification to maintenance operators prior to reaching a computer memory utilization threshold at which target data may be lost or dropped.
- The probability that the system fails to notify ATC when surveillance data is missing for an adaptable amount of time shall be no more than 10^{-7}.
- When selecting locations for ADS-B ground stations, the FAA shall perform a coverage / siting analysis that considers aircraft bank angles which may result in line-of-sight coverage problems (e.g., the aircraft banks such that the transmit / receive antenna is angled away from the ground station antenna).
- The FAA shall perform a collision risk analysis in accordance with Flight Standards guidelines to determine the required availability of the Aircraft/Vehicle function given terminal separation standards and end-to-end (i.e., air / ground) system performance parameters
- Hardware for the Aircraft/Vehicle function shall comply with RTCA DO-160D Environmental Conditions and Test Procedures for Airborne Equipment.
- The approval process for design, production, installation, and operation of ADS-B equipment onboard civil aircraft shall comply with "The FAA and Industry Guide to Product Certification" and "The FAA and Industry Guide to Avionics Approvals."
- The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B and ancillary equipment.
- The end-to-end system latency shall not exceed the maximum acceptable latency based on Flight Standards collision risk analysis.
- The FAA shall ensure accuracy of the terrain/airfield map displayed to ATC.
- The FAA shall develop and implement procedures to verify alignment of surveillance sensor data to the automation system display map.
- The probability that the system displays an incorrect target ID to the controller shall be less than 10^{-6}.
- The FAA shall develop and implement certification procedures to verify that barometric pressure correction applied at the automation system is accurate.
- The FAA shall maintain legacy surveillance systems until ADS-B equipage level deemed sufficient to remove legacy systems and transition to NRA.

- The FAA shall analyze and characterize the separation errors at the ATC display between each combination of ADS-B and radar-only targets.
- The FAA shall perform a collision risk analysis to validate separation standards.
- The FAA shall develop and publish procedures for pilots to implement when concerned with ATC instructions based on traffic and / or weather information presented on the CDTI (Note: This recommended requirement does not preclude defining procedures in which the pilot must comply with ATC instructions regardless of information presented on the CDTI).
- Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI.
- Train pilots to check for updated weather information pre-flight and in-flight and to refrain from over-relying on the CDTI.
- The FAA shall provide NOTAMS or other pilot notification to indicate that not all traffic are participants in CDTI- based applications.
- Provide warnings and cautions regarding over-reliance on CDTI in avionics equipment manuals, pilot training manuals, and AIM.
- Provide placard on CDTI to indicate application / display only for situational awareness / advisory use.
- The CDTI shall provide the air crew with an indication when: (a) Inadequate or invalid surveillance data would cause unacceptable traffic information display. (b) Inadequate or invalid own-ship data would cause unacceptable traffic information display. (c) Application processing is not functioning normally. The RTCA shall define specific performance requirements for acceptable traffic information display.
- Processing and interface capacities shall be specified to accommodate the traffic densities and operating ranges for the most demanding application(s).
- The enhanced visual application shall notify the air crew when altitude information is missing.
- The Conflict Detection Application shall provide an indication that alerts have been disabled
- Software for the Aircraft/Vehicle function shall satisfy the objectives for Software Level C defined in RTCA DO-178B or an equivalent software design assurance standard.
- The CDTI shall provide volume control to adjust for ambient noise in the cockpit.
- The Conflict Detection application shall present only one alert level at a time. (Note: Verify that corresponding ASA MASPS statement in section D.2.2.2 pg D-24 for preventing issuance of simultaneous alerts is carried through in MOPS)

DOCUMENT CHANGE HISTORY

VERSION	DATE	DESCRIPTION OF CHANGES

DOCUMENT ORGANIZATION

VOLUME I
1. INTRODUCTION
2. SYSTEM DESCRIPTION
3. PROPOSED CHANGE TO THE NAS
4. ANALYSIS METHODOLOGY

VOLUME II
5. HAZARD ANALYSIS

VOLUME III
6. LIST OF SAFETY REQUIREMENTS
7. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS
8. REFERENCES / BIBLIOGRAPHY
APPENDIX A: ACRONYMS

VOLUME IV
APPENDIX B: FAULT TREES AND EVENT TREES

ATTACHMENT 1 – NATIONAL AIRSPACE SYSTEM SURVEILLANCE AND BROADCAST SERVICES CONCEPT OF OPERATIONS

ATTACHMENT 2 – FUNCTIONAL ANALYSIS OF THE SURVEILLANCE AND BROADCAST SERVICES (SBS) SYSTEM

SURVEILLANCE AND BROADCAST SERVICES PROGRAM
SEGMENT 1

SAFETY RISK MANAGEMENT DOCUMENT:
PRELIMINARY HAZARD ANALYSIS

VOLUME I – SYSTEM DESCRIPTION

SEPTEMBER 18, 2006

VERSION 1.0

TABLE OF CONTENTS

1. INTRODUCTION 9

1.1 PURPOSE 9
1.2 PARTICIPANTS 9
1.3 SCOPE 10
1.4 EXPECTED BENEFIT 10

2. SYSTEM DESCRIPTION 10

2.1 SERVICES 11
2.1.1 Automatic Dependent Surveillance-Broadcast (ADS-B) 11
2.1.2 Traffic Information Service-Broadcast (TIS-B) 12
2.1.3 Automatic Dependent Surveillance-Rebroadcast (ADS-R) 12
2.1.4 Flight Information Service-Broadcast (FIS-B) 12
2.2 APPLICATIONS 12
2.2.1 ATC Surveillance 14
2.2.2 Weather and NAS Status Situational Awareness 15
2.2.3 Enhanced Visual Acquisition 15
2.2.4 Enhanced Visual Approach 15
2.2.5 Final Approach and Runway Occupancy Awareness 15
2.2.6 Airport Surface Situational Awareness 15
2.2.7 Conflict Detection 16
2.3 CONCEPT OF OPERATIONS 16
2.3.1 NAS Service Providers 16
2.3.2 NAS Users 16
2.4 FUNCTIONAL ANALYSIS 16
2.4.1 F1 - Aircraft/Vehicle (A/V) Function 19
2.4.2 F2 - Link Specific Processing Function 19
2.4.3 F3 - Broadcast Services Function 19
2.4.4 F4 - ATC Automation Function 19
2.4.5 F5 - Maintenance Function 19

3. PROPOSED CHANGE TO THE NAS 20

3.1 IMPLEMENTATION STRATEGY 21
3.1.1 Phased Deployment 21
3.1.2 Segment Applications 21
3.2 MAINTENANCE CONCEPT 21

4. ANALYSIS METHODOLOGY 22

4.1 GENERAL ASSUMPTIONS AND CAVEATS 22
4.2 HAZARD MODEL 23
4.2.1 Overview 23
4.2.2 Definitions 23
4.3 RISK DETERMINATION 24

LIST OF TABLES

TABLE 1-1: ANALYSIS PARTICIPANTS 9
TABLE 2-1 APPLICATIONS, SERVICES, AND FUNCTIONS 10
TABLE 2-2 SUMMARY OF CDTI REQUIREMENTS FOR NEAR-TERM TRAFFIC APPLICATIONS 14
TABLE 4-1: SEVERITY DEFINITIONS 26
TABLE 4-2: LIKELIHOOD DEFINITIONS 26
TABLE 4-3: RISK ASSESSMENT MATRIX 27
TABLE 4-4: RISK ACCEPTANCE CRITERIA 28

LIST OF FIGURES

FIGURE 2-1 SURVEILLANCE AND BROADCAST SERVICES SYSTEM....11
FIGURE 2-2 SCOPE OF SURVEILLANCE AND BROADCAST SERVICES....13
FIGURE 2-3 TOP-LEVEL FUNCTIONAL BLOCK DIAGRAM FOR SBS SYSTEM....18
FIGURE 2-4 TOP-LEVEL N^2 DIAGRAM FOR SBS SYSTEM....18
FIGURE 4-1: HAZARD ANALYSIS MODEL....23

1. INTRODUCTION

1.1 Purpose

The purpose of the PHA is to make an early identification of the hazards, hazardous system states (with all of the accompanying system implications), and safety requirements. The PHA is not intended to affect control of all risks, because sufficient information is not available at this stage in the SBS Program.

This PHA was developed in accordance with the requirements of the Federal Aviation Administration's (FAA's) System Safety Management Program (SSMP) version 10 and the Safety Management System (SMS) version 1.1.

1.2 Participants

The table below identifies the SBS Safety Risk Management Panel representatives that participated in this analysis.

Table 1-1: Analysis Participants

NAME	ORGANIZATION	ROLE
Mike Allocco	Flight Standards AFS-430	Provided expert safety engineering guidance concerning application-specific hazards; reviewed preliminary hazard list
Jeff Breunig	SBS Program Office	Provided feedback from a pilot's perspective on system states and severities for hazards associated with in-cockpit applications
Roxaneh Chamlou	SBS Program Office / MITRE	Researched existing ADS-B-related safety analyses; identified and analyzed hazards for all applications; identified existing hazard controls and recommended safety requirements
Jonathan Hammer	SBS Program Office / MITRE	Identified existing hazard control and recommended safety requirements for multiple applications; analyzed hazard likelihoods
Jennifer Lamont	SBS Program Office / Systems Enginuity	Identified and analyzed hazards for all applications; identified existing hazard controls and recommended safety requirements
John Marksteiner	SBS Program Office	Provided feedback from a pilot's perspective on system states and severities for hazards associated with in-cockpit applications
Chris Moody	SBS Program Office / MITRE	Provided feedback from a pilot's perspective on scenarios and existing controls for hazards associated with the Weather and NAS Status Situational Awareness Application
Robert Novia	ATC (Houston Center)	Provided feedback from an en route, oceanic, and offshore / helicopter air traffic control perspective on system states and severities for hazards associated with the ATC Surveillance Application
Dave Rudolf	ATC (Terminal)	Provided feedback from a terminal air traffic control perspective on system states and severities for hazards associated with the ATC Surveillance Application (surface and terminal domains)
Rob Strain	SBS Program Office / MITRE	Provided feedback from a pilot's perspective on scenarios and existing controls for hazards associated with the Weather and NAS Status Situational Awareness Application

1.3 Scope
The PHA addresses the system and life cycle phase specific safety risks associated with the SBS Program.

1.4 Expected Benefit
The output of the PHA is used in: (1) further developing system safety requirements to be added to the System Safety Requirements List, (2) preparing performance requirements specifications, and (3) initiating the hazard tracking and risk resolution process.

2. SYSTEM DESCRIPTION
ADS-B is an advanced surveillance technology that enables equipped aircraft, or surface vehicles, to broadcast their identification, position, altitude, velocity, and other information. Since the position information is normally derived from the Global Positioning System (GPS) and broadcast approximately once per second, it provides improved accuracy and more timely information updates than conventional surveillance. The superior positional accuracy and the ability to provide additional aircraft-derived flight parameters (flight objects or flight data message elements) will result in enhanced surveillance in the NAS. ADS-B is automatic because no external stimulus is required; it is dependent because it relies on on-board navigation sources and onboard 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, aircraft or ground-based, are receiving its broadcast.

ADS-B technology additionally facilitates the implementation of Traffic Information Service-Broadcast (TIS-B), ADS-B Rebroadcast (ADS-R), and Flight Information Service-Broadcast (FIS-B) to support enhanced situational awareness and other applications. TIS-B service provides traffic information to equipped aircraft and surface vehicles based on the conventional radar returns received for non-equipped aircraft. ADS-R provides traffic information to equipped aircraft based on ADS-B transmission from aircraft on independent data links. FIS-B provides weather and NAS Status information to equipped aircraft.

Per the FAA's ADS-B Link Decision, two data link technologies, the 1090 MHz extended squitter (1090ES) and the 978 MHz Universal Access Transceiver (UAT) have been approved for use in the NAS. It is anticipated that air transport category aircraft will equip with the 1090ES link and general aviation will equip with the UAT link.

The introduction of ADS-B services into the NAS will enable some well established applications, currently supported by radar and other existing surveillance sources, and facilitate the introduction of new applications, that promise to improve safety and increase capacity. See the FAA's Surveillance and Broadcast Services Concept of Operations (CONOPS) for further details on ADS-B Services and Applications. Table 2-1 summarizes the relationship between ADS-B the ADS-B services (Section 2.1) that enable the applications (Section 2.2), and the ADS-B operational system functions (Section 2.3) required to provide the ADS-B services.

Table 2-1 Applications, Services, and Functions

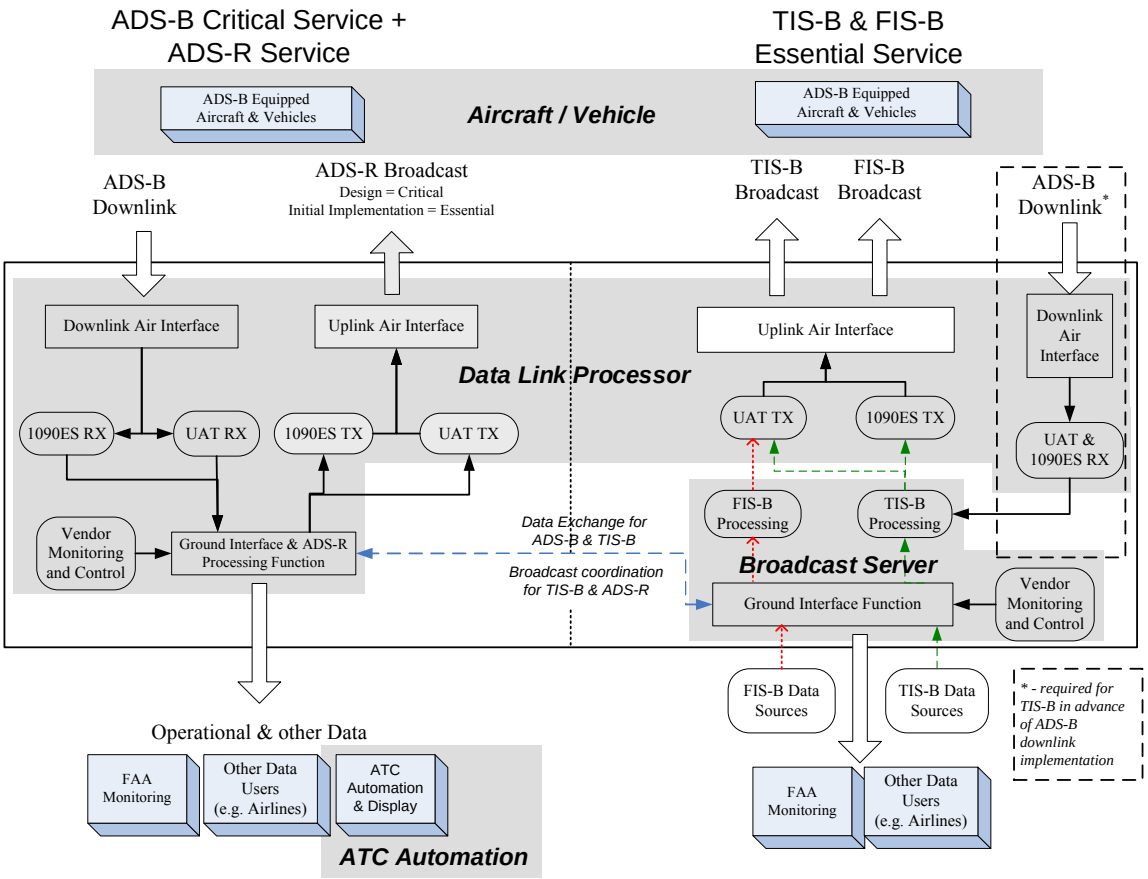
ADS-B Enabled Applications	Services	Broadcast Services Function	Link-Specific Processing Function	ATC Automation Function	Aircraft / Vehicle Function
ATC Surveillance	ADS-B		X	X	X (Transmit)
Airport Surface Situational Awareness (ASSA) Final Approach Runway Occupancy (FAROA) Enhanced Visual Acquisition (EVAcq) Enhanced Visual Approach (EVApp) Conflict Detection (CD)	ADS-B (only Aircraft/Vehicle Functionality Required) ADS-R TIS-B*	X	X		X (Receive)
Weather and NAS Status Situational Awareness	FIS-B	X	X		X (Receive)

* TIS-B, as specified herein, supports the ASSA and EVAcq applications only

The Surveillance and Broadcast Services System's functions (Aircraft/Vehicle, Link Specific Processing, Broadcast Services, ATC Automation) provide the ADS-B services that support ADS-B applications. Figure 2-1 shows the relationship between the principle and sub-system components. TIS-B and FIS-B services require all functions except ATC Automation. The ADS-B Rebroadcast (ADS-R) Service is a subset of the fundamental TIS-B Service.

- The Aircraft/Vehicle function is identified as the components located in the avionics section at the top of the illustration.
- The Link Specific function is identified as the air interfaces and 1090ES and UAT receive/transmit components located mid illustration.
- The Broadcast Services function is identified as the ground interfaces and associated TIS-B and FIS-B processors.
- ATC Automation.

Figure 2-1 Surveillance and Broadcast Services System



2.1 Services

The Surveillance and Broadcast Services provides four services, ADS-B, TIS-B, ADS-R, and FIS-B. These services enable ADS-B applications to be performed. The following sections describe the services in Surveillance and Broadcast Services in more detail.

2.1.1 Automatic Dependent Surveillance-Broadcast (ADS-B)

ADS-B equipped aircraft and vehicles broadcast their state vector (horizontal and vertical position, horizontal and vertical velocity) and other information over one of the link technologies approved for use in the FAA NAS, UAT or 1090ES. These ADS-B Message broadcasts are received by other aircraft in the vicinity of the transmitting aircraft as well as the ADS-B ground infrastructure. Aircraft equipped with the proper equipment receive the ADS-B Messages and process and display the information for use in the applications described in Sections 2.1.2 through

2.1.6. The ADS-B ground infrastructure processes the ADS-B Messages and formats them into ADS-B Reports that are provided to ATC for use in delivering separation assurance and other services in support of the ATC Surveillance application.

During NAS-wide deployment of ADS-B, aircraft will begin equipping with ADS-B avionics. These equipped aircraft will receive broadcast ADS-B Messages directly from other aircraft equipped with the same data link technology. Thus an aircraft equipped with a particular data link will have surveillance information on like-equipped aircraft. However, it will lack surveillance information on other aircraft in the vicinity that are not ADS-B equipped and those that are equipped with the other data link technology. The TIS-B and ADS-R Services address these shortfalls.

2.1.2 Traffic Information Service-Broadcast (TIS-B)

TIS-B provides the ability of ADS-B equipped targets to see those aircraft that are not equipped with ADS-B. The Surveillance and Broadcast Services ground infrastructure broadcasts TIS-B Messages for targets detected and reported by radar, or other surveillance systems, on both the UAT and 1090ES data links for reception by equipped aircraft. This permits the use of a subset of the air-to-air operations between equipped and non-equipped aircraft. TIS-B in conjunction with the ADS-R service will provide equipped aircraft the information needed for a complete picture of traffic in their vicinity. This TIS-B Service, as specified herein, supports the Enhanced Visual Acquisition and the Airport Surface Situational Awareness applications.

2.1.3 Automatic Dependent Surveillance-Rebroadcast (ADS-R)

As aircraft operating in the NAS may equip with either UAT or 1090ES data link technologies, the ground infrastructure will provide a service to rebroadcast ADS-B Messages received down one link back up the other link. This ADS-R Service permits aircraft and vehicles equipped with only a single data link to obtain a complete air traffic picture of all ADS-B equipped aircraft and vehicles.

2.1.4 Flight Information Service-Broadcast (FIS-B)

FIS-B provides the broadcast of weather and non-control, advisory information providing users valuable, near real-time aeronautical information, supporting safe and efficient operations. FIS-B products include, but are not limited to: Graphical and textual weather reports and forecasts, Special Use Airspace (SUA) information, NOTAMS, electronic pilot reports (E-PIREPS), and other similar meteorological and aeronautical information. FIS-B products, from both government and commercial sources, will be broadcast to aircraft from the ground on the UAT link only. In limited circumstances, aircraft will also broadcast FIS-B products. Aircraft derived products will be communicated in the ADS-B Message to other aircraft and to the ground.

2.2 Applications

Many ADS-B applications are in various stages of development. A subset was selected for near-term NAS implementation based on maturity and cost / benefits (see Table 2-1).

These applications fall into two categories: (a) ATC surveillance intended for automation, and (b) the rest of the applications intended for cockpit use. Figure 2-2 depicts the scope of the Surveillance and Broadcast Services system..

An abbreviated description for each near-term ADS-B application, taken from the NAS Automatic Dependent Surveillance-Broadcast Concept of Operations (CONOPS), is provided in following sections.

Table 2-2, derived from the Minimum Aviation System Performance Standards for Aircraft Surveillance Application (ASA MASPS RTCA DO-289), summarizes the minimum functional requirements on the receiving aircraft's CDTI for each of the applications. The requirements are stated in the ASA MASPS subparagraphs as noted in the section references included in Table 2.2-1.

Figure 2-2 Scope of Surveillance and Broadcast Services

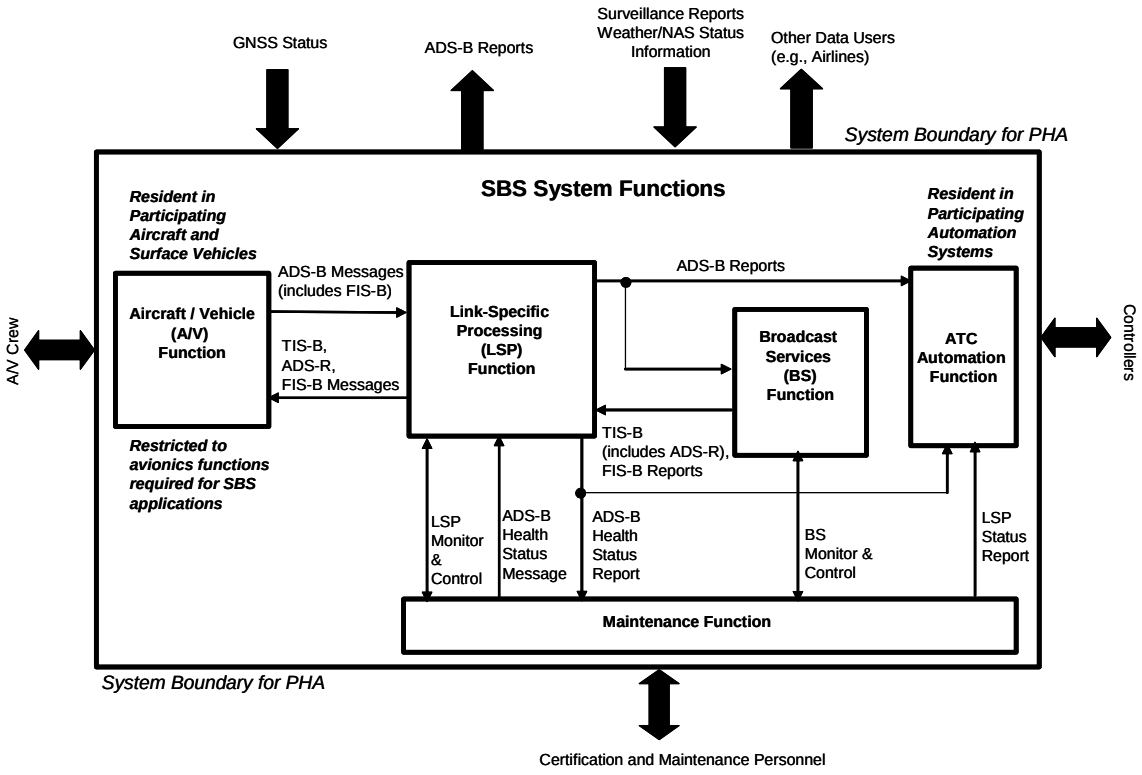


Table 2-2 Summary of CDTI Requirements for Near-Term Traffic Applications

	ASA-MASPS Section References	Features	Applications			
			EV Acq.	CD	FAROA, ASSA	EV App.
Display Elements	3.3.3.1.1.1	Display Range /Map Scale	R	R	R	R
	3.3.3.1.1.1.1	Reduced Display Range			R	
	3.3.3.1.1.1.2	Extended Display Range				
	3.3.3.1.1.1.3	Range / Map Scale Ref.	R	R	R	R
	3.3.3.1.1.2	Display Orientation	R	R	D	R
	3.3.3.1.1.3	Application-Specific Display Features				
	3.3.3.1.1.3.1	Airport Surface Map			R	
	3.3.3.1.1.3.2	Extended Runway Center Line and Final Approach Course			R	
	3.3.3.1.1.3.3	ANDS Indication		R		
	3.3.3.1.1.3.4	Low Level Alert disabled		R		
	3.3.3.1.1.3.5	Recommended Speed				
Symbols	3.3.3.1.2.1	Own-Ship Symbol	R	R	R	R
	3.3.3.1.2.2	Traffic Symbols – basic requirements	R	R	R	R
	3.3.3.1.2.3	Traffic Symbols – variations	R	R	R	R
	3.3.3.1.2.4	Selected Target	D	D	D	R
	3.3.3.1.2.5	Coupled Target				
	3.3.3.1.2.6	Traffic Information Quality	R	R	R	R
Misc.	3.3.3.1.3.1	Traffic Display Criteria	R	R	R	R
	3.3.3.1.3.2	Loss of Own-Ship Directionality	R	R	R	R
Traffic	3.3.3.1.4.1	Time of Applicability	R	R	R	R
	3.3.3.1.4.2	Traffic ID (Call Sign / Flight ID)		D	D	R
	3.3.3.1.4.3	Traffic Category	D	D	D	D
	3.3.3.1.4.4	Traffic Length / Width Codes			R	
	3.3.3.1.4.5	Traffic Horizontal Position	R	R	R	R
	3.3.3.1.4.6	Traffic Air / Ground Status	R	R	R	R
	3.3.3.1.4.7	Traffic Altitude (Relative or Actual)	R	R	R	R
	3.3.3.1.4.8	Traffic Vertical Rate Indicator	R	R	R	R
	3.3.3.1.4.9	Traffic Horizontal Velocity Vector		D		R
	3.3.3.1.4.10	Traffic Heading			R	
Selected Target	3.3.3.1.5.1	Selected Target Highlighting	D	D	D	R
	3.3.3.1.5.2	Selected Target ID	D	D	D	R
	3.3.3.1.5.3	Selected Target Category	D	D	D	R
	3.3.3.1.5.4	Selected Target Ground Speed	D	D	D	R
	3.3.3.1.5.5	Selected Target Range	D	D	D	R
	3.3.3.1.5.6	Selected Target Closure Rate	D	D	D	R
	3.3.3.1.5.7	Off-Display Selected Target Bearing	D	D	D	R
Alerting	3.3.3.1.6.1	Alerted Traffic Symbol		R		D
	3.3.3.1.6.2	Off-Display alerted Traffic Bearing Indicator		R		D
	3.3.3.1.6.3	Application Alerts		R		D

R = Required; D = Desired
Source: RTCA DO-289 Table 3-19

2.2.1 ATC Surveillance

The goal of this application is to use Surveillance and Broadcast Services information as a qualified surveillance source to provide ATC services throughout the NAS. ATC will use ADS-B surveillance information in the same manner current dependent/cooperative surveillance system information is used e.g., to assist aircraft with navigation, to separate aircraft, and to issue safety alerts and traffic advisories. Secondarily, the ADS-B surveillance

information will be used as a back-up surveillance system during loss of radar-based surveillance, and it will be used to enhance the quality of existing radar-based surveillance information for ATC automation system functions e.g., tracking, MSAW, Conflict Alert, and Mode-C Intruder Alert. The targeted implementation areas include terminal, en route, off-shore, and oceanic domains. ADS-B surveillance will allow ATC to apply separation between ADS-B-to-ADS-B and ADS-B-to-radar based targets.

2.2.2 Weather and NAS Status Situational Awareness

The primary objective of this application is to provide the flight crew with improved access to weather information and aeronautical data. Many types of information are not suitable for conveyance by voice, such as graphical weather products. In the transfer of this information by voice, considerable detail is lost and the time and attention devoted to conveying the information is lengthy and diverts the pilot from primary flight duties. The application will improve access to textual and graphical weather and other aeronautical information (i.e., METAR, TAF, SIGMENT, PIREP, NOTAM, NEXRAD, Special Use Airspace status, etc) by use of a cockpit-based display.

2.2.3 Enhanced Visual Acquisition

The objective of this application is to provide the flight crew enhanced traffic situational awareness in controlled or uncontrolled airspace. The application uses a cockpit display to assist the out-the-window visual acquisition of air traffic. Flight crews will refer to the display during the instrument scan to supplement visual observations. The display can be used to either initially detect an aircraft or to receive further information on an aircraft that was reported by ATC. The application provides the flight crew with the relative range, altitude, and bearing of other aircraft.

2.2.4 Enhanced Visual Approach

The Enhanced Visual Approach application is an extension of the current visual approach procedure, entailing the use of an in-cockpit display of traffic information (CDTI) to assist the flight crew with achieving and maintaining visual contact with relevant traffic. This application is intended to enhance successive approaches for aircraft cleared to maintain visual separation from another aircraft on the approach. The goal is to maintain visual approach procedure operation arrival rates even during periods of reduced visibility or obstructions vision (haze, fog, sunlight, etc).

To achieve these objectives, flight crews will be supported by a CDTI of nearby traffic. This will provide continually updated identity and position information to assist the flight crew with achieving and maintaining visual contact with relevant traffic. Additional information such as range and speed will be provided to assist flight crews in maintaining an appropriate distance from the preceding aircraft. The display may also be used to monitor aircraft on parallel approaches. The aircraft may be either ahead and approaching the same runway (i.e. in-trail), or ahead and approaching an adjacent closely spaced parallel runway. Flight crews must maintain visual contact with the preceding aircraft (i.e., the aircraft ahead) during visual approaches. The CDTI provides traffic position, spacing, flight identification, closure rate or ground speed, and ground track information to assist the flight crew in maintaining an appropriate distance from the preceding aircraft.

2.2.5 Final Approach and Runway Occupancy Awareness

The objective of this application is to increase the flight crew's awareness of aircraft and vehicles on or near the runway surface or on final approach (up to approximately 1000 feet above ground level). Flight crews will use a cockpit display that depicts the runway environment, their aircraft position, and other traffic, to help determine runway occupancy and to help support go-around decision-making.

2.2.6 Airport Surface Situational Awareness

The objective of this application is to reduce the potential for deviations, errors, and collisions through an increase in flight crew situational awareness while operating an aircraft on the airport surface. Flight crews use a cockpit display to increase awareness of their and other traffic positions on the airport surface, e.g., runways, taxiways, and ramps. Additionally, the display may be used to determine the position of ground vehicles, e.g., snow plows, emergency vehicles, tugs, follow-me vehicles, baggage vehicles, fuel trucks, and catering trucks.

2.2.7 Conflict Detection

The objective of the application is to provide alerting and relevant traffic information to help the flight crew identify conflicts with other aircraft based on current flight states and intentions. Aircraft equipped with a cockpit display have the capability to display aircraft location and intent. More than simply displaying traffic, the application will alert pilots of developing conflicts. The long surveillance range afforded by ADS-B will enable alerts to be issued in time to solve the conflict with minimum disruption to the flight path.

2.3 Concept of Operations

The purpose of the Surveillance and Broadcast Services functions are to provide ADS-B, ADS-R, TIS-B, and FIS-B services. These broadcast services provide new or improved operational capabilities. Service providers will use the new surveillance capability to provide ATC services. Users will use the surveillance and broadcast services capability to support flight operations.

The complete system Concept of Operations is contained in Attachment 1.

2.3.1 NAS Service Providers

The Surveillance and Broadcast Services will provide service providers with new or improved surveillance capability. ADS-B surveillance information will provide the ability to use radar-like air traffic services in areas not covered by primary or secondary radar surveillance, will supplement or improve surveillance information in existing radar coverage areas, and may provide cost effective replacement or improvement to existing surveillance technologies used for airport surface, terminal, and en route air traffic control operations. Service Providers will use the new operational enhancements to improve safety, capacity, and efficiency in the following manner:

- ***To Improve Surveillance.*** ADS-B information will provide airspace and surface surveillance in areas not currently served. The high accuracy and greater update rate ADS-B surveillance provides will supplement and improve existing surveillance information.
- ***To Improve Air Traffic Control Automation and Safety Functions.*** The information provided by ADS-B will improve surveillance and automation system performance, including automation safety functions such as conflict and low altitude alerting
- ***To Improve Separation Services.*** ADS-B will support surveillance-based separation standards in non-radar coverage areas. High accuracy ADS-B surveillance information will facilitate the use of a common separation standard for all service domains and may lead to reduced separation standards in select situations.
- ***To Improve Planning and Traffic Flow Management Functions.*** The ADS-B surveillance (message set elements) provides accurate, real-time information for traffic flow management, fleet management, and other planning functions.

2.3.2 NAS Users

Users will be provided cockpit-based surveillance and near real-time access to aeronautical flight information. In the near term, user situational awareness in both visual meteorological conditions (VMC) and instrument meteorological conditions (IMC) will be enhanced. Flight crews operating aircraft in-flight (controlled or uncontrolled airspace) or on the airport surface will have the capability to detect conflicts or hazards created by aircraft, obstacles, weather areas, airspace restrictions, and airport surface vehicles. In the long-term end-state environment; select spacing, sequencing, and separation tasks may be performed by qualified and certified aircrews/aircraft within defined criteria and/or in designated situations or areas. Depending on the availability of ADS-B services, level of accuracy, and type of application, users will use the new operational enhancements to improve safety and efficiency in the following manner:

- ***To Enhance Situational Awareness.*** These are ADS-B-enabled applications will enhance the pilot's knowledge of the weather, NAS status, and the surrounding traffic situation, both in the air and on the airport surface. No changes in separation tasks or responsibilities are required.

2.4 Functional Analysis

The Surveillance and Broadcast Services can be logically divided into five major functions (see Figure 2-2):

1. Aircraft/Vehicle Function
2. Link-Specific Processing (LSP) Function
3. Broadcast Services (BCS) Function
4. ATC Automation Function
5. Maintenance Function

The first four functions are operational, while the maintenance function provides for the control and monitoring of the operational functions. Note that only the operational functions are listed in Table 2-1, as the maintenance function supports the services and applications in an indirect manner. The Aircraft/Vehicle function resides in participant aircraft and surface vehicles. The ATC automation function resides in participant automation systems. The Link-Specific processing, broadcast services, and maintenance functions form the ADS-B ground infrastructure.

The Surveillance and Broadcast Services receives surveillance reports, from various NAS systems, to support the TIS-B service and weather and NAS status information, from government and commercial sources, to support the FIS-B service. The Surveillance and Broadcast Services distributes ADS-B Reports to authorized user systems. The status of the GPS constellation is also an input to the Surveillance and Broadcast Services to determine degraded operations on an outage within this constellation.

The complete system functional analysis is contained in Attachment 2.

Figure 2-3 Top-Level Functional Block Diagram for SBS System

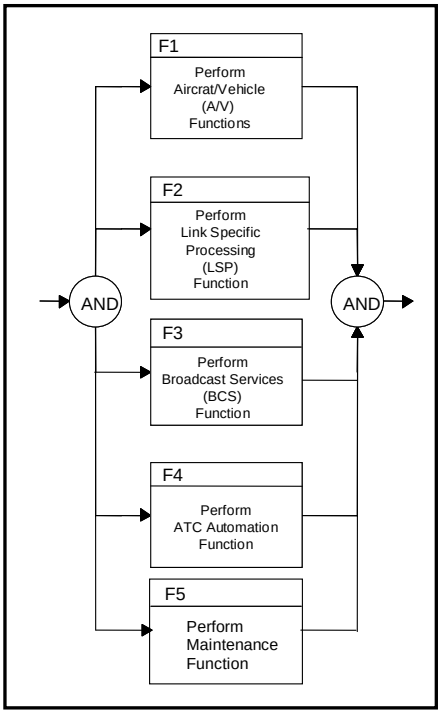


Figure 2-4 Top-Level N^2 Diagram for SBS System

External Function	- UTC -Own Position Data - Velocity Data - Aircrew Input - Barometric Altitude - Barometric Vertical Rate - Identification Data - Airport Maps	- UTC	UTC - FIS-Products, - Radar Meas. -Multilat & Surface Data -Surveillance Status -Airport Maps	- UTC, - Flight Plan Information -Radar Meas. -GNSS Status	-Control Parameters
- In-Cockpit Application Information (E.g., traffic position, conflict detection alerts, weather information)	**F1** **Perform Aircraft/Vechicle (A/V) Function**	- ADS-B Message (1090ES as DF17, UAT)			
	- TIS-B Message, (1090ES as DF 18, UAT) - FIS-B Message (UAT), -ADS-R Message (1090ES as DF 18, UAT as TIS-B)	**F2** **Perform Link Specific Processing (LSP) Function**	- ADS-B Report,	-ADS-B Report - ADS-B Health Status Report (F2)	-LSP Monitored Parameters - ADS-B Health Status Report
- Flight Monitoring Data		- TIS-B Report (includes ADS-R) - FIS-B Report,	**F3** **Perform Broadcast Service (BCS) Function**	-	- BCS Monitored Parameters
- ATC Surveillance Application Information (E.g., aircraft position, conflict alerts, MSAWs,)			- Flight Plan Information*	**F4** **Perform ATC Automation Function**	
-Monitored Parameters		- LSP Control Parameters - ADS-B Health Status Message	- BCS Control Parameters	-LSP & BCS Status Report	**F5** **Perform Maintenance Function**

2.4.1 F1 - Aircraft/Vehicle (A/V) Function

The Aircraft/Vehicle includes a transmit capability, to support the ATC Surveillance application, and a receive capability, to support the applications in Section 2.2. All aircraft require the transmit capability to participate in the seven applications defined in this document. For aircraft/vehicle operators desiring to conduct the air-to-air applications, the receiver capability is also required.

2.4.1.1 A/V ADS-B Transmit Capability

The Aircraft/Vehicle function is the source of ADS-B information. The function derives state vector information, using GNSS or other navigation sources, and determines associated integrity and accuracy indicators. The Aircraft/Vehicle function also ascertains altitude information from a qualified pressure altitude source. The function collects other ownship data, potentially including weather related measurements, and provides a means for crew input of additional information, such as aircraft identification data. The aircraft/vehicle function encodes and broadcasts ADS-B Messages, conveying the collected information.

2.4.1.2 A/V ADS-B Receive Capability

The Aircraft/Vehicle function receives and decodes ADS-B Messages transmitted by other Aircraft/Vehicles equipped with the same data link and TIS-B and ADS-R Messages transmitted by the ADS-B LSP Function. Aircraft/Vehicle functions equipped with the UAT data link additionally receive and decode FIS-B Messages transmitted by the LSP Function. The Aircraft/Vehicle function processes and displays the information conveyed in received messages.

2.4.2 F2 - Link Specific Processing Function

The LSP Function provides the Surveillance and Broadcast Services transmit/receive functionality on the ground. This function receives ADS-B Messages from equipped aircraft and surface vehicles, formats the associated ADS-B Reports, and distributes them to ATC Automation, the BCS function, and other authorized users. LSP transmits TIS-B, ADS-R, and FIS-B Messages as directed by the BCS Function. This Function supports all services and applications.

2.4.3 F3 - Broadcast Services Function

The BCS function tracks, filters, and applies quality indicators to surveillance reports from external sources and ADS-B Messages from the LSP Function. Broadcast Services generates TIS-B and ADS-R Reports for transmission as TIS-B and ADS-R Messages by LSP. The BCS Function additionally processes weather and NAS status data from external sources and generates applicable FIS-B Reports for transmission as FIS-B Messages by LSP. This function supports TIS-B, ADS-R, and FIS-B Services, but is not required for ADS-B. It supports all applications except ATC Surveillance.

2.4.4 F4 - ATC Automation Function

The ATC automation function uses ADS-B surveillance data much like it uses radar system surveillance information. The function supports environments with ADS-B Surveillance only as well as those having both ADS-B and radar surveillance. ATC Automation validates the position information provided in ADS-B Reports by comparing it with reports from other surveillance sources, as available. The function associates the ADS-B Report data with filed flight plans, creates and updates tracks, and displays target and emergency information to ATC Controllers. ATC Automation performs safety function processing, including Minimum Safe Altitude Warning (MSAW) and Conflict Alert (CA), using ADS-B and radar data, as available, and displays any associated alerts.

2.4.5 F5 - Maintenance Function

The maintenance function provides for the control and monitoring of the ADS-B ground infrastructure operational functions, Link-Specific Processing and Broadcast Services. Control includes the setting of configuration items, downloading new software, requesting the read back of monitored parameter values, and any other actions necessary to control the operation and support the maintenance of the system. Monitoring includes the generation of alerts and alarms as well as the injection of Health Status Messages (test targets) into the LSP Function, and any other monitoring activities necessary to support the operation and maintenance of the system. The maintenance function uses information gathered in monitoring the system to generate status reports, containing high-level alarm and alert information and system counts, such as number of ADS-B Messages received, number of TIS-B Reports generated, etc. and distributing them to the ATC automation function.

The maintenance function additionally monitors ADS-B receptions and the GPS constellation to analyze coverage and identify potential quality issues with Aircraft/Vehicle performance. The function provides an interface to systems engineers and technicians for use in control and monitoring of the ADS-B System.

3. PROPOSED CHANGE TO THE NAS

Changes expected to the NAS as part of the Surveillance and Broadcast Services Program include:

- ATC use of ADS-B surveillance information for separating aircraft in all air traffic domains
- Modifications to the existing surveillance and telecommunications infrastructure at Juneau to support the ATC Surveillance Application
- Modifications to automation system platforms to accept, process, and display ADS-B surveillance data in all air traffic domains
- Deployment of additional telecommunications infrastructure in the Gulf of Mexico to support the ATC Surveillance Application in En Route and Offshore (Helicopter) domains
- Expansion of the existing prototype TIS-B / FIS-B infrastructure (a.k.a., East Coast Plus) for data collection and analysis purposes (Note: This infrastructure was initially deployed under Safe Flight 21)
- Development and deployment of essential broadcast services (i.e., commissioned TIS-B / FIS-B capabilities) to support in-cockpit situational awareness applications (Note: The commissioned TIS-B / FIS-B capabilities are distinct from the prototype infrastructure and may not consist of the same design solution)
- Avionics system requirements needed to support each application (Note: Avionics manufacturers and airlines are responsible for complying with safety requirements. However, the FAA is responsible for defining avionics-related safety requirements, via rulemaking, and certifying that the avionics' designs and installations are safe)
- Mandated equipage with ADS-B transmit capability to support the ATC surveillance application
- Voluntary equipage with and flight crew use of other avionics to support Enhanced Visual Acquisition, Enhanced Visual Approach, Conflict Detection, Final Approach and Runway Occupancy Awareness, Airport Surface Situational Awareness, and Weather and NAS Status Situational Awareness applications

Air traffic control facilities will use ADS-B surveillance information (airborne and airport surface) for air traffic control operations and services including situational awareness, separation assurance, and improved automation system safety functions. Other authorized facilities (traffic flow management, ramp control, airline operations center, etc) may use ADS-B surveillance information to track flight activities and optimize operations. The inherent accuracy and high update rate of ADS-B will provide service providers and user improvements in safety, capacity, and efficiency.

ADS-B surveillance data broadcast by aircraft in-flight is used by aircraft equipped with Cockpit Display of Traffic Information (CDTI, see Appendix B) to support cockpit-based applications including situational awareness and separation assurance (conflict detection and in the future, conflict management). Aircraft and vehicles operating on the airport surface use ADS-B surveillance information for situational awareness. Flight safety benefits when pilots can determine airborne and airport surface hazards.

Providing real-time, in- cockpit access to traffic and aeronautical information (weather, NOTAMS, Airspace status, etc) will improve aviation safety, capacity, and efficiency. Pilots will have the ability to determine the type, intensity, and extent of weather areas provided by NEXRAD, TDWR, ITWS, and other weather sensors. Also, aircrews will be able to access NOTAM information and Special Use Airspace status. This will enable pilots to avoid the impacts from restricted/closed areas or NAS resource outages (e.g., NAVAIDS and runways), and make timely adjustments to their route/flight path. Providing knowledge of changing conditions as they occur during the flight progress will improve pilot situational awareness and overall aviation safety and system capacity.

Rulemaking activities are planned to require aircraft equipage with ADS-B transmit capability to support the ATC Surveillance application.

Use of the Traffic / Flight Information Broadcast Services and performing the following applications is voluntary: NAS and Weather Situational Awareness, Enhanced Visual Acquisition, Enhanced Visual Approaches, Final Approach and Runway Occupancy Awareness, Airport Surface Situational Awareness, and Conflict Detection. Equipping with the CDTI avionics necessary to support these applications is also voluntary.

Proposed locations for deploying or updating the Surveillance and Broadcast Services System's ADS-B and TIS-B/FIS-B ground infrastructure include the Gulf of Mexico, Louisville, and Juneau. These locations are subject to change based on the refinement of the Surveillance and Broadcast Services Program business case.

3.1 Implementation Strategy

3.1.1 Phased Deployment

The Surveillance and Broadcast Services will be implemented in a phased approach consisting of program segments. Initial segments will consist of SBS infrastructure deployments for targeted locations to support select applications. Later segments will be used to expand the system NAS-wide and eventually introduce higher system functionality and for more complex applications. The general time interval for each segment is as follows:

Segment 1: FY 2007 – 2010

Segment 2: FY 2010 – 2014

Segment 3: FY 2015 – 2020

Segment 4: FY 2021 – 2025

3.1.2 Segment Applications

The following ADS-B applications have been selected as the initial group for implementation based on their application's maturity, cost and operational benefits, and understanding of the performance requirements.

- ATC Surveillance
- Enhanced Visual Acquisition
- Enhanced Visual Approach
- Weather and NAS Status Situational Awareness
- Conflict Detection
- Final Approach and Runway Occupancy Awareness
- Airport Surface Situational Awareness

Other ADS-B applications (see CONOPS Appendix C) will be considered for potential future implementation based on the same criteria and the updated FAA ADS-B deployment strategy.

3.2 Maintenance Concept

The Surveillance and Broadcast Services maintenance concept must address both the ADS-B avionics and the ground infrastructure. Surveillance and Broadcast Services ground infrastructure maintenance may be provided by government personnel or commercial enterprises.

Avionics

Avionics will undergo periodic maintenance checks and will be subject to corrective maintenance as needed to ensure continued airworthiness.

Data Link Processor and Broadcast Server

The Data link Processors and Broadcast Servers will have Built-In-Test/Fault Isolation Test (BIT/FIT) and provide adjustable parameters to support maintenance of the systems. Both local and remote monitoring and control will be offered for maintenance personnel visiting the sites and for maintenance personnel stationed at centralized monitoring equipment, respectively. The systems will support periodic and corrective maintenance without disrupting normal system operation.

ATC Automation

Legacy ATC automation system maintenance concepts, documented in automation system maintenance manuals, are not expected to change.

4. ANALYSIS METHODOLOGY

The sections below describe the general approach used to develop this PHA in accordance with the FAA System Safety Management Program (SSMP), Revision 10 and the FAA System Safety Handbook, Revision 7.

Hazard analysis techniques employed in this analysis include:

- Functional analysis
- Fault tree analysis
- What-if scenario analysis
- A review of historical safety experience based on subject matter expert interviews

Hazards were identified according to the following categories:

- Hazards due to a loss of data
- Hazards due to inaccurate, corrupted, latent, or otherwise misleading data (Hazardously Misleading Information (HMI))
- Transitional hazards specific to a phase in the system's lifecycle (e.g., mixed equipage environment in which only some aircraft are ADS-B equipped)
- "Interoperability" hazards related to the impacts the new system will have on existing NAS equipment (e.g., impact of increased utilization of the 1090 MHz link on aircraft transponder occupancy and TCAS)
- Hazards related to the environment in which the system must operate

4.1 General Assumptions and Caveats

The ground rules and assumptions applicable to this analysis are as follows:

- Safety is defined as freedom from unacceptable risk, where unacceptable risk includes, at a minimum, those risks assessed to be high
- Without appropriate contingency, loss control, recovery, or damage control, lower risks could develop into higher risk
- A set of hazard controls has been identified to mitigate particular scenarios. It is expected that risk will increase should the recommendations, hazard controls, and precautions not be followed or implemented. Some controls may not be totally effective in all cases. An assumption of hazard control effectiveness has been made when residual risks were characterized within this analysis.
- The analysis is not all-inclusive; unknown risks are present within any operation
- Security and Occupational Safety and Health Assessment (OSHA) risks are outside the scope of this analysis per the SMS. It should be noted that security risks will be addressed in the SBS Program Security Certification and Authorization Package (SCAP). Identification, assessment, mitigation, and tracking of OSHA-related risks will be coordinated with the FAA's Environmental, Occupational Health and Safety (EEOSH) Services organization.
- Whenever fault trees were not provided, "OR" gates between the hazard causes can be assumed.
- When assumptions are made concerning the system states for an application, they are documented as recommended controls in accordance with the SSMP.
- There is no distinction made in the analysis between UAT or 1090, because requirements for both 1090 and UAT are identical per ADS-B MASPS (DO-242).
- Many of the existing controls cited in the hazard tables in Volume II are extracted from the Final Program Requirements for Surveillance and Broadcast Services, Version 1.0, dated May 9, 2006. The Final

Program Requirements (fPR) are validated but not implemented and verified. The SBS Program plans to derive system requirements specifications from the fPR and is using a requirements management tool to track and trace all requirements. fPR requirements designated as existing controls in the PHA will be denoted as such in the SBS Program's requirements management tool to ensure that any proposed changes to fPR requirements and derived specifications are examined for safety impacts.

- Although the system's lifecycle is not explicitly defined in the Surveillance and Broadcast Services Final Program Requirements Document, a 20-year life cycle is assumed

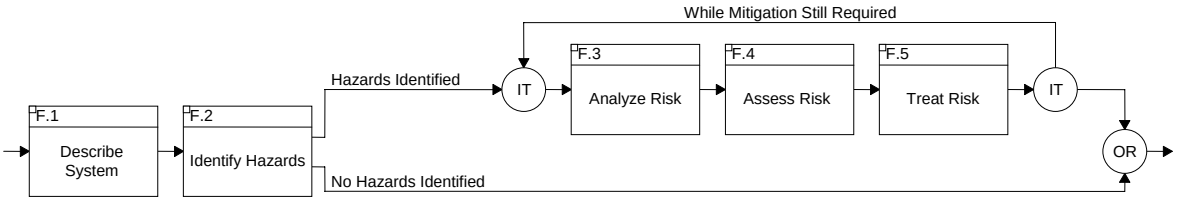
Application-specific and system state assumptions are contained in Volume II of the SBS PHA.

4.2 Hazard Model

4.2.1 Overview

Hazards, worst credible system states, and potential effects were identified in accordance with Section 4.0 of the SSMP. Fault trees are included in Volume III.

Figure 4-1: Hazard Analysis Model



Source: ATO-P

4.2.2 Definitions

Causes

The causes are events that lead to a hazard or hazardous condition. Causes can occur by themselves or in combinations and can be technical and/or procedural in nature.

Hazard

The hazard is the adverse event that occurs as a result of the cause(s). The SSH defines a hazard as "anything real or potential, that could make possible or contribute to an accident. The hazards, when they occur in the worst credible system states, result in the harm (effects of the hazard in the worst credible system state). Hazards are composed of one or more causes.

System State

In the SEM and the SSH, a system is defined as a "composite of people, procedures, materials, tools, equipment, facilities, and software operating in a specific environment to perform a specific task or achieve a specific purpose, support, or mission requirement." Given this definition, the system state is an expression of the various conditions, characterized by quantities or qualities, in which the system can exist. System state can be described in operational/procedural terms (e.g., Visual Flight Rules (VFR) vs. Instrument Flight Rules (IFR), Instrument Landing System (ILS) approach, etc.), conditional (e.g., Instrument (IMC) vs. Visual Meteorological Conditions (VMC), low altitude, rough terrain, etc.), or physical terms (Electromagnetic Environment Effects, Precipitation, low rotor speed, low hydraulic pressure, high impedance, etc.).

Effects

The effect (or harm) is a description of the potential outcome of the hazard if it occurs in the defined system state.

Severity

Severity is determined by the worst credible potential outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects must be considered. Severity is independent of likelihood.

Likelihood
Likelihood is an estimation for each hazard of how often the "effects or harm" will occur, considering the worst case system state. The procedure for assessing likelihood is as follows:

1. First, determine how often the hazard can be expected to occur. This can be a quantified or a qualified estimate. Usually it is a function of the likelihood of the combinations of the cause(s). Sometimes this can be determined by evaluating incident or accident databases to see how often the hazard has been recorded in the field.
2. Make an estimate of the likelihood of the worst case system state. This estimate also can be quantified or qualified.
3. For the effects to be manifested in the worst case, both the hazard and the worst case system state must occur at the same time. An estimate of the likelihood of this can be made by multiplying the likelihood of the hazard occurring and the likelihood of the worst case system state occurring (assuming the events are independent).

Risk / Risk Assessment Code (RAC)
Risk is the composite of severity and likelihood of the outcome/effect (or harm) of the hazard in the worst credible system state. The risk is expressed as a Risk Assessment Code.

Initial Risk
Initial risk is the severity and likelihood of a hazard when it is first identified and assessed. It is used in the beginning or very preliminary stages of a decision, program or analysis. Initial Risk is determined by considering both verified requirements and assumptions made about system state. Once the initial risk is established it not changed. Typically, Initial Risk is an assessment formed and kept within the purview of system safety.

Current Risk
Current Risk is the predicted severity and likelihood of a hazard as it exists currently, using both validated requirements and verified requirements. Current Risk may change over time based on actions taken by the decision maker that relate to the validation and/or verification of the requirements or controls associated with the hazard.

Residual Risk
Residual Risk is the risk that remains after all requirements have been implemented or exhausted and all requirements have been verified. Only verified requirements or controls can be used to assess Residual Risk. When conducting an analysis, Predicted Residual Risk is the term used prior to formal verification of requirements or controls based on the assumption that validated and recommended safety requirements will be verified.

Predicted Residual Risk
Predicted Residual Risk is the risk status predicted to occur when recommended controls or requirements are both validated and verified.

Safety Requirements
Safety requirements are requirements used to control hazards. These requirements are documented in the program's SRVT. All safety requirements must be identified as such in the program's requirements documents. Changes to safety requirements must be reported to the program's SRMP and, if necessary, to the ATO SSWG. Recommended safety requirements are defined as requirements that the safety engineer determines to have the potential to mitigate a hazard but are not yet validated requirements. They can also be referred to as Candidate Safety Requirements until they are validated by the IPT/PO. Once they have been validated, the recommended safety requirements become validated safety requirements. Recommended safety requirements associated with a hazard description are maintained in the NAS Hazard Tracking System (HTS) until all of the candidate safety requirements have been validated and verified.

4.3 Risk Determination

In order to determine the risk associated with each hazard, two factors were analyzed: the severity of consequence and the likelihood of occurrence. The tables below include the definitions for the range of severity and likelihood classifications as specified in the SSMP.

For more information regarding these definitions, refer to FAA Advisory Circular 25.1309-1A, *System Design Analysis*, 06-21-88.

Table 4-1: Severity Definitions

Effect on:	Hazard Severity Classification				
	No Safety Effect (5)	**Minor (4)**	**Major (3)**	**Hazardous (2)**	**Catastrophic (1)**
General		Does not significantly reduce system safety. Required actions are within operator's capabilities. Includes (see below):	Reduces the capability of the system or operators to cope with adverse operating condition to the extent that there would be a (see below):	Reduces the capability of the system or the operator's ability to cope with adverse conditions to the extent that there would be a (see below):	Total loss of systems control such that (see below):
Air Traffic Control	Slight increase in ATC workload	Slight reduction in ATC capability, or significant increase in ATC workload	Reduction in separation as defined by a low/moderate severity operational error (as defined in FAA Order 7210.56), or significant reduction in ATC capability	Reduction in separation as defined by a high severity operational error (as defined in FAA Order 7210.56), or a total loss of ATC (ATC Zero)	Collision with other aircraft, obstacles, or terrain
Flying Public[1]	- No effect on flight crew - Has no effect on safety -Inconvenience	- Slight increase in workload - Slight reduction in safety margin or functional capabilities - Minor illness or damage - Some physical discomfort	- Significant increase in flight crew workload - Significant reduction in safety margin or functional capability - Major illness, injury, or damage - Physical distress	- Large reduction in safety margin or functional capability - Serious or fatal injury to small number - Physical distress/ excessive workload	Outcome would result in: - Hull loss - Multiple fatalities

Table 4-2: Likelihood Definitions

	NAS Systems			Flight Procedures	ATC Operational	
		Qualitative			Periodicity	
	Quantitative	**Individual Item/System**	**ATC Service/ NAS Level System**		**Per Facility**	**NAS-wide**
Frequent A	Probability of occurrence per operation/ operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 months for an item	Experienced continuously in the system	$P \geq 1 \times 10^{-5}$	Expected to occur more than once per week	Expected to occur more than every 1-2 days
Probable B	Probability of occurrence per operation/ operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system		Expected to occur about once every month	Expected to occur about several times per month
Remote C	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in life cycle of an item	Expected to occur numerous times in system life cycle	$10^{-5} > P \geq 10^{-7}$	Expected to occur about once every year	Expected to occur about once every few months
Extremely Remote D	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system's life cycle	$10^{-7} > P \geq 10^{-9}$	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years
Extremely Improbable E	Probability of occurrence per operation/ operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	$P < 10^{-9}$	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years

Note: Segment 1 of the SBS Program is being implemented at select facilities as opposed to a NAS-wide level. In addition, many hazard causes are attributed to aircraft avionics malfunctions and failures that are considered at the "individual item / system" level.

The risk is then determined from the Risk Assessment Matrix shown in Table 3. Severity is shown in the left column, and likelihood is the first row.

Table 4-3: Risk Assessment Matrix

	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

High
Medium
Low

* Unacceptable with single point and common cause failures

Table 4 shows the criteria for risk acceptability. A high risk is considered unacceptable, and must be mitigated or controlled to reduce the risk to a lower category. Medium and low risk acceptability is also defined in the table.

Table 4-4: Risk Acceptance Criteria

	High Risk	Tracking in a Hazard Tracking Risk Resolution System is required until the risk is reduced or accepted at the appropriate management level.
	Medium Risk	Acceptable with review by the appropriate management level. Tracking in a Tracking Risk Resolution System is required.
	Low Risk	Acceptable without review. Entry in a Tracking Risk Resolution System is required; no tracking is required.

SURVEILLANCE AND BROADCAST SERVICES PROGRAM
SEGMENT 1

SAFETY RISK MANAGEMENT DOCUMENT:
PRELIMINARY HAZARD ANALYSIS

VOLUME II – HAZARD ANALYSIS

SEPTEMBER 18, 2006

VERSION 1.0

DOCUMENT CHANGE HISTORY

VERSION	DATE	DESCRIPTION OF CHANGES

TABLE OF CONTENTS

5. HAZARD ANALYSIS....4

5.1 ATC SURVEILLANCE APPLICATION....4
5.1.1 Ground Rules and Assumptions....4
5.1.2 ATC Surveillance Hazards....8
5.2 IN-COCKPIT APPLICATIONS....28
5.2.1 General....29
5.2.2 Enhanced Visual Acquisition....30
5.2.3 Enhanced Visual Approach....40
5.2.4 Airport Surface Situational Awareness (ASSA)....49
5.2.5 Final Approach and Runway Occupancy Awareness (FAROA)....56
5.2.6 Conflict Detection....65
5.2.7 Weather and NAS Status Situational Awareness....78

LIST OF TABLES

TABLE 5-1: ATC SURVEILLANCE PRELIMINARY HAZARDS....8
TABLE 5-2: GENERAL IN-COCKPIT APPLICATION PRELIMINARY HAZARDS....29
TABLE 5-3: ENHANCED VISUAL ACQUISITION PRELIMINARY HAZARDS....30
TABLE 5-4: ENHANCED VISUAL APPROACH PRELIMINARY HAZARDS....40
TABLE 5-5: ASSA PRELIMINARY HAZARDS....49
TABLE 5-6: FAROA PRELIMINARY HAZARDS....57
TABLE 5-7: CONFLICT DETECTION PRELIMINARY HAZARDS....66
TABLE 5-8: WEATHER AND NAS STATUS SITUATIONAL AWARENESS PRELIMINARY HAZARDS....79

5. HAZARD ANALYSIS

The hazard tables contained in this section shows traceability from:

- System functional analysis to hazard causes,
- Existing controls to hazard causes, and
- Recommended safety requirements and objectives to hazard causes

For example, in hazard H1, cause C1 (LSP function failure) traces to function F2 in the functional analysis as annotated in square brackets. Existing control 3.2.1.1(ADS-B Service Availability) and recommended safety objective J52 concerning design assurance both trace to cause C1.

5.1 ATC Surveillance Application

ATC Surveillance applies to the following airspace domains: surface, terminal, en route, oceanic, and offshore / helicopter operations. ADS-B-based ATC surveillance in the offshore domain is restricted to helicopter operations between 1500 and 7000 feet in the Gulf of Mexico. Higher altitude traffic operating offshore is addressed under en route or oceanic domains, depending on separation criteria and availability of radio communications.

5.1.1 Ground Rules and Assumptions

Scope

- Hazards are only presented for the terminal domain. It is assumed that the terminal domain accounts for the worst-case system state elements present in any airspace domain, including high density traffic and separation standards among others.
- Some aircraft are currently equipped with ADS-B or UAT avionics. Impacts of legacy ADS-B transmitter performance are not evaluated in this analysis (i.e., DO-260 vs. DO-260A compliance).
- Potential, future decommissioning of legacy surveillance equipment was not analyzed in this PHA. No decommissioning plans were established as part of the SBS Program at the time of this analysis.
- Hazards which may be unique to a particular automation system design are not identified in this analysis.

Other

- Functional failures are cited as causes for certain hazards (e.g., automation function failure). These functional failures are defined as the total loss of the indicated function as opposed to malfunction.
- Hazards that entail Hazardously Misleading Information (HMI) are broken out by type of HMI, such as inaccurate position, inaccurate altitude, etc.

System States

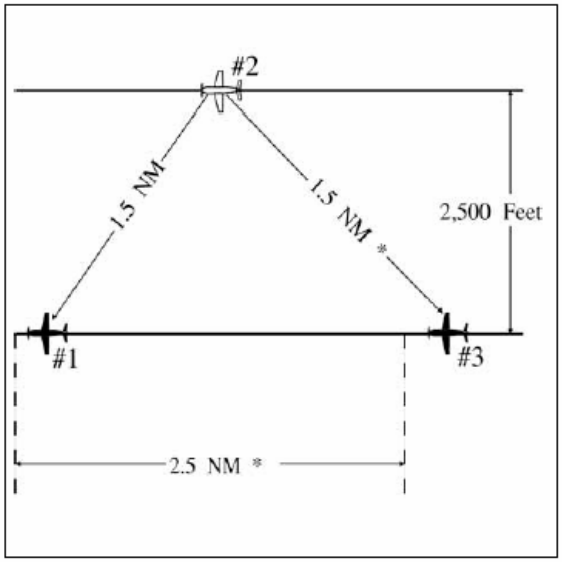
- State 1: 2.5 nmi longitudinal and 1.5 nmi diagonal separation for aircraft on parallel, dependent ILS approach courses separated by 2,500 ft
  - State 1 is based on the following excerpt from FAA Order 7110.65P, Section 5-9-6:

    5−9−6. PARALLEL DEPENDENT ILS/MLS APPROACHES TERMINAL
    a. Apply the following minimum separation when conducting parallel dependent ILS, MLS, or ILS and MLS approaches:
    1. Provide a minimum of 1,000 feet vertical or a minimum of 3 miles radar separation between aircraft during turn on.
    2. Provide a minimum of 1.5 miles radar separation diagonally between successive aircraft on adjacent localizer/azimuth courses when runway centerlines are at least 2,500 feet but no more than 4,300 feet apart.

    EXAMPLE−
    In FIG 5−9−6, Aircraft 2 is 1.5 miles from Aircraft 1, and Aircraft 3 is 1.5 miles or more from Aircraft 2. The resultant separation between Aircrafts 1 and 3 is at least 2.5 miles.

FIG 5−9−6

Parallel Dependent ILS/MLS Approaches



EXAMPLE−

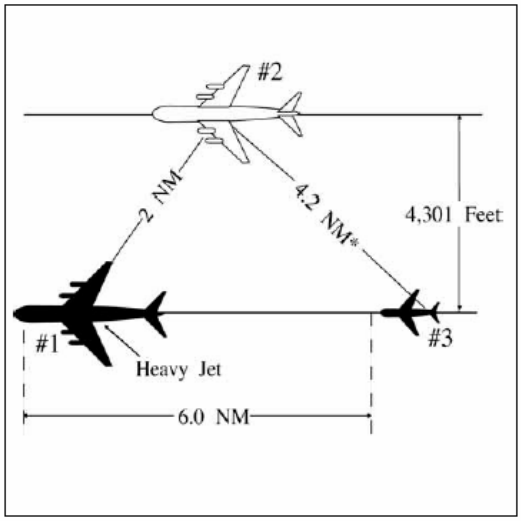
In FIG 5−9−6, Aircraft 2 is 1.5 miles from Aircraft 1, and Aircraft 3 is 1.5 miles or more from Aircraft 2. The resultant separation between Aircrafts 1 and 3 is at least 2.5 miles.

3. Provide a minimum of 2 miles radar separation diagonally between successive aircraft on adjacent localizer/azimuth courses where runway centerlines are more than 4,300 feet but no more than 9,000 feet apart.

EXAMPLE−
In FIG 5−9−7, Aircraft 2 is 2 miles from heavy Aircraft 1. Aircraft 3 is a small aircraft and is 6 miles from Aircraft 1. *The resultant separation between Aircrafts 2 and 3 is 4.2 miles.

FIG 5−9−7

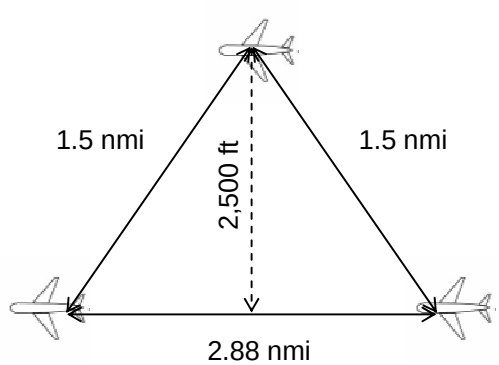
Parallel Dependent ILS/MLS Approaches



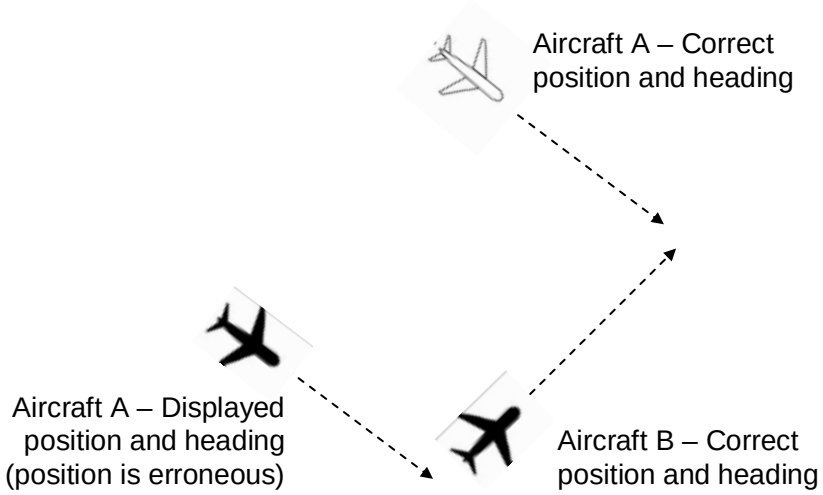
EXAMPLE−
*In FIG 5−9−7, Aircraft 2 is 2 miles from heavy Aircraft 1. Aircraft 3 is a small aircraft and is 6 miles from Aircraft 1. *The resultant separation between Aircrafts 2 and 3 is 4.2 miles.*

4. Provide the minimum applicable radar separation between aircraft on the same final approach course.
REFERENCE−
FAAO 7110.65, Section 5, Radar Separation, Minima, Para 5−5−4.
b. The following conditions are required when applying the minimum radar separation on adjacent localizer/azimuth courses allowed in subpara a:
1. Apply this separation standard only after aircraft are established on the parallel final approach course.
2. Straight-in landings will be made.
3. Missed approach procedures do not conflict.
4. Aircraft are informed that approaches to both runways are in use. This information may be provided through the ATIS.
5. Approach control shall have the interphone capability of communicating directly with the local controller at locations where separation responsibility has not been delegated to the tower.
NOTE−
The interphone capability is an integral part of this procedure when approach control has the sole separation responsibility.
REFERENCE−
FAAO 7110.65, Approach Separation Responsibility, Para 5−9−5.
FAAO 7210.3, Authorization for Separation Services by Towers,
Para 2−1−15.
c. Consideration should be given to known factors that may in any way affect the safety of the instrument approach phase of flight, such as surface wind direction and velocity, wind shear alerts/reports, severe weather activity, etc. Closely monitor weather activity that could impact the final approach course. Weather conditions in the vicinity of the final approach course may dictate a change of approach in use.
REFERENCE−
FAAO 7110.65, Final Approach Course Interception, Para 5−9−2.

- Note: Based on the separation geometry described in FAA Order 7110.65, the minimum longitudinal separation between aircraft is closer to 2.9 nmi. However, 2.5 nmi longitudinal separation was assumed in the system state.



- State 2: IMC
- State 3: High density traffic
- State 4: ADS-B system is sole means of surveillance
- State 5: Aircraft courses are converging whereas the displayed aircraft positions and headings indicate otherwise (applies to hazard H4; see figure below)



Existing Controls

- Pilot "see and avoid" rules are referenced frequently as an existing control. These rules are abbreviated as "Pilot see and avoid rule" in the hazard tables; the complete rule is contained in the following excerpt from the Federal Aviation Regulations (FAR):

  Title 14: Aeronautics and Space, PART 91—GENERAL OPERATING AND FLIGHT RULES, Subpart B—Flight Rules (Source: Docket No. 18334, 54 FR 34294, Aug. 18, 1989)
  § 91.113 Right-of-way rules: Except water operations.
  (a) Inapplicability. This section does not apply to the operation of an aircraft on water.
  (b) General. When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, **vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft.** When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear.

- Traffic Collision Avoidance System ("TCAS") is referenced frequently as an existing control. Per FAR Parts 91, 121, 125, 129, and 135, certain aircraft must be equipped with a traffic collision avoidance system.
- ATC non-radar separation procedures are also referenced frequently as an existing mitigation (e.g., for hazards entailing loss of all surveillance). These procedures are contained in Section 6 (Nonradar) of FAA Order 7110.65R and require operational ATC / pilot radio communications. Accordingly, "ATC / pilot communications" is also referenced as an existing control.
- Terrain Awareness and Warning System ("TAWS") is referenced as an existing control for certain hazards. Per FAR Parts 91, 121, and 135, certain aircraft must be equipment with a terrain awareness and warning system. In addition, the FAR specifies that the Airplane Flight Manual shall contain appropriate procedures for (1) The use of the terrain awareness and warning system; and (2) Proper flight crew reaction in response to the terrain awareness and warning system audio and visual warnings.

5.1.2 ATC Surveillance Hazards

Table 5-1: ATC Surveillance Preliminary Hazards

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
H1	Loss of ADS-B Surveillance (All Aircraft)	Primary and backup surveillance information (if present) is lost for all aircraft within a service volume. The automation system ceases to display ADS-B surveillance information for all ADS-B equipped aircraft.	C400 GNSS failure [External] C401 Aircraft backup navigation data source for ADS-B not present or fails [External] C1 LSP function failure [F2] C6 ADS-B ground station affected by temporary or transient electromagnetic interference [Environmental] C4 Loss of automation function [F4] C3 Failure of communications interface between LSP and automation functions [F2, F4] C403 Facility / equipment power failure [External]	• ADS-B system is sole means of surveillance • High density traffic • IMC • Aircraft are on a converging or collision course	Loss of controller situational awareness Significant increase in ATC workload (due to increased ATC / pilot communications entailed in non-radar separation procedures) Significant increase pilot workload (due to increased ATC / pilot communications entailed in non-radar separation procedures) Large reduction in safety margin (near mid air collision)	It is assumed that controllers will detect that aircraft surveillance information is lost when automation system ceases to display ADS-B data for all aircraft.	2 (Hazardous) Aircraft are not separated by altitude once established on final approach. If surveillance is lost, ATC will apply existing non-radar separation procedures to achieve course divergence and altitude separation. A near mid-air collision may occur if: aircraft are on a collision course, ATC non-radar separations procedures are not completely effective, and TCAS (if present) is not successful in resolving the traffic conflict, but pilot see and avoid rules prevent a catastrophic outcome. .	fPR 3.1.6 ADS-B Backup a. ATC Surveillance application shall continue to operate in the event of GNSS failure. [C400] fPR 3.2.1.1 ADS-B Service Availability The ADS-B service is a safety-critical service as classified by NAS-SR-1000 for surveillance services. This requirement is driven by the ATC Surveillance application. a. The ADS-B service shall meet a minimum Availability of 0.99999. Note: **ADS-B Service availability applies to total outages in a service volume for the navigation source, back up surveillance source, the broadcast services infrastructure, and the automation system**. It does not apply to outages that may occur on individual aircraft. [C1, C4, C3, C400] NAS-SR-1000 3.8.1 NAS equipment, systems, installations, and facilities shall be kept in an operable and committable state according to their criticality to safe operation of aircraft. A. 1. Critical – Functions or services which, if lost, would prevent the NAS from exercising safe separation and control over aircraft. 2. Essential – Functions or services which, if lost, would reduce the capability of the NAS to exercise safe separation and control over	Remote (C) The likelihood that the hazard occurs during an operational flight hour is ~ 10^{-5}. This is based on the over-arching existing control for ASD-B system availability of 99.999% for the ATC surveillance application. The likelihood that aircraft are on a collision course is conservatively estimated at ~ 10^{-1}. The likelihood that TCAS (if present) fails to successfully resolve a traffic conflict is ~ 10^{-1} based on a MITRE analysis of TCAS effectiveness. The combined probability that the hazard occurs and results in a near mid air collision is 10^{-7} (i.e., $10^{-5} * 10^{-1} * 10^{-1}$).	2C (High)	The SBS Contractor shall adhere to industry best practices for software development. [C1, C3 (partial)] The FAA shall define and implement requirements for an independent automated safety monitoring capability that monitors inputs and outputs at interfaces between SBS subsystems and provides fault diagnostics, failure control and correction, and configurable status monitoring and alarm annunciation. Software for the automated safety monitoring capability shall satisfy the objectives for Assurance Level 2 defined in RTCA DO-278 or an equivalent software design assurance standard. [H1] The ASD-B system shall be designed to meet Mil-STD-461 requirements for electromagnetic susceptibility and interference. [C6] The combined probability that ADS-B primary and backup surveillance fails shall be no more than extremely remote (i.e., 10^{-7}) [H1] The FAA shall develop and implement certification procedures to verify that SBS ground equipment performance is	2D (Medium)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								aircraft. B. Table 3-6: Critical 0.99999; Essential 0.999. [C3, C403] fPR 4.9 Power Systems and Commercial Power 4.9.1 Electrical Power Electrical power shall be provided in accordance with NFPA 70, National Electric Code ®; FAA Order, Electrical Power Policy; FAA Order 6950.2, Electrical Power Policy Implementation, NAS Facilities; and FAA Order 6950.25, Power Conditioning Devices at FAA Facilities.[C403] Ctrl-1 Automation system displays coasted track when surveillance data is missing for an adaptable amount of time. (See STARS System / Sub-system Specification and CARTS Functional Specification) [H1] fPR 3.1.5 Maintenance Function 3.1.5.2 Processing h. The Maintenance Function shall provide a centralized monitor and control capability to evaluate performance during operation, control the equipment, monitor system health, and identify faulted modules. i. The Maintenance Function shall generate Alerts and Alarms when monitored parameters exceed allowable tolerances. 3.1.5.3 Outputs a. The Maintenance Function shall display system performance and certification data to the operator to assess the status of the system.			within tolerance. [C1, C4, C3]	

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								b. The Maintenance Function shall display Alerts and Alarms to the system operator. c. The Maintenance Function shall display the operating status of system functions and components. [C1, C4, C3, C400] FAA Order 7110.65 ATC non-radar separation procedures [H1] ATC / pilot communications [H1] Pilots may use ground VORs for navigation and position reporting. [H1] TCAS [H1] Pilot see and avoid rules [H1]				
H17	Loss of ADS-B Surveillance (Multiple Aircraft)	Primary and backup surveillance information for multiple aircraft is lost within a service volume. The automation system ceases to display ADS-B surveillance information for multiple ADS-B equipped aircraft.	C404 ADS-B system coverage gap [F2] C49 Increased congestion of the 1090 MHz spectrum affects ADS-B system ability to detect ADS-B equipped aircraft [External] C9 Number of aircraft exceeds ADS-B system capacity [F2, F4] C6 ADS-B ground station affected by temporary or transient electromagnetic	• ADS-B system is sole means of surveillance • High density traffic • IMC • Aircraft are on a converging or collision course	Loss of controller situational awareness Significant increase in ATC workload (due to increased ATC / pilot communications entailed in non-radar separation procedures) Significant increase pilot workload (due to increased ATC / pilot communications entailed in non-radar separation procedures)	The causes for H17 differ from those entailed in H1.	2 (Hazardous) Aircraft are not separated by altitude once established on final approach. If surveillance is lost for multiple aircraft, ATC will apply existing non-radar separation procedures to achieve course divergence and altitude separation. A near mid-air collision may occur if: aircraft are on a collision course, ATC non-radar separations procedures are not completely effective, and TCAS (if present) is not successful in resolving the traffic conflict, but	fPR 3.2.3.2.5 Coverage a. ADS-B surveillance coverage shall include, but not be limited to the following: • in en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3.G (3) and (4) [C404] fPR 3.2.3.2.3 Update Rate Each aircraft/vehicle will transmit ADS-B Messages with a position and velocity at least once every second. Aircraft/vehicle identification data may be transmitted less often. The ADS-B update rate as seen by the LSP/BCS is a function of operating environment and transmission range. a. The LSP/BCS shall	Extremely Remote (D) The combined probability that the hazard occurs and results in a near mid air collision is qualitatively estimated as extremely remote. None of the causes are completely mitigated by existing controls. A coverage gap or an increased traffic volume could result in dropped or lost target data. The likelihood that TCAS (if present) fails to successfully	2D (Medium)	The FAA shall perform an analysis of 1090 MHz spectrum utilization impacts given peak ADS-B, Mode S, and Mode A/C target loads and densities and the worst-case potential combination of ATC surveillance systems which utilize the 1090 MHz spectrum in the same service area. The spectrum analysis shall evaluate the impacts to aircraft transponder occupancy, TCAS performance, and the probability of target detection for each ATC surveillance system considered above. If deemed necessary based	2E (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
			interference [Environmental] C425 GPS jamming C415 System does not notify ATC that surveillance is missing for one or more targets		Large reduction in safety margin (near mid air collision)		pilot see and avoid rules prevent a catastrophic outcome. .	provide position and velocity data from each aircraft/vehicle in terminal airspace coverage with an update rate sufficient to support 3nm separation standards. [C404, C9] fPR 3.2.4.1.5 Coverage a. The ATC Automation Function *shall* process and display ADS-B target data within the coverage volumes of the LSP Function and the BCS Function. [C404] fPR 3.1.5.3 Outputs g. The Maintenance Function shall provide analysis results indicating areas where coverage is predicted to exist, where actual coverage is acceptable, where actual coverage is not acceptable, and areas where coverage is unknown due to lack of targets of opportunity. [C404] fPR 3.2.3.2.6 Capacity a. The LSP/BCS shall process all ADS-B Messages received from aircraft/vehicles within ADS-B surveillance coverage (Reference section 3.2.3.2.5). [C9 (partial)] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.6 Automation System Capacity a. The ATC Automation Function shall have sufficient capacity to process the ADS-B peak and steady state target capacity loading. [C9 (partial)] Ctrl-1 Automation system displays coasted track when surveillance data is missing	resolve a traffic conflict is ~ 10^{-1} based on a MITRE analysis of TCAS effectiveness.		on the results of the spectrum analysis, the FAA shall develop a mitigation strategy to minimize the risk to maintaining required ATC surveillance systems' performance and required TCAS performance. [C49] The system shall provide a notification to maintenance operators prior to reaching a telecommunications loading threshold at which target data may be lost or dropped. [C9] The system shall provide a notification to maintenance operators prior to reaching a computer processing utilization threshold at which target data may be lost or dropped. [C9] The system shall provide a notification to maintenance operators prior to reaching a computer memory utilization threshold at which target data may be lost or dropped. [C9] The ASD-B system shall be designed to meet Mil-STD-461 requirements for electromagnetic susceptibility and interference. [C6] The probability that the system fails to notify ATC when surveillance data is missing for an adaptable amount of time shall be no more than 10^{-7}. [C415]	

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								for an adaptable amount of time. [H17] TCAS [H17] Pilot see and avoid rules [H17] Pilots may use ground VORs for navigation and position reporting. [H17]				
H2	Loss of ADS-B Surveillance (Single Aircraft) (Undetected by ATC)	ADS-B surveillance information for a single aircraft is lost. The automation system ceases to display ADS-B surveillance information for a single ADS-B equipped aircraft.	C404 ADS-B system coverage gap [F2] C32 Line-of-sight from aircraft to ADS-B system ground station temporarily blocked (e.g., aircraft banks such that antenna is angled away from ground station antenna) [External] C23 ADS-B ground station loses data for 1 track (design failure) [F2] C9 Number of aircraft exceeds ADS-B system capacity [F2, F4] C415 System does not notify ATC that surveillance is missing for one or more targets C10 Aircraft ADS-B avionics / transmitter soft failure [F1] C5 Aircraft ADS-B avionics / ADS-B transmitter hard failure [F1] C420	• ADS-B system is sole means of surveillance • High density traffic • IMC • Aircraft are on a converging or collision course OR • Aircraft is flying over mountainous terrain	Loss of controller situational awareness MSAW not issued when required Potential collision Potential Controlled Flight Into Terrain (CFIT) given IMC and lack of controller situational awareness		1 (Catastrophic) If surveillance for a single aircraft is lost when that aircraft is entering an arrival flow or nearing mountainous terrain and ATC does not detect the loss, hazard severity may be catastrophic (1). If ATC is unaware that an aircraft is present (due to lost surveillance), another aircraft may be established on a collision course with that aircraft. Also, if an aircraft is flying over mountainous terrain, ATC may not be able to issue low altitude warnings to the pilot without surveillance and Minimum Safety Altitude Warning information.	fPR 3.2.3.2.5 Coverage a. ADS-B surveillance coverage shall include, but not be limited to the following: • in en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3.G (3) and (4), • the aircraft movement area at airports with a control tower. [C404] fPR 3.2.3.2.3 Update Rate Each aircraft/vehicle will transmit ADS-B Messages with a position and velocity at least once every second. Aircraft/vehicle identification data may be transmitted less often. The ADS-B update rate as seen by the LSP/BCS is a function of operating environment and transmission range. a. The LSP/BCS shall provide position and velocity data from each aircraft/vehicle in terminal airspace coverage with an update rate sufficient to support 3nm separation standards. [C404, C9] fPR 3.2.4.1.5 Coverage a. The ATC Automation Function *shall* process and display ADS-B target data within the coverage volumes of the LSP Function and the BCS Function. [C404]	Remote (C) Cause C5 can be probable (B) (i.e., failure of avionics transmitter (~1E-4)). However, for the loss of ADS-B surveillance to go undetected for one target, automation system coasting functionality (Ctrl 1 for C415) would also have to fail. This is estimated as an extremely remote occurrence. The combination of the above is qualitatively estimated as remote (C).	1C (High)	The system shall provide a notification to maintenance operators prior to reaching a telecommunications loading threshold at which target data may be lost or dropped. [C9] The system shall provide a notification to maintenance operators prior to reaching a computer processing utilization threshold at which target data may be lost or dropped. [C9] The system shall provide a notification to maintenance operators prior to reaching a computer memory utilization threshold at which target data may be lost or dropped. [C9] When selecting locations for ADS-B ground stations, the FAA shall perform a coverage / siting analysis that considers aircraft bank angles which may result in line-of-sight coverage problems (e.g., the aircraft banks such that the transmit / receive antenna is angled away from the ground station antenna). [C32]	1E (Medium)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
			Aircraft avionics EMI [External] C421 Aircraft wiring problems [External] C422 Aircraft avionics mis-installation [External] C423 ADS-B avionics transmission inadvertently turned off. [External] C49 Increased congestion of the 1090 MHz spectrum affects ADS-B system ability to detect ADS-B equipped aircraft [External]					fPR 3.1.5.3 Outputs g. The Maintenance Function shall provide analysis results indicating areas where coverage is predicted to exist, where actual coverage is acceptable, where actual coverage is not acceptable, and areas where coverage is unknown due to lack of targets of opportunity. [C404] fPR 3.2.3.2.6 Capacity a. The LSP/BCS shall process all ADS-B Messages received from aircraft/vehicles within ADS-B surveillance coverage (Reference section 3.2.3.2.5). [C9 (partial)] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.6 Automation System Capacity a. The ATC Automation Function shall have sufficient capacity to process the ADS-B peak and steady state target capacity loading. [C9 (partial)] Ctrl-1 Automation system displays coasted track when surveillance data is missing for an adaptable amount of time. [C415, H2] fPR 3.2.2.2.2 Aircraft/Vehicle ADS-B Transmission The Aircraft/Vehicle transmits ADS-B Messages in support of all applications. The requirements in this section apply to all applications, unless a specific application is listed in the requirement text. 3.2.2.2.2.6 Availability a. Aircraft/Vehicle			The SBS Contractor shall adhere to industry best practices for software development. [C1, C3 (partial)] The FAA shall define and implement requirements for an independent automated safety monitoring capability that monitors inputs and outputs at interfaces between SBS subsystems and provides fault diagnostics, failure control and correction, and configurable status monitoring and alarm annunciation. Software for the automated safety monitoring capability shall satisfy the objectives for Assurance Level 2 defined in RTCA DO-278 or an equivalent software design assurance standard. [H2] The probability that the system fails to notify ATC when surveillance data is missing for an adaptable amount of time shall be no more than 10^{-7}. [C415] The FAA shall perform a collision risk analysis in accordance with Flight Standards guidelines to determine the required availability of the Aircraft/Vehicle function given terminal separation standards and end-to-end (i.e., air / ground) system performance parameters [C5] Hardware for the Aircraft/Vehicle function shall comply with RTCA	

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								function shall provide a minimum availability of 0.9995 for non-redundant installations. [C10, C5 (partial)] TCAS [H2] Pilot see and avoid rules [H2]			DO-160D Environmental Conditions and Test Procedures for Airborne Equipment. [C10, C5, C420] The approval process for design, production, installation, and operation of ADS-B equipment onboard civil aircraft shall comply with "The FAA and Industry Guide to Product Certification" and "The FAA and Industry Guide to Avionics Approvals." [C10, C5] The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B avionics and ancillary equipment. [C10, C5, C421, C422] The FAA shall perform an analysis of 1090 MHz spectrum utilization impacts given peak ADS-B, Mode S, and Mode A/C target loads and densities and the worst-case potential combination of ATC surveillance systems which utilize the 1090 MHz spectrum in the same service area. The spectrum analysis shall evaluate the impacts to aircraft transponder occupancy, TCAS performance, and the probability of target detection for each ATC surveillance system considered above. If deemed necessary based on the results of the spectrum analysis, the FAA shall develop a	

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
											mitigation strategy to minimize the risk to maintaining required ATC surveillance systems' performance and required TCAS performance. [C49]	
H4	Inaccurate Aircraft Position Displayed to Controller (Single Aircraft)	The position for a single aircraft as displayed to the controller on the automation system is inaccurate. The true position of the aircraft may be closer to or farther away from nearby aircraft.	C31 GPS / navigation positioning error for single aircraft [External] C405 Aircraft avionics / STP processing error for ownship data [F1.2] C406 Aircraft avionics / receiver or ASSAP processing error for received data [F1.3] C7 Aircraft avionics / ADS-B transmitter provides inaccurate position [F1.4] C22 ADS-B ground station fault – transient corruption of target data [F2.1, F2.3.3] C30 Automation system fault – transient corruption of target data [F4.2]	• ADS-B system is sole means of surveillance • High density traffic • IMC	E1 Loss of controller situational awareness leading to increased ATC workload and unsafe aircraft separation E8 Automation system provides a minimum safe altitude warning when one should not be issued (false warning) E4 Automation system provides a conflict alert when one should not be issued (false alert) E3 Automation system does not provide minimum safe altitude warning when one should be issued E2 Automation system does not provide conflict alert when one should be issued E18 Potential aircraft collision		1 (Catastrophic) If ATC does not detect that the displayed position is erroneous, hazard severity may be catastrophic. If the pilot's navigation source fails or malfunctions, the pilot may not be aware of his location. Moreover, if the same navigation source provides aircraft position information to ATC, then ATC also loses awareness of the aircraft location.	J 51 Provide on-board position source integrity monitoring per DO-242A, DO-260A, DO-282A [C31 (partial)] fPR 3.2.2.2.2.4 Position and Velocity Information Accuracy Vertical and horizontal position and velocity uncertainty is a 95% accuracy limit on the position and velocity, respectively. 3.2.2.2.2.4.1 Horizontal Position f. The Aircraft/Vehicle shall provide position information with a 95% probability of a maximum error less than or equal to 0.1NM to support the ATC Surveillance application in the terminal environment. [C7] fPR 3.2.3.2.2 Position Accuracy The aircraft navigation source and avionics are contributors to ADS-B Report position and velocity accuracy. The ADS-B Report also includes quality parameters for the reported position and velocity. a. The LSP/BCS Function shall preserve the target position and velocity accuracy represented in each ADS-B Report. [C22] fPR 3.2.3.2.4 Integrity	Extremely remote (D) GPS integrity monitoring brings this probability down to ~ 10E-7.	1D (High)	The SBS Contractor shall adhere to industry best practices for software development. [C405, C406] Software for the Aircraft/Vehicle function shall satisfy the objectives for Software Level C defined in RTCA DO-178B or an equivalent software design assurance standard. [C405, C406, C7] The FAA shall perform a collision risk analysis in accordance with Flight Standards guidelines to validate the required Aircraft/Vehicle function performance, including positional accuracy, accounting for end-to-end (i.e., air / ground) system performance parameters. [C7] Hardware for the Aircraft/Vehicle function shall comply with RTCA DO-160D Environmental Conditions and Test Procedures for Airborne Equipment. [C405, C406, C7]	1E (Medium) Extremely Improbable (E) Collision risk analysis expected to show at least a reduction of 2 orders of magnitude between the possible error and the collision risk

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
					E16 Increased ATC workload			ADS-B Messages are received, processed and transported by the LSP/BCS function to the ATC Automation Function. The integrity of ADS-B Reports cannot be compromised by the LSP/BCS as a result of software or hardware failures. a. The probability that LSP/BCS introduces hazardously misleading information into an ADS-B Report while being processed shall be 10-5 or better per hour. [C22] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.2 Accuracy a. The ATC Automation Function shall preserve the airborne horizontal position accuracy of ADS-B Reports. b. The ATC Automation Function tracking performance with ADS-B data shall be equal or exceed tracking performance with radar in automation systems. c. The ATC Automation Function shall only use ADS-B Reports with accuracy and integrity values that meet configured/adapted thresholds as inputs to tracking, safety alert and display functions. [C30] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.4 Integrity a. The ATC Automation Function shall preserve the integrity of reported airborne horizontal positions. b. The ATC Automation Function probability that Automation fails to detect large jumps in an aircraft position in an ADS-B Report				

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								that is outside the probable position shall be better than or equal to 10-3. Note: The requirement addresses the ability to detect erroneous information in the report, which is not introduced by ATC Automation. c. The ATC Automation Function allowable rate of false (self) conflict alerts due to non-correlation of ADS-B and radar targets in overlapping ADS-B/radar airspace shall not impact ATC's ability to control air traffic. [C30] TCAS [H4] Pilot see and avoid rules [H4]				
H5	Inaccurate Aircraft Position Displayed to Controller (All Aircraft)	The positions for all aircraft as displayed to the controller on the automation system are inaccurate. The true positions of the aircraft may be closer to or farther away from nearby aircraft.	C34 Undetected wide-area failure of GPS positioning [F5.1.4] C21 ADS-B ground station corrupts data for multiple targets [F2.1, F2.3.3] C27 Automation system corrupts data for multiple targets [F4.2] C408 Inaccurate automation system display map [F4] C8 Misalignment of surveillance data to automation system map [F4] C11 Design flaw - Total latency from aircraft to ground systems exceeds what is acceptable	• ADS-B system is sole means of surveillance • High density traffic • IMC • 3 nmi longitudinal and 1.5 nmi diagonal separation for parallel, dependent ILS approaches	E1 Loss of controller situational awareness leading to increased ATC workload and unsafe aircraft separation E8 Automation system provides a minimum safe altitude warning when one should not be issued (false warning) E4 Automation system provides a conflict alert when one should not be issued (false alert) E3 Automation system does not provide minimum safe altitude warning when one should be		1 (Catastrophic) If ATC does not detect that that the displayed aircraft positions are inaccurate, a catastrophic (1) severity may occur. Based on erroneous traffic position information, ATC may inadvertently put aircraft on a collision course.	fPR 3.1.5 Maintenance Function 3.1.5.1 Inputs d. The Maintenance Function shall receive GNSS status from external sources to assess the operational status of the GNSS sources in the Aircraft/Vehicle Function. [C34 (partial)] fPR 3.1.5 Maintenance Function fPR 3.1.5.3 Outputs a. The Maintenance Function shall display system performance and certification data to the operator to assess the status of the system. b. The Maintenance Function shall display Alerts and Alarms to the system operator. c. The Maintenance Function shall display the operating status of system functions and components. [C34 (partial)] J 51 Provide on-board position source integrity	Extremely Remote (D) Existing specifications and designs for GPS integrity make the likelihood of an undetected common-mode failure independently affecting multiple aircraft in a way that would make them appear to be farther apart than they actually are is estimated to be extremely remote.	1D (High)	The end-to-end system latency shall not exceed the maximum acceptable latency based on Flight Standards collision risk analysis. [C11] ML 32: The FAA shall ensure accuracy of the terrain/airfield map displayed to ATC. [C408] The FAA shall develop and implement procedures to verify alignment of surveillance sensor data to the automation system display map. [C8]	1E (Medium) Extremely improbable (E)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
			for achieving positional accuracy required for safe separation [F0]		issued E2 Automation system does not provide conflict alert when one should be issued E18 Potential aircraft collision Significant increase in ATC workload (due to increased ATC / pilot communications entailed in non-radar separation procedures) Significant increase pilot workload (due to increased ATC / pilot communications entailed in non-radar separation procedures)			monitoring per DO-242A, DO-260A, DO-282A [C34 (partial)] fPR 3.2.3.2.2 Position Accuracy The aircraft navigation source and avionics are contributors to ADS-B Report position and velocity accuracy. The ADS-B Report also includes quality parameters for the reported position and velocity. a. The LSP/BCS Function shall preserve the target position and velocity accuracy represented in each ADS-B Report. [C21] fPR 3.2.3.2.4 Integrity ADS-B Messages are received, processed and transported by the LSP/BCS function to the ATC Automation Function. The integrity of ADS-B Reports cannot be compromised by the LSP/BCS as a result of software or hardware failures. a. The probability that LSP/BCS introduces hazardously misleading information into an ADS-B Report while being processed shall be 10-5 or better per hour. [C21] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.2 Accuracy a. The ATC Automation Function shall preserve the airborne horizontal position accuracy of ADS-B Reports. b. The ATC Automation Function tracking performance with ADS-B data shall be equal or exceed tracking performance with radar in automation systems. c. The ATC Automation				

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								Function shall only use ADS-B Reports with accuracy and integrity values that meet configured/adapted thresholds as inputs to tracking, safety alert and display functions. [C27] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.4 Integrity a. The ATC Automation Function shall preserve the integrity of reported airborne horizontal positions. b. The ATC Automation Function probability that Automation fails to detect large jumps in an aircraft position in an ADS-B Report that is outside the probable position shall be better than or equal to 10-3. Note: The requirement addresses the ability to detect erroneous information in the report, which is not introduced by ATC Automation. [C27] fPR 3.2.1.5 System Latency for ATC Surveillance Application The System Latency is the sum of the aircraft/vehicle latency from the time of applicability, the LSP/BCS latency with telecommunications, and the ATC Automation latency. a. The latency from time of applicability of the ADS-B Message data until display by ATC Automation shall be less than or equal to 2.7 seconds to provide ATC Surveillance in Terminal airspace. [C11] FAA Order 7110.65 ATC non-radar separation procedures [H5]				

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								ATC / pilot communications [H5] Pilots may use ground VORs for navigation and position reporting. [H1] TCAS [H5]				
H6	Duplicate Aircraft Targets Displayed to Controller	Two aircraft are displayed to the controller where only one aircraft exists.	C12 Automation system fails to correlate data for the same target provided by multiple surveillance sources [F4.2.4] C19 Pilot changes beacon code in-flight [External] C409 ADS-B system fails to detect that an aircraft's beacon code changed and displays two targets (i.e., one based on the old code and one based on the new code) [F2, F4] C407 ADS-B system "splits" a single track or target report, resulting in two tracks or reports for one target [F4]	• High density traffic • IMC • 3 nmi longitudinal and 1.5 nmi diagonal separation for parallel, dependent ILS approaches	E4 Automation system provides a conflict alert when one should not be issued (false alert) ATC issues unnecessary maneuver instructions to pilot Pilot workload increase due to unnecessary maneuver	This problem is detected. This hazard implies a design problem that may be systemic.	3 (Major) If the duplicate (false) target appeared in proximity to an aircraft on one of the parallel dependent ILS approach courses, the automation system may issue a conflict alert. ATC would take action to separate real traffic from the duplicate target, treating both targets as real. It is expected that ATC will eventually realize that one target was false when there is no pilot acknowledgement of ATC instructions.	fPR 3.1.4 ATC Automation Function 3.1.4.2 Processing d. The ATC Automation Function shall link valid ADS-B Reports with other surveillance sources to avoid duplicate tracks on a single target from being displayed. [C12] fPR 3.1.4 ATC Automation Function 3.1.4.2 Processing j. The ATC Automation Function shall provide registration between ADS-B and radar. Note: The ATC Automation Function may use ADS-B Reports to aid in the correction of radar registration and bias errors. [C12] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.4 Integrity c. The ATC Automation Function allowable rate of false (self) conflict alerts due to non-correlation of ADS-B and radar targets in overlapping ADS-B/radar airspace shall not impact ATC's ability to control air traffic. [H6]	Extremely Remote (D) Based on interviews with ATC representatives from ZAN, duplicate targets have been observed on MEARTS particularly at the fringes of radar coverage areas where ADS-B coverage exists. However, implementation and verification of existing controls reduce the likelihood to an acceptable level.	3D (Low)		3D (Low)
H7	Inaccurate Aircraft Identification Displayed to Controller (Single	The identification for an aircraft displayed to the controller is incorrect. Incorrect identification	C15 Automation system associates the wrong ID (e.g., flight ID) with a target report	• High density traffic • IMC • 3 nmi longitudinal	Collision or CFIT E9 Based on mis-identified target, controller issues	An incorrect ID may have no safety effect is ATC notices that the displayed ID does not match the ID	2 (Hazardous) ATC may issue instructions to the wrong aircraft based on incorrect aircraft ID.	fPR 3.2.2.2.2.5.4 Identification and Altitude Integrity a. The likelihood that the Aircraft/Vehicle transmits an aircraft identification (Mode	Extremely Remote (D) Existing procedures already control this to an acceptable level.	2D (Medium)	The probability that the system displays an incorrect target ID to the controller shall be less than 10^{-6}. [C15, C30]	2E (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
	Aircraft)	includes aircraft ID (ACID), flight ID, and beacon code.	[F4.2] C410 Aircraft avionics transmits incorrect ID [F1.1.3, F1.2, F1.4] C22 ADS-B ground station fault – transient corruption of target data [F2.1, F2.3.3] C30 Automation system fault – transient corruption of target data [F4.2]	and 1.5 nmi diagonal separation for parallel, dependent ILS approaches	instructions to wrong aircraft E1 Loss of controller situational awareness leading to increased ATC workload and unsafe aircraft separation	recorded on a flight strip. Also, ATC will notice the error when the pilot contacts ATC and states a different ID than what is shown on the controller's display.	Although ATC will eventually detect that the wrong aircraft is complying with instructions, there may be a significant reduction in safety margin before the situation is corrected For example, an aircraft may begin descending based on ATC instructions. Aircraft are only separated by 1,000 ft in altitude and can quickly lose vertical separation before ATC realizes. For ATC to observe vertical movement, aircraft must shift at least 200 feet in altitude. Lag in altitude update rate coupled with aircraft descent rate are other factors. Also, if an aircraft is on a collision course with another aircraft or terrain, an incorrect ID may result in a significant reduction in safety margin. The pilot of the endangered aircraft may not realize ATC is trying to contact him if ATC is using the wrong ID in the radio communication.	A code, International Civil Aviation Organization (ICAO) code, or call sign) that differs from the true identification shall be less than 10-3 per flight hour to support the ATC Surveillance application. [C410] JH 55: Use of error detecting and correction codes in ADS-B transmissions per DO-260A and DO-282A. [C22] fPR 3.2.3.2.4 Integrity ADS-B Messages are received, processed and transported by the LSP/BCS function to the ATC Automation Function. The integrity of ADS-B Reports cannot be compromised by the LSP/BCS as a result of software or hardware failures. a. The probability that LSP/BCS introduces hazardously misleading information into an ADS-B Report while being processed shall be 10-5 or better per hour. [C22] ML 3: ATC specialist use of 7110.65 procedures for validating aircraft ID, position, and altitude [H7]	New use of error correcting codes in ADS-B will reduce the likelihood of this problem as compared to today with existing transponders.			
H8	Inaccurate Aircraft Altitude Displayed to Controller (Single Aircraft)	Altitude for a single aircraft displayed to the controller is inaccurate. The true altitude of the aircraft may be higher or lower than the altitude displayed to the controller. The true location of the aircraft may be closer to or farther away from the	C42 Aircraft barometric sensor fails [External] C45 Pilot does not set altimeter correctly [External] C18 Aircraft avionics / ADS-B transmitter improperly configured / installed	• IMC • Mountain-ous terrain	E16 Increased ATC workload Large reduction in safety margin due to CFIT risk Increased pilot workload	In general, ATC may become distracted / confused due to erroneous information on display and take the wrong action. Barometric (not "geo") altitude used. ADS-B uses the same barometric altitude	2 (Hazardous) ATC may not realize that the reported altitude for an aircraft is erroneous and that an aircraft is on a collision course with another aircraft or with terrain. A large reduction in safety margin may occur in the event that TCAS fails to resolve a traffic conflict but pilots see	fPR 3.1.1 Aircraft/Vehicle Function 3.1.1.1 ADS-B Transmission 3.1.1.1.1 Inputs b. The Aircraft/Vehicle Function shall include an FAA approved pressure altitude sensor as the primary barometric altitude data source. [C42 (partial)] AIM Section 7-2-2 Altimeter Setting Procedures [C45]	Extremely Remote (D) likelihood of undetected problem – existing controls and procedures already control this to an acceptable level.	2D (Medium)	The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B avionics and ancillary equipment. [C18]	2E (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
		ground.	[External] C405 Aircraft avionics / STP receive or processing error for ownship data [F1.1.3, F1.2] C406 Aircraft avionics / receiver or ASSAP processing error for received data [F1.3] C17 Aircraft avionics / ADS-B transmitter provides inaccurate altitude [F1.4] C22 ADS-B ground station fault – transient corruption of target data [F2.1, F2.3.3] C30 Automation system fault – transient corruption of target data [F4.2]			sources that are used for transponders today. ATC may detect that a displayed altitude is erroneous if there is a discrepancy with the pilot-reported altitude. In this case, the controller will ask the pilot to verify altimeter setting. If the altimeter is correct, but the Mode C is wrong, the controller will ask the pilot to stop squawking Mode C. The controller's workload may increase slightly in order to verify and resolve a bad Mode C. The controller's workload may also increase due to suppressing MSAWs which may be issued based on an erroneous altitude.	and maneuver to avoid a collision. Similarly, a large reduction in safety margin may occur in the event that TAWS fails to resolve a CFIT risk but the pilot sees and maneuvers to avoid collision with terrain.	fPR 3.2.2.2.2.4.4 Vertical Position b. The Aircraft/Vehicle shall provide barometric altitude with an accuracy commensurate with the pressure altitude source to support the ATC Surveillance application. Note: Ground vehicles are not required to report altitude. [C17] fPR 3.2.2.2.2.5.4 Identification and Altitude Integrity b. The likelihood that the Aircraft/Vehicle transmits an incorrect altitude shall be less than 10-3 per flight hour for aircraft without an RVSM altimetry system to support the ATC Surveillance application. c. The likelihood that the Aircraft/Vehicle transmits an incorrect altitude shall be less than 10-5 per flight hour for aircraft with RVSM altimetry systems to support the ATC Surveillance application. [C405, C406, C17] JH 55: Use error detecting and correction codes in ADS-B transmissions per DO-260A and DO-282A. [C42, C18, C405, C406, C17] fPR 3.2.3.2.4 Integrity ADS-B Messages are received, processed and transported by the LSP/BCS function to the ATC Automation Function. The integrity of ADS-B Reports cannot be compromised by the LSP/BCS as a result of software or hardware failures. a. The probability that LSP/BCS introduces hazardously misleading information into an ADS-B				

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								Report while being processed shall be 10-5 or better per hour. [C22] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.2 Accuracy a. The ATC Automation Function shall preserve the airborne horizontal position accuracy of ADS-B Reports. b. The ATC Automation Function tracking performance with ADS-B data shall be equal or exceed tracking performance with radar in automation systems. c. The ATC Automation Function shall only use ADS-B Reports with accuracy and integrity values that meet configured/adapted thresholds as inputs to tracking, safety alert and display functions. [C30] ML 3: ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude [H8] TCAS [H8] TAWS [H8] Pilot see and avoid rules [H8]				
H9	Inaccurate Aircraft Altitude Displayed to Controller (All Aircraft)	Aircraft altitudes for all aircraft displayed to the controller are inaccurate. The true altitudes of the aircraft may be higher or lower than the altitudes displayed to the controller. The true locations of the aircraft may be closer to or farther away from the ground.	C424 Extremely cold temperatures cause systemic altimeter errors in which aircraft is significantly lower than indicated altitude C16 Barometric pressure correction applied incorrectly [F4] C46 Pressure sensor for	• High density traffic • IMC • Mountain-ous terrain	E1 Loss of controller situational awareness leading to increased ATC workload and unsafe aircraft separation E8 Automation system provides a minimum safe altitude warning when one should not be issued	Barometric (not "geo") altitude used. ADS-B uses the same barometric altitude sources that are used for transponders today.	2 (Hazardous) Except in the case of a systemic altitude error at the avionics end, ATC will quickly notice if the displayed altitudes for all aircraft differ from pilot-reported altitudes or assigned altitudes. If all displayed altitudes are wrong, ATC will initially ask each pilot to report altitude and record the information in flight strips.	ML 3: ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude [H9] NOTAMs are issued to indicate altitude corrections that pilots must apply. [C424] AIM Chapter 7 Section 2 Altimeter Setting Procedures [C424] TAWS [H9]	Extremely remote (D) This hazard exists today. No new causes attributed to ADS-B were identified. Existing 7110.65 procedures already control this hazard to an acceptable level	2D (Medium)	The FAA shall develop and implement certification procedures to verify that barometric pressure correction applied at the automation system are accurate. [C16] The FAA shall develop and implement certification procedures to verify that SBS ground equipment performance is within tolerance. [C46]	2E (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
			automation system fails [F4]		(false warning) E4 Automation system provides a conflict alert when one should not be issued (false alert) E3 Automation system does not provide minimum safe altitude warning when one should be issued E2 Automation system does not provide conflict alert when one should be issued		Subsequently, ATC will ask pilots to report when leaving specific altitudes and update the flight strips. Controller workload increases significantly due to extra pilot / ATC communications and manual corrections to altitudes using flight strips.					
H82	One or More Aircraft Not Detected and Displayed To ATC	Certain aircraft are not detected and displayed to ATC. During the transition to full ADS-B equipage, a mixture of different aircraft equipage will exist. ADS-B, Mode S, Mode A/C, and non-equipped aircraft may operate in the same airspace. Non-ADS-B equipped aircraft operating in ADS-B only surveillance coverage areas will not be detected. ADS-B equipped aircraft and no other transponder operating in radar only surveillance coverage areas will not be detected unless primary radar coverage is	C411 Aircraft not ADS-B equipped in Non Radar Airspace (NRA) [Operating Environment] C412 ADS-B messages transmitted by aircraft do not conform to specified message formats [F1] C413 ADS-B messages transmitted by aircraft do not conform to specified spectrum characteristics (e.g., power, frequency, pulse shape) [F1] C5 Aircraft ADS-B avionics / ADS-B transmitter hard failure [F1] C422 Aircraft avionics	• ADS-B system is sole means of surveillance • High density traffic • IMC • Aircraft are on a converging or collision course	Inadequate controller situational awareness MSAW not issued when required Conflict alert not issued when required Potential collision	The scenario in which a non-ADS-B-equipped aircraft is not detected in radar-only airspace is not addressed in this hazard given that this scenario exists with or without ADS-B.	1 (Catastrophic) If ATC is unaware that one or more aircraft are not detected and displayed, a catastrophic situation (e.g., collision) may result.	DO-260A and DO-282A provide requirements for ADS-B message formats [C412] DO-260A and DO-282A specify spectrum requirements for ADS-B transmission [C413] fPR 3.2.2.2.2 Aircraft/Vehicle ADS-B Transmission The Aircraft/Vehicle transmits ADS-B Messages in support of all applications. The requirements in this section apply to all applications, unless a specific application is listed in the requirement text. 3.2.2.2.2.6 Availability a. Aircraft/Vehicle function shall provide a minimum availability of 0.9995 for non-redundant installations. [C5 (partial)] fPR 3.1.5 Maintenance Function	Remote (C) The combined probability that the hazard occurs and results in a near mid air collision is qualitatively estimated as remote. None of the causes are completely mitigated by existing controls.	1C (High)	The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B avionics and ancillary equipment. [C422] The FAA shall maintain legacy surveillance systems until ADS-B equipage level deemed sufficient to remove legacy systems and transition to NRA. [C411] The FAA shall analyze and implement procedural controls, such as reservation of airspace specifically for non-ADS-B equipped aircraft during the transition to complete ADS-B equipage, as necessary. [C411]	1E (Medium)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
		provided.	mis-installation [External]					3.1.5.3 Outputs h. The Maintenance Function shall provide a list of ADS-B equipped aircraft/vehicles that are not in compliance with the datalink standards. [C412, C413] Pilot see and avoid rules [H82] TCAS [H82]				
H83	Erroneous Distance between ADS-B Target Symbols and Radar Target Symbols Displayed to ATC	Legacy non-ADS-B and ADS-B surveillance systems may cover the same airspace (i.e., RAD). The ATC automation system may display ADS-B and non-ADS-B surveillance data in a mosaic fashion (i.e., ADS-B data is displayed in one area and non-ADS-B data is displayed in another area). This is typical in the en route domain where more than one sensor is required to cover the airspace displayed at one ATC position. Due to a registration error, the apparent spacing between ADS-B and radar target symbols may be less than or greater than what is displayed.	C414 Radar position is biased with respect to ADS-B position [External, F4] C502 Accuracy of ADS-B position is worse than accuracy of radar position [F1, F2, F4] C503 Failure to register radar and ADS-B sensors [External, F4]	• ADS-B and radar-only targets operating in same airspace • Large aircraft • 5 nmi separation standards for en route	Loss of controller situational awareness leading to unsafe aircraft separation Conflict alert not issued when required Near mid air collision Large reduction in safety margin Potential wake turbulence upset	There are inherent differences in surveillance performance (e.g., position error) given different types of equipage and surveillance systems.	Hazardous (2) If displayed separation distances between aircraft are distorted, ATC may be led to believe that there is adequate separation between aircraft when there is not. A large reduction in safety margin may occur.	fPR 3.1.4.2 Processing j. The ATC Automation Function shall provide registration between ADS-B and radar. Note: The ATC Automation Function may use ADS-B Reports to aid in the correction of radar registration and bias errors. [C414, C503] fPR 3.2.2.2.2.4 Position and Velocity Information Accuracy Vertical and horizontal position and velocity uncertainty is a 95% accuracy limit on the position and velocity, respectively. 3.2.2.2.2.4.1 Horizontal Position f. The Aircraft/Vehicle shall provide position information with a 95% probability of a maximum error less than or equal to 0.1NM to support the ATC Surveillance application in the terminal environment. [C502] fPR 3.2.3.2.2 Position Accuracy The aircraft navigation source and avionics are contributors to ADS-B Report position and velocity accuracy. The ADS-B Report also includes quality parameters for the reported position and velocity.	Extremely Remote (D) For this hazard to occur, there would have to be a gross system design or adaptation flaw in lack of sensor registration and bias correction. This design flaw is estimated to have an extremely remote (D) probability of occurrence. For a near mid air collision to occur, TCAS would also have to fail to resolve any traffic conflicts.	2D (Medium)	The FAA shall analyze and characterize the separation errors at the ATC display between each combination of ADS-B and radar-only targets. [H83] The FAA shall perform a collision risk analysis to validate separation standards. [H83]	2E (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
								a. The LSP/BCS Function shall preserve the target position and velocity accuracy represented in each ADS-B Report. [C502] fPR 3.2.4.1 ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.2 Accuracy a. The ATC Automation Function shall preserve the airborne horizontal position accuracy of ADS-B Reports. b. The ATC Automation Function tracking performance with ADS-B data shall be equal or exceed tracking performance with radar in automation systems. c. The ATC Automation Function shall only use ADS-B Reports with accuracy and integrity values that meet configured/adapted thresholds as inputs to tracking, safety alert and display functions. [C502] Pilot see and avoid rules [H83] TCAS [H83]				
H85	Differences Between Traffic or Weather Information Displayed to ATC and Pilots	Traffic and weather information displayed to pilots may be different than what is displayed to ATC in the same ADS-B and/or TIS-B/FIS-B service volume. Pilots may question ATC instructions on the basis of information (e.g., presence of traffic or weather displayed on CDTI) available in the cockpit. Pilot confusion concerning ATC-	C500 Different data sources for ATC and aircrew traffic and/or weather information C501 Same data sources for ATC and aircrew traffic and/or weather information but different processing and presentation / display	• High density traffic • IMC	Pilot confusion Pilot questions ATC instruction Pilot delay in complying with ATC instruction Significant reduction in safety margin Increased pilot workload Increased ATC workload	This hazard does not address differences in ATC versus pilot information due to data corruption. Data corruption is addressed in ATC Surveillance hazards H4 – H9 and In-Cockpit Application hazards H22 – H80.	3 (Major) If a pilot becomes confused by discrepancies between traffic / weather shown on the CDTI versus ATC instructions, the pilot may question ATC instructions. Delays in complying with ATC instructions may cause a significant reduction in safety margin.	Pilot see and avoid rules [H85] TCAS [H85]	Probable (B) There are no known requirements that prevent or mitigate the possibility that different data sources (or different information derived from the same source) lead to this hazard.	3B (High)	Provide warnings and cautions regarding over-reliance on CDTI in avionics equipment manuals, pilot training manuals, and AIM [H85] Provide placard on CDTI to indicate application / display only for situational awareness / advisory use [H85] The FAA shall develop and publish procedures for pilots to implement when concerned with ATC instructions based on traffic and / or weather information presented on	3D (Low)

No.	Hazard Title	Hazard Description	Hazard Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Requirements & Objectives	Predicted Residual Risk
		provided information or instruction versus CDTI may result.									the CDTI (Note: This recommended requirement does not preclude defining procedures in which the pilot must comply with ATC instructions regardless of information presented on the CDTI). [H85] Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H85]	

5.2 In-Cockpit Applications

Ground Rules and Assumptions for All In-Cockpit Application Hazards

- Per the SBS System Concept of Operations, all in-cockpit applications selected for Segment 1 of the SBS Program are for situational awareness and advisory purposes only. The Concept of Operations indicates that pilots shall not maneuver solely on the basis of information presented in any of these applications. Instead, pilots must verify the presence of other traffic by some other means independent of the in-cockpit application.
- A potential exists for pilots to over-rely on the in-cockpit applications to the extent of compromising the see and avoid rule. Rather than including this potential in every application-specific hazard, a general hazard (H81) accounts for this possibility.
- Hazards associated with specific CDTI display implementations are not evaluated in this analysis. CDTI implementations may include multifunction displays, dedicated cockpit displays, electronic flight bag displays, and integrated displays (e.g., CDTI integrated with TCAS display). This extends to implementations involving more than one CDTI (e.g., one CDT with specific settings for pilot use and another CDTI with different settings for co-pilot / air crew use).
- This analysis does not consider potential functional and performance differences among CDTIs manufactured by different vendors. For example, some CDTIs may display traffic positions projected to the same time while others may not.
- It is assumed that the air crew will not use the information from any of the Segment 1 applications for position reporting to ATC (e.g., the pilot does not use the ownship position information shown on a CDTI in the enhanced visual acquisition application to report aircraft position to ATC).
- Certain cargo airlines and other aircraft operators have equipped with CDTIs and associated in-cockpit applications such as Enhanced Visual Acquisition. The FAA's Aircraft Certification (AIR) organization has approved the use of this equipment via Supplemental Type Certificates (STCs). Any hazards associated with legacy CDTI installations and ADS-B-, TIS-B-, and FIS-B-related applications are not examined in this analysis.

5.2.1 General

The following table contains hazards that are not application-specific.

Table 5-2: General In-Cockpit Application Preliminary Hazards

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H81	Pilot Over-Reliance on CDTI	The pilot over-relies on the CDTI for traffic and weather situational awareness. The pilot fails to regularly scan out the window for traffic and check for updated weather information in-flight.	C416 Lack of pilot training to maintain vigilance in executing see and avoid procedures [External] C426 Lack of pilot training to check for weather updates prior to take-off and in-flight [External] C417 Marginal visibility conditions make it more difficult to scan out the window for traffic [Environment] C418 Lack of pilot understanding that not all traffic will be displayed on CDTI (i.e., aircraft lacking appropriate equipage will not be displayed) [External]	• Uncontrolled airport • Aircraft are not TCAS equipped • Traffic is busy due to a seasonal event at a GA airport • Pilot is on a VFR flight plan • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic	Potential collision Potential loss of aircraft control due to encountering severe weather		1 (Catastrophic) If pilot inadvertently or inappropriately relies on display, and there is an unidentified target in the area, there is a collision risk in VMC. Extends to IFR / VFR traffic mix. Severity is potentially catastrophic (1). Conditions for collision: (1) a/c on collision course, (2) if TCAS (or equiv.) equipped, TCAS fails or not equipped, (3) see and avoid procedure not used correctly	Pilot see and avoid rules [H81] Aircraft use "flying lights" (aids visibility to and from other traffic) [C417] AIM Chapter 4 Section 1 (4-1-9. Traffic Advisory Practices at Airports Without Operating Control Towers) Radio communication to announce intentions upon approach to uncontrolled airport [C417]	C Expected occur several times in life cycle of an item	1C (High)	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [C416] Train pilots to check for updated weather information pre-flight and in-flight and to refrain from over-relying on the CDTI [C426] The FAA shall provide NOTAMS or other pilot notification to indicate that not all traffic are participants in CDTI- based applications [C418] Provide warnings and cautions regarding over-reliance on CDTI in avionics equipment manuals, pilot training manuals, and AIM [C416, C418] Provide placard on CDTI to indicate application / display only for situational awareness / advisory use [C416, C418]	1E (Medium)

5.2.2 Enhanced Visual Acquisition

Ground Rules and Assumptions

- Aircraft which are not appropriately equipped will not be displayed on the CDTI. These aircraft are considered non-participants for this application. I.e., the CDTI will not aid the pilot in visually acquiring these aircraft via "out-the-window" scans.
- Even if the CDTI ceases to display a traffic symbol for an aircraft due to loss of data or application malfunction, the pilot must still visually acquire this aircraft via "out-the-window" scans. In the case where the pilot does not detect that a traffic symbol is missing on the CDTI, the effect is the same as if that aircraft was a non-participant in the application.

Table 5-3: Enhanced Visual Acquisition Preliminary Hazards

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H19	Loss of All Traffic on In-Cockpit Display	Although traffic is present, no traffic is indicated on the Cockpit Display of Traffic Information (CDTI).	C33 Loss of primary and secondary navigation for the aircraft [External] C76 Aircraft / Vehicle Function: STP failure to receive ownship data [F1.1] C78 Aircraft / Vehicle Function: STP failure to process ownship data [F1.2] C77 Aircraft / Vehicle Function: ASSAP failure to receive ownship data [F1.1] C80 Aircraft / Vehicle Function: ADS-B receive subsystem failure to process received data [F1.3] C81 Aircraft / Vehicle Function: ADS-B receive subsystem does not correctly decode received messages [F1.3] C82 Aircraft / Vehicle Function: ADS-B receive	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic • 3 nmi longitudinal separation	Increases pilot workload slightly.	The same potential for collision exists with and without the application in this case. Aircraft receive traffic information from: i) other aircraft (i.e., air-to-air), ii) rebroadcast of information received on one link via the other (i.e., ADS-R / ground-to-air), and iii) broadcast of traffic information from non-ADS-B surveillance sources (i.e., TIS-B / ground-to-air).	4 (Minor) The pilot readily detects that application is not working when no information is shown on the display. However, if the display appears normal, but no traffic is shown, there may be an unidentified malfunction. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. The severity of the hazard is minor (4) given some additional pilot workload to determine the application has malfunctioned.	See and avoid procedures JH 50: Provide a backup system for surveillance or navigation [C33] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C78]	B Expected occur once a year per item. Likelihood of this hazard depends primarily on own ship equipment continuity with an expected MTTF of 5000 hours for low-end equipment.	4B (Medium)	The CDTI shall provide the air crew with an indication when: (a) Inadequate or invalid surveillance data would cause unacceptable traffic information display. (b) Inadequate or invalid own-ship data would cause unacceptable traffic information display (c) Application processing is not functioning normally. The RTCA shall define specific performance requirements for acceptable traffic information display. [C78,77,80,81,85] Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H19]	4D (Low) Failure is readily evident to a trained flight crew

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			subsystem does not correctly assemble reports [F1.3] C85 Aircraft / Vehicle Function: CDTI malfunction [F1.6]									
H44	Loss of One or More Aircraft on In-Cockpit Display	The presence of one or more aircraft is not indicated on the Cockpit Display of Traffic Information (CDTI). Except for a few aircraft, traffic presence is otherwise displayed to the air crew.	C200 Number of aircraft exceeds avionics ADS-B system capacity [F1.3, F1.5, F1.6] C90 Broadcast Services Function: BS failure to generate ADS-R report [F3.2, F3.3] C91 Link Specific Processing Function: LSP failure to output ADS-R message [F2.2, F2.3]	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited	Significant increase in pilot workload.	Pilot should still be looking out the window.	3 (Major) Loss of multiple but not all traffic on the display may not be readily detectable. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. The same potential for collision exists with and without the application in this case. The severity of the hazard is major (3) given the potentially significant additional pilot workload to determine that the application has malfunctioned.	See and avoid procedures [H44] All aircraft should be using "flying" lights.[H44] DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols [C200] fPR 3.2.3.4 ADS-R Surveillance Service The LSP/BCS receives ADS-B on each approved data link and provides corresponding ADS-R Messages	D Requires loss of multiple independent aircraft and not own-ship failure (which results in loss of all ships); likelihood of multiple independent failures is extremely remote.	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			C50 Pilot selects wrong range scale; traffic outside of selected range not shown [External] C175 ASSAP/CDTI Equipment random failure [F1.3, F1.6] C176 ASSAP/CDTI Equipment design fault [F1.3, F1.6] C178 Traffic not ADS-B participant and not covered by ground surveillance system and broadcast on TIS-B [External] C179 Data link interference [External] C180 Insufficient quality ADS-B/TIS-B to support ASA application [External]	visibility from the cockpit to other traffic • 3 nmi longitudinal separation				on the opposite datalinks. a. The LSP/BCS *shall* provide ADS-R data on those aircraft/vehicles actively transmitting ADS-B only on UAT to aircraft able to receive on 1090ES. b. The LSP/BCS *shall* provide ADS-R data on those aircraft/vehicles actively transmitting ADS-B only on 1090ES to aircraft able to receive on UAT. c. The ADS-R service *shall* meet the performance requirements for the Enhanced Visual Acquisition [C90, C91] DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols [C200] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175,C176] Pilots may use radio communications				

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [C178] ML 46: Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations. [C179] fPR 3.2.3.3 TIS-B Surveillance Service: a. The TIS-B Service *shall* support the following application: • Enhanced Visual Acquisition. [C180]				
H22	False Traffic Indication Displayed to Air Crew	Traffic is indicated on the Cockpit Display of Traffic Information (CDTI) when not appropriate. Non-existent traffic or traffic which is not of interest is displayed to the air crew.	C54 TIS-B message is sent for an ADS-B equipped aircraft (i.e., a case of transmitted TIS-B "shadow") [F3.2] C55 TIS-B message is sent on an erroneous target position report generated by FRUIT,	Marginal VMC GA pilot is on a VFR flight plan GA traffic are entering traffic pattern to land at an uncontrolled airport • Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace		Significant increase in pilot work load due to scanning for traffic near ownship that is not real (i.e., when "shadow" is on ownship.)	3 (Major) If a TIS-B shadow were shown near ownship (due to lacks of track correlation in ground system and failure in ASSAP to correlate and suppress TIS-B on ownship) or TIS-B false track were shown near ownship (due to reflections, mulitpath, etc), the air crew's workload could significantly increase due to scanning for traffic that is not real. The air crew could perceivably initially maneuver on the basis of the shadow in violation of the see and avoid	See and avoid procedures [H22] All aircraft should be using "flying" lights. [H22] fPR 3.2.3.3.9 False Report Rate a. The LSP/BCS *shall* not increase the false TIS-B Report rate relative to the	D (Extremely Remote) False tracks possible but probability is extremely remote based on implementation and verification of existing controls	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			reflections, multipath, or splits or a position report with an error that exceeds 1200 feet from the actual position of the aircraft. [F3.2]	• Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic • 3 nmi longitudinal separation			principle. (This is also covered under the application misuse hazard.) It is assumed that in such a case it would not choose a collision course with another (real) a/c which is depicted on the display. This hazard is rated as major due to the significant increase in workload.	false measurement rate of the contributing sensor or sensors used to produce the TIS-B Reports. [C55] ASA MAPS R3.172 The ASSAP ***shall*** include a correlation function that associates traffic data from different surveillance sources that relate to the same a/v track, [C54] ASA MAPS R3.172 The ASSAP ***shall*** include a correlation function that associates traffic data from different surveillance sources that relate to the same a/v track [C54] fPR 3.1.3.2 Processing g. The BCS shall associate ADS-B equipped targets with TIS-B Tracks. h. The BCS Function shall filter TIS-B Reports that have a corresponding ADS-B track on the same target. [C54]				

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H23	Loss of Altitude or Relative Altitude on In-Cockpit Display	A traffic symbol is shown, but traffic altitude or relative altitude is not shown on the Cockpit Display of Traffic Information (CDTI).	C42 Ownship Aircraft barometric sensor fails [External]	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic • 3 nmi longitudinal separation	Slight increase in pilot workload.		4 (Minor) Because a traffic symbol is still shown, the pilot is aware that traffic is present even if no altitude is shown. The application still provides a cue to the pilot to scan for traffic. Increased pilot workload may occur to scan up and down to locate traffic not associated with a specific altitude but at the correct bearing from ownship. Hazard severity is minor in this case.	All aircraft should be using "flying" lights. [H23] See and avoid procedures [H23]	C Expected occur several times in life cycle of an item	4C (Low)	The enhanced visual application shall notify the air crew when altitude information is missing. [C42]	4D (Low)
H24	Erroneous Altitude for One or More Targets Displayed to Air Crew	Erroneous altitude information for one or more targets is displayed to the air crew.	C87 Link Specific Processing Function: LSP corrupts TIS-B altitude data [F2.2, F2.3] C86 Broadcast Services Function: BS provides inaccurate TIS-B altitude data [F3.2, F3.3] C17 Aircraft / Vehicle Function: ADS-B	Aircraft are on a collision course. This may occur in any domain when pilots are trying to go to the same VOR intersection point.	Increases pilot workload slightly.	The following causes apply to Enhanced Visual Acquisition but not Enhanced Visual Approach: C86, C87 The same potential for collision exists with and without the application in this case.	4 (Minor) A pilot may believe that the opposite aircraft is above whereas it is actually at the same altitude. With incorrect altitude, pilots will still look in the correct direction for traffic and can more readily locate the traffic. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. The severity of the hazard is minor	See and avoid procedures [H24] Pilot training includes guidance to scan for other traffic at VOR intersections [H24] fPR 3.2.3.3.4 Integrity a. The probability that the LSP/BCS introduces hazardously misleading information into a TIS-B Report while being processed shall	C Expected occur several times in life cycle of an item	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			transmitter design flaw [F1.4] C18 ADS-B transmitter improperly configured / installed [F1.4]				(4) given the additional pilot workload. It is expected that see and avoid procedures will enable pilots to resolve and traffic conflicts before a large reduction in safety margin occurs.	not exceed 10^{-3} per hour of operation. [C86, C87] fPR 3.2.3.3.2 Position Accuracy c. The LSP/BCS *shall* provide TIS-B Reports with altitude accuracy of 148 feet with a 95% probability. [C86]				
H25	Erroneous Bearing for One or More Targets Displayed to Air Crew	The traffic symbol of one or more aircraft is displayed with a relative bearing error that is significantly different from that of other traffic near to it. This includes bearing errors relative to ownship position.	C7 Aircraft / Vehicle Function: Aircraft avionics / ADS-B transmitter provides inaccurate position C31 GPS / navigation positioning error for single aircraft [External] C5 Aircraft / Vehicle Function: Aircraft ADS-B avionics / ADS-B transmitter failure [F1.4]	Aircraft are on a collision course. This may occur in any domain when pilots are trying to go to the same VOR intersection point.	Significant increase in pilot workload.	Pilots interviewed regarding this hazard scenario consider erroneous bearing more significant than erroneous altitude. This is due to the additional areas a pilot must scan for traffic when there is a bearing error versus an altitude error. The same potential for collision exists with and without the application in this case.	3 (Major) Erroneous bearing may lead the pilot to initially look in the wrong direction for traffic. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. This hazard results in significant workload increase given the additional areas a pilot must scan for traffic based on a bearing error.	fPR 2.2.2.2.4.1 Horizontal Position d. The Aircraft/Vehicle shall provide horizontal position with a maximum error of less than or equal to 0.1 NM with a 95% probability to support the Enhanced Visual Approach application. [C7] Pilot see and avoid rules [H25] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31] fPR 3.2.2.2.2 Aircraft/Vehicle ADS-B Transmission The Aircraft/Vehicle transmits ADS-B Messages in support of all applications. The requirements in	D All hazard causes are mitigated to an extremely remote likelihood based on existing controls.	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								this section apply to all applications, unless a specific application is listed in the requirement text. 3.2.2.2.2.6 Availability a. Aircraft/Vehicle function shall provide a minimum availability of 0.9995 for non-redundant installations. [C5]				
H26	Erroneous Bearing for All Traffic Displayed to Air Crew	Traffic symbols for all traffic are displayed with approximately the same error in relative bearing, that is, the relative bearing of all traffic shown on the Cockpit Display of Traffic Information (CDTI) is rotated from the true relative bearing.	C92 Aircraft / Vehicle Function: Failure or inability to correct for the crab angle of the aircraft in high crosswinds	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic • 3 nmi longitudinal separation	Increases pilot workload slightly.		4 (Minor) Erroneous bearing for all traffic is readily detectable.	See and avoid procedures All aircraft should be using "flying" lights.	D Unlikely to occur, but possible in an item's life cycle	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H29	Erroneous Range for One or More Targets Displayed to Air Crew	The traffic symbol for one or more aircraft is displayed at the wrong range from ownship position.	C7 Aircraft / Vehicle Function: Aircraft avionics / ADS-B transmitter provides inaccurate position C31 GPS / navigation positioning error for single aircraft [External] C5 Aircraft / Vehicle Function: Aircraft ADS-B avionics / ADS-B transmitter failure	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the cockpit to other traffic • 3 nmi longitudinal separation	Significant increase in pilot workload.		3 (Major) At night, it is harder for pilots to gauge distance with other traffic. With incorrect range, pilots will still look in the correct direction for traffic and can more readily locate the traffic . Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. The same potential for collision exists with and without the application in this case. The severity of the hazard is major (3) given the additional pilot workload.	See and avoid procedures [H29] All aircraft should be using "flying" lights. [H29] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]	D All hazard causes are mitigated to an extremely remote likelihood based on existing controls.	3D (Low)		3D (Low)
H37	Erroneous Range Reference on In-Cockpit Display	The range reference (i.e., range scale) on the Cockpit Display of Traffic Information (CDTI) is incorrect. Traffic are shown at the wrong distance from ownship and may be closer to or farther from ownship.	C85 CDTI malfunction [F1.6]	• Aircraft is in a descent and arrival phase of flight; traffic is converging toward the same arrival sector corner post in busy terminal airspace • Pilot workload is relatively high given phase of flight and entails visually scanning out the window for traffic, performing arrival checklist procedures, configuring and maneuvering aircraft for descent, etc. • Pilot is only aircraft occupant and assumes full crew workload • Night time with no moon and marginal VMC; limited visibility from the	Slight increase in pilot workload.		4 (Minor) The pilot will readily detect the problem.	See and avoid procedures All aircraft should be using "flying" lights.	D Unlikely to occur, but possible in an item's life cycle	4D (Low)		4E (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
				cockpit to other traffic • 3 nmi longitudinal separation								

5.2.3 Enhanced Visual Approach

Per FAA Order 7110.65R, Section 7-4-1, "A visual approach is an ATC authorization for an aircraft on an IFR flight plan to proceed visually to the airport of intended landing; it is not an instrument approach procedure. Also, there is no missed approach segment. An aircraft unable to complete a visual approach shall be handled as any go-around and appropriate separation must be provided."

Table 5-4: Enhanced Visual Approach Preliminary Hazards

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H19	Loss of All Traffic on In-Cockpit Display	Although traffic is present, no traffic is indicated on the CDTI.	C33 Loss of primary and secondary navigation for the aircraft [External] C76 Aircraft / Vehicle Function: STP failure to receive ownship data [F1.1] C78 Aircraft / Vehicle Function: STP failure to process ownship data [F1.2] C77 Aircraft / Vehicle Function: ASSAP failure to receive ownship data [F1.1] C80 Aircraft / Vehicle Function: ADS-B receive subsystem failure to process received data [F1.3] C81 Aircraft / Vehicle Function: ADS-B receive subsystem does not correctly decode received messages [F1.3] C82 Aircraft / Vehicle Function: ADS-B receive subsystem does not correctly assemble reports C85 Aircraft / Vehicle Function: CDTI malfunction [F1.6]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly	The same potential for collision exists with and without the application in this case.	4 (Minor) The pilot readily detects that application is not working when no information is shown on the display. However, if the display appears normal, but no traffic is shown, there may be an unidentified malfunction. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual approach application. In addition to see and avoid procedures, ATC must provide traffic advisories when aircraft courses appear likely to converge. The severity of the hazard is minor (4) given some additional pilot workload to determine the application has malfunctioned.	See and avoid procedures JH 50: Provide a backup system for surveillance or navigation 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C78]	B Expected occur once a year per item. Likelihood of this hazard depends primarily on own ship equipment continuity with an expected MTTF of 5000 hours for low-end equipment.	4B (Medium)	The CDTI shall provide the air crew with an indication when: (a) Inadequate or invalid surveillance data would cause unacceptable traffic information display. (b) Inadequate or invalid own-ship data would cause unacceptable traffic information display (c) Application processing is not functioning normally. The RTCA shall define specific performance requirements for acceptable traffic information display. [C78,77,80,81,85] Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H19]	4D (Low) Failure is readily evident to a trained flight crew

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H44	Loss of One or More Aircraft on In-Cockpit Display	The presence of one or more aircraft is not indicated on the Cockpit Display of Traffic Information (CDTI). Except for a few aircraft, traffic presence is otherwise displayed to the air crew.	C200 Number of aircraft exceeds avionics ADS-B system capacity [F1.3, F1.5, F1.6] C90 Broadcast Services Function: BS failure to generate ADS-R report [F3.2, F3.3] C91 Link Specific Processing Function: LSP failure to output ADS-R message [F2.2, F2.3] C50 Pilot selects wrong range scale; traffic outside of selected range not shown [External] C175 ASSAP/CDTI Equipment random failure [F1.3, F1.6] C176 ASSAP/CDTI Equipment design fault [F1.3, F1.6] C178 Traffic not ADS-B participant and not covered by ground surveillance system and broadcast on TIS-B [External] C179 Data link interference [External] C180 Insufficient quality ADS-B/TIS-B to support ASA application [External]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase in pilot workload	Pilot should still be looking out the window. The same potential for collision exists with and without the application in this case.	3 (Major) Loss of multiple but not all traffic on the display may not be readily detectable. If the application ceased to display traffic on an adjacent parallel approach, the pilot may become confused as to the location of adjacent traffic. Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual approach application. In addition to see and avoid procedures, ATC must provide traffic advisories when aircraft courses appear likely to converge. The severity of the hazard is major (3) given the potentially significant additional pilot workload to visually locate traffic of concern and to determine that the application has malfunctioned.	See and avoid procedures All aircraft should be using "flying" lights. JH 50: Provide a backup system for surveillance or navigation 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols [C200] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175] Pilots may use radio communications to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [C178]	D Requires loss of multiple independent aircraft and not own-ship failure (which results in loss of all ships); likelihood of multiple independent failures is extremely remote.	3D (Low)	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H44] Processing and interface capacities shall be specified to accommodate the traffic densities and operating ranges for the most demanding application(s). [C200]	3E (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H22	False Traffic Indication Displayed to Air Crew	Traffic is indicated on the CDTI when not appropriate. Non-existent traffic or traffic which is not of interest is displayed to the air crew.	C54 TIS-B message is sent for an ADS-B equipped aircraft (i.e., a case of transmitted TIS-B "shadow") [F3.2]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase in pilot work load due to scanning for traffic near ownship that is not real.	There is an effect on workload if the "shadow" is on ownship.	3 (Major) May increase workload and distraction as flight crew tries to identify traffic that is non-existent.	See and avoid procedures [H22] ASA MASPS R3.172 The ASSAP ***shall*** include a correlation function that associates traffic data from different surveillance sources that relate to the same a/v track, [C54] fPR 3.1.3.2 g. The BCS shall associate ADS-B equipped targets with TIS-B Tracks. h. The BCS Function shall filter TIS-B Reports that have a corresponding ADS-B track on the same target. [C54]	D (Extremely Remote) False tracks possible but probability is extremely remote based on implementation and verification of existing controls	3D (Low)		3D (Low)
H23	Loss of Altitude or Relative Altitude on In-Cockpit Display	A traffic symbol is shown, but traffic altitude or relative altitude is not shown on the CDTI.	C42 Ownship aircraft barometric sensor fails[External]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) Because a traffic symbol is still shown, the pilot is aware that traffic is present even if no altitude is shown. The application still provides a cue to the pilot to scan for traffic. Increased pilot workload may occur to scan up and down to locate traffic not associated with a specific altitude but at the correct bearing from ownship. Hazard severity is minor in this case.	All aircraft should be using "flying" lights. See and avoid procedures 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied.	C Likelihood of losing barometric altitude sensor is no more than remote	4C (Low)	The enhanced visual application shall notify the air crew when altitude information is missing. [C42]	4D (Low) With notification the risk of hazard propagating to something more serious is extremely remote.

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H24	Erroneous Altitude for One or More Targets Displayed to Air Crew	Erroneous altitude information for one or more targets is displayed to the air crew.	C87 Link Specific Processing Function: LSP corrupts TIS-B altitude data [F2.2, F2.3] C86 Broadcast Services Function: BS provides inaccurate TIS-B altitude data [F3.2, F3.3] C17 Aircraft / Vehicle Function: ADS-B transmitter design flaw [F1.4] C18 ADS-B transmitter improperly configured / installed [F1.4]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) A pilot must maintain visual contact with the lead aircraft involved in a visual approach. Given this, erroneous altitude associated with the lead aircraft is readily detectable. If the altitude for an aircraft on an adjacent parallel approach is erroneous, pilot may increase slightly to detect that the application has malfunctioned.	See and avoid procedures [H24] Pilot training includes guidance to scan for other traffic at VOR intersections [H24] fPR 3.2.3.3.4 Integrity a. The probability that the LSP/BCS introduces hazardously misleading information into a TIS-B Report while being processed shall not exceed 10^{-3} per hour of operation. [C86, C87] fPR 3.2.3.3.2 Position Accuracy c. The LSP/BCS *shall* provide TIS-B Reports with altitude accuracy of 148 feet with a 95% probability. [C86]	C Expected occur several times in life cycle of an item	4C (Low)		4C (Low)
H25	Erroneous Bearing for One or More Targets Displayed to Air Crew	The traffic symbol of one or more aircraft is displayed with a relative bearing error that is significantly different from that of other traffic near to it. This includes bearing errors relative to ownship position.	C7 Aircraft / Vehicle Function: Aircraft avionics / ADS-B transmitter provides inaccurate position [F1.4] C31 GPS / navigation positioning error for single aircraft [External] C5 Aircraft / Vehicle Function: Aircraft ADS-B avionics / ADS-B transmitter failure [F1.4]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase in pilot workload	Pilots interviewed regarding this hazard scenario consider erroneous bearing more significant than erroneous altitude. This is due to the additional areas a pilot must scan for traffic when there is a bearing error versus an altitude error.	3 (Major) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the application is functioning properly. Unless the pilot is distracted, they should observe nearby traffic without relying on the enhanced visual application. Bearing errors associated with the lead aircraft involved in a visual approach are readily detectable. If the bearing of an aircraft on an adjacent parallel approach is erroneously shown on a collision course with ownship, the pilot may	fPR 2.2.2.2.4.1 Horizontal Position d. The Aircraft/Vehicle shall provide horizontal position with a maximum error of less than or equal to 0.1 NM with a 95% probability to support the Enhanced Visual Approach application. [C7] Pilot see and avoid rules [H25] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual	D All hazard causes are mitigated to an extremely remote likelihood based on existing controls.	3D (Low)		3D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
							immediately scan for traffic conflicts. The severity of the hazard is major (3) given the additional pilot workload to visually confirm that no traffic conflicts exist and to determine that the application has malfunctioned.	separation is being applied. [H25] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]				
H26	Erroneous Bearing for All Traffic Displayed to Air Crew	Traffic symbols for all traffic are displayed with approximately the same error in relative bearing, that is, the relative bearing of all traffic shown on the CDTI is rotated from the true relative bearing.	C92 Aircraft / Vehicle Function: Failure or inability to correct for the crab angle of the aircraft in high crosswinds [F1.3]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) Erroneous bearing for all traffic is readily detectable.	See and avoid procedures [H26] All aircraft should be using "flying" lights. [H26]	D Unlikely to occur, but possible in an item's life cycle	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H29	Erroneous Range for One or More Targets Displayed to Air Crew	The traffic symbol for one or more aircraft is displayed at the wrong range from ownship position.	C7 Aircraft / Vehicle Function: Aircraft avionics / ADS-B transmitter provides inaccurate position [F1.4] C31 GPS / navigation positioning error for single aircraft [External] C5 Aircraft / Vehicle Function: Aircraft ADS-B avionics / ADS-B transmitter failure [F1.4]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase in workload.		3 (Major) At night, it is harder for pilots to gauge distance with other traffic. A pilot may believe that there is sufficient range between ownship and the lead aircraft involved in a visual approach based on the range information provided in this application. If the distance between ownship and the lead aircraft is decreasing, a potential for wake upset exists. However, visual separation rules still apply and ATC still maintains awareness of traffic separation on visual approaches. ATC will issue wake turbulence cautionary advisories to aircraft on visual approaches as required.	fPR 2.2.2.2.4.1 Horizontal Position d. The Aircraft/Vehicle shall provide horizontal position with a maximum error of less than or equal to 0.1 NM with a 95% probability to support the Enhanced Visual Approach application. [C7] Pilot see and avoid rules [H25] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. [H25] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]	D All hazard causes are mitigated to an extremely remote likelihood based on existing controls.	3D (Low)		3D (Low)
H33	Loss of Traffic Horizontal Velocity on In-Cockpit Display	A velocity vector is not shown for one or more aircraft.	C175 ASSAP/CDTI equipment random failure [F1.3, F1.6] C176 ASSAP/CDTI design fault [F1.3, F1.6]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) The purpose of velocity vector is supplemental and lack of reported horizontal velocity would not hinder the visual approach. There may be a slight increase in pilot workload to determine that the application has malfunctioned.	See and avoid procedures [H33] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, 176]	D likelihood of individually losing one data item is extremely remote	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H34	Erroneous Traffic Horizontal Velocity on In-Cockpit Display	The velocity vector does not correctly indicate the direction and / or speed of flight.	C150 Aircraft avionics / ADS-B transmitter provides inaccurate horizontal velocity (other a/c) [F1.3, F1.5] C31 GPS / navigation positioning error for single aircraft [External] C151 Aircraft avionics / ADS-B receiver provides inaccurate horizontal velocity (own a/c) [F1.1, F1.2]	Night time IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase in workload.	Bearing errors are addressed in hazards H25 and H26.	3 (Major) At night, it is harder for pilots to gauge distance with other traffic. A pilot may believe that there is sufficient range between ownship and the lead aircraft involved in a visual approach based on speed and range information provided in this application. If the distance between ownship and the lead aircraft is decreasing, a potential for wake upset exists. However, visual separation rules still apply and ATC still maintains awareness of traffic separation on visual approaches. ATC will issue wake turbulence cautionary advisories to aircraft on visual approaches as required. The severity of the hazard is major (3) given the additional pilot workload to visually confirm that no traffic conflicts exist and to determine that the application has malfunctioned.	See and avoid procedures [H34] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. [H34] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]	D Existing procedures control the likelihood to extremely remote	3D (Low)		3D (Low)
H35	Erroneous Target Closure Rate or Ground Speed on In-Cockpit Display	Target closure rate is (a) presented for a different aircraft than the one highlighted on CDTI or (b) for the correct aircraft but the value is incorrect.	C175 ASSAP/CDTI equipment random failure [F1.3, F1.6] C176 ASSAP/CDTI design fault [F1.3, F1.6]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Significant increase of workload.		Major (3) Closure rate is expressed as the difference in speed between an aircraft selected by the air crew and ownship. If closure rate erroneously indicates that ownship is gaining on the lead aircraft, the pilot may slow down in order to maintain safe separation on a visual approach. Alternatively,	See and avoid procedures [H35] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being	D Existing procedures control the likelihood to extremely remote	3D (Low)		3D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
							a pilot may execute a missed approach unnecessarily based on erroneous closure rate information.	applied. [H35] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176]				
H36	Erroneous Target Highlighting on In-Cockpit Display	A different target is highlighted than the one intended by crew	C85 CDTI malfunction [F1.6] C57 Air crew selects wrong target on the display [External]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) The pilot may become temporarily confused if the displayed information for the (erroneously) highlighted target conflicts with out-the-window observation of traffic dynamics.	See and avoid procedures [H36] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. [H36] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C85]	D Existing procedures control the likelihood to extremely remote	4D (Low)		4D (Low)
H37	Erroneous Range Reference	The range reference displays at the wrong distance from own a/c symbol	C85 CDTI malfunction [F1.6]	IFR traffic cleared for visual approaches 3 nmi longitudinal separation Marginal VMC Independent, parallel approach operations to two runways spaced 4,300 ft laterally	Increases pilot workload slightly		4 (Minor) If the displayed range scale is changed or otherwise erroneous, a pilot may select the wrong aircraft for obtaining closure rate or other traffic information. The pilot may become temporarily confused if the displayed information for the highlighted target conflicts with out-the-window observation of traffic dynamics.	See and avoid procedures [H37] 7110.65 (Section 7-2-1): Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied. [H37] DO-289 Table 3-20 Subsystem integrity and availability risk	D Existing procedures control the likelihood to extremely remote	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								requirements [C85]				

5.2.4 Airport Surface Situational Awareness (ASSA)

Table 5-5: ASSA Preliminary Hazards

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H42	Missing Ownship Symbol on In-Cockpit Display	CDTI does not display ownship symbol	C175 ASSAP/CDTI Equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI Equipment design flaw [F 1.6, F1.3]	Controlled airport Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	Slight increased workload (confusion / distraction)		4 (Minor) If ownship symbol is not displayed, the airport surface moving map functionality may not work. Missing ownship may cause a slight increase in pilot workload to determine that the application is malfunctioning.	Pilot may stop to ask ATC direction [H42] Crew cross check with other redundant info. (e.g., visual, paper maps, mental model). [H42] DO-289 Table 3-20 Subsystem integrity and availability risk requirements[C175, C176]	D The likelihood of design error related causes (in particular, failure to display ownship symbol) in combination with the system state (i.e., marginal VMC at night time) is qualitatively unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)
H43	Displayed Location of Ownship is Wrong on In-Cockpit Display	The location of ownship displayed on the CDTI is wrong. (a) The position source used to determine own-ship position (e..g., position, ground speed, heading)is significantly in error. (b) The CDTI incorrectly displays the state information.	C175 ASSAP/CDTI Equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI Equipment design faultflaw [F 1.6, F1.3] C31 GPS / navigation positioning error for single aircraft [F1.1] C78 STP failure to process ownship data [F1.1]	Controlled airport Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	Increased workload for crew		4 (Minor) If ownship location is not shown in the correct place on the airport map, the pilot may become temporarily confused until airport signage, paper maps, or other visual cues indicate true ownship location. Hazard severity is minor given a slight increase in crew workload.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H43] Airport Movement Area signage DO-289 Table 3-20 Subsystem integrity and availability risk requirements[C78, C176] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]	D The likelihood of design error related causes (in particular, STP fault to process ownship symbol) in combination with the system state (i.e., marginal VMC at night time) is qualitatively unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H44	Loss of One or More Aircraft on In-Cockpit Display	The presence of one or more aircraft is not indicated on the Cockpit Display of Traffic Information (CDTI). Except for a few aircraft, traffic presence is otherwise displayed to the air crew.	C9 Number of aircraft exceeds ADS-B system capacity C90 Broadcast Services Function: BS failure to generate ADS-R report [F 3.3] C91 Link Specific Processing Function: LSP failure to output ADS-R message [F 3.3.2] C175 ASSAP/CDTI Equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI Equipment design fault [F 1.6, F1.3] C178 Traffic not ADS-B participant and not covered by ground surveillance system and broadcast on TIS-B C179 Data link interference C180 Insufficient quality ADS-B/TIS-B to support ASA application	Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	Significant increase in pilot workload		4 (Minor) Provided traffic is in the pilot's field of vision, the pilot should visually detect traffic. Even if the pilot did not immediately see nearby traffic, the relatively slow surface speeds leave pilots more time to react to see and avoid traffic. High speed taxiways are used to expedite aircraft turning off the runway after landing, thus reducing runway occupancy time. When considering a high speed taxiway, a controlled airport is assumed where ATC would not permit other aircraft or vehicles to cross the taxiway when a lander is exiting the runway.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H44] Pilots may use radio communications to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [H44] Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations [C9, C90, C91]. fPR 3.2.3.4 ADS-R Surveillance Service The LSP/BCS receives ADS-B on each approved data link and provides corresponding ADS-R Messages on the opposite datalinks. [C90] fPR 3.2.3.4.4 ADS-R Surveillance Service Coverage a. ADS-R shall be user-accessible within the coverage volumes designated for this service. b. ADS-R coverage shall include, but not be limited to the following: • In en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3 G(3) and (4) • The aircraft movement area at airports with a	D The likelihood of design error related causes (in particular, random failure in ASSAP) in combination with the system state (i.e., conflict exists for an a/c on final approach in marginal VMC at night) is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								control tower. [C90] fPR 3.1.5.2 Maintenance Function Processing [C91] fPR 3.2.4.1.6 Automation System Capacity a. The ATC Automation Function shall have sufficient capacity to process the ADS-B peak and steady state target capacity loading. [C9] fPR 3.2.3.2.6 Capacity a. The LSP/BCS shall process all ADS-B Messages received from aircraft/vehicles within ADS-B surveillance coverage (Reference section 3.2.3.2.5).[C9] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176] Pilots may use radio communications to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [C178] ML 46: Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations [C179] fPR 3.2.3.4 ADS-R Surveillance Service c. The ADS-R service				

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								shall meet the performance requirements for ASSA [C180]				
H45	Erroneous Traffic Position on In-Cockpit Display	Traffic positions shown on the CDTI are wrong relative to ownship and/or the runway map.	C175 ASSAP/ CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3] C31 GPS / navigation positioning error for single aircraft [F1.1] C78 STP failure to process ownship data [F1.1] C181 Airport map database is incorrect	Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic is stationary or moving at slow speeds	(a) Slight increased workload for crew		4 (Minor) The CDTI may show an aircraft position at the hold short line for a runway when the aircraft has stopped some distance before the actual line. A pilot may believe there is more distance to stop behind the displayed aircraft than what exists.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H45] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C78, C175, C176] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31] The Flight Information Publication (FLIP) is updated every 56 days to account for airport map changes such as those due to magnetic drift. [C181] Airports must be resurveyed whenever there is an Airport Movement Area change. [C181] fPR 3.2.2.2.3.2 Airport Map: a. AMDB airport data shall be formatted in accordance with RTCA DO-291,	C The likelihood of design error related causes (in particular, random failure in ASSAP/CDTI) in combination with the system state (i.e., conflict exists between a/c on final approach and an a/v on the ground in marginal VMC) is qualitatively expected to occur several times in the life cycle of the avionics	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								Interchange Standards for Terrain, Obstacle, and Aerodrome Mapping Data. b. The AMDB shall be in accordance with RTCA DO-272, User Requirements for Aerodrome Mapping Information, and DO 200-A, Standards for Processing Aeronautical Data. c. The Aircraft/Vehicle shall include airport map databases for intended United States, civil and joint-use, towered-airports within the areas of operation. AMDB production and maintenance capability shall be expandable and scalable to accommodate the airports at which the operator desires to employ the Airport Surface Situational Awareness and Final Approach and Runway Occupancy Awareness applications. [C181]				
H32	Erroneous Traffic ID is Shown with One or More Traffic Symbols on In-Cockpit Display	Incorrect Traffic ID is shown with one or more traffic symbols, or the crew misreads the IDs or misinterprets the association between IDs and traffic symbols	C175 ASSAP/CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3]	Aircraft on final approach in marginal VMC at night	(a) Increase flight crew workload (confusion) (b) Potentially erroneous maneuver (e.g., following the wrong / mislabeled		4 (Minor) Provided that traffic symbols are still displayed, erroneous traffic IDs are not critical in this application. Air crew work load may increase slightly in trying to determine correct ID.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H32] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176]]	C The likelihood of design error related causes (in particular, random failure in ASSAP/CDTI) in combination with the system state (i.e., conflict exists between a/c on final approach and a/v on the ground in marginal VMC) is qualitatively expected to occur several	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
					traffic) This could cause confusion when trying to correlate traffic with other information.				times in the life cycle of the avionics			
H22	False Traffic Indication Displayed to Air Crew	Traffic is indicated on the CDTI when not appropriate. Non-existent traffic or traffic which is not of interest is displayed to the air crew.	C175 ASSAP/CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3]	Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	(a) Erroneous maneuver (b) Increased workload for crew		4 (Minor) False traffic may cause increased pilot workload to verify that traffic is false.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H22] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176]	D The likelihood of design error related causes (in particular, random failure in ASSAP) in combination with the system state (i.e., marginal VMC at night) is qualitatively expected to unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)
H47	Incorrect Airport Map on In-Cockpit Display	Airport map is out-of-date or otherwise inaccurate (e.g., taxiways and / or runways may be mis-labeled or the wrong map is shown for a particular airport).	C181 Airport map database is incorrect.	Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds airport	Increased workload for crew		4 (minor) Airport maps that are out-of-date may not show modifications to taxiway numbering or taxiway closures.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H47] The Flight Information Publication (FLIP) is updated every 56 days to account for airport map changes such as those due to magnetic drift [C181]. Airports must be resurveyed whenever there is an Airport Movement Area change. [C181] fPR 3.2.2.2.3.2 Airport Map: a. AMDB airport data *shall* be formatted in accordance with RTCA DO-291, *Interchange*	D The likelihood of an error in airport map in combination with the system state and existing controls is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								Standards for Terrain, Obstacle, and Aerodrome Mapping Data. b. The AMDB *shall* be in accordance with RTCA DO-272, *User Requirements for Aerodrome Mapping Information*, and DO 200-A, *Standards for Processing Aeronautical Data*. c. The Aircraft/Vehicle *shall* include airport map databases for intended United States, civil and joint-use, towered-airports within the areas of operation. d. AMDB production and maintenance capability *shall* be expandable and scalable to accommodate the airports at which the operator desires to employ the Airport Surface Situational Awareness and Final Approach and Runway Occupancy Awareness applications. [C181]				
H48	In-cockpit Display Orientation Unclear or Misleading	Display orientation is unclear or misleading. The orientation may be north up, track-up, or course up and does not necessarily adjust with ownship direction.	C85 CDTI malfunction	Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	Slight increase in pilot workload		4 (Minor) A confusing display orientation may lead to increased pilot workload in trying to interpret display.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H48] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C85]	D The likelihood of design error related misleading orientation in combination with the system state (i.e., ASSA in marginal VMC) is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

5.2.5 Final Approach and Runway Occupancy Awareness (FAROA)

Ground Rules and Assumptions

- FAROA applies to aircraft on or near the runway surface up to 1000 ft AGL on final approach, runway surface vehicular traffic, traffic taxiing over or crossing runways.
- When FAROA is not conduced during taxiing, the ASSA application may be used.
- FAROA applies to aircraft / vehicle speeds during taxiing, takeoff, and landing and all aircraft types (military, GA, commercial) at controlled and uncontrolled airports and airports with low to high density traffic.
- Cockpit display includes runway environment and other traffic
- Air crew determines runway occupancy with the aid of display; supports go-around decisions
- Includes surface moving map with runway layout map (may or may not include taxiways and maps)
- FAROA does not include any required alerts; alerting functionality which may be an enhancement to FAROA is excluded from this analysis.
- Hazards associated with vendor-specific CDTI designs entailing optional features such as use of picture-in-picture features are excluded from this analysis
- Per Section F.1.2.2.1 of the RTCA DO-289 ASA MASPS, ATC procedures are not expected to change based on this application
- There may be conflicting information from ASDE-3/AMASS/ASDE-X (used by ATC) versus the FAROA application; however, there is no safety effect due to this situation.
- The following FAROA application features are also used in the enhanced visual acquisition and / or enhanced visual approach applications. These common features are not re-assessed as part of the FAROA application, because they are not generated or used differently in FAROA, nor are there any phase-of-flight or domain-specific differences: target highlighting, closure rate, range to target.
- Potential hazards associated with transitioning between the ASSA and FAROA applications were not examined
- Based on Section F.3.1 of the RTCA DO-289 ASA MASPS, it is assumed that the air crew will not use the FAROA application during takeoff roll at which time misleading information may lead to aborted takeoffs.

System States

- IFR and VFR traffic can "mix" in the terminal domain. VFR and IFR traffic may be as close as 500 ft vertically. Depending on aircraft weight class and class of airspace, VFR and IFR traffic may be as close as 1 1/2 miles down to “target resolution” for lateral separation from an ATC perspective.

Table 5-6: FAROA Preliminary Hazards

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H22	False Traffic Indication Displayed to Air Crew	Traffic is indicated on the CDTI when not appropriate. Non-existent traffic or traffic which is not of interest is displayed to the air crew.	C175 ASSAP/CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3]	Aircraft on final approach in marginal VMC at night	(a) Unnecessary go-around maneuver (b) Increased workload for crew E# Increased controller workload		4 (Minor) Traffic may be displayed on a runway when there is not any. If the aircraft on approach is far enough from the airport (i.e., prior to receiving ATC clearance to land), the pilot may contact ATC to verify that the runway is or is not occupied. The pilot may continue to check the runway for traffic once the airport is in sight. If ATC has cleared the pilot to land, and the FAROA application subsequently indicates traffic is on the intended runway, the pilot will look out the window and possibly contact ATC to verify the runway status. Either visual observation or ATC may indicate that the FAROA application is in error. If the pilot cannot visually verify that no traffic is on the runway due to limited visibility at night or in marginal VMC, the pilot may execute a go-around unecessarily despite ATC assurance that no traffic is on the runway. The unecessary go-around results in pilot and ATC workload increases. ATC and pilots must always be prepared to handle go-around maneuvers regardless of this application.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H22] DO-289 Table 3-20 Subsystem integrity and availability risk requirements[C175, C176]	D The likelihood of design error related causes (in particular, random failure in ASSAP) in combination with the system state (i.e., marginal VMC at night) is qualitatively expected to unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H44	Loss of One or More Aircraft on In-Cockpit Display	The presence of one or more aircraft is not indicated on the Cockpit Display of Traffic Information (CDTI). Except for a few aircraft, traffic presence is otherwise displayed to the air crew.	C9 Number of aircraft exceeds ADS-B system capacity C90 Broadcast Services Function: BS failure to generate ADS-R report [F 3.3] C91 Link Specific Processing Function: LSP failure to output ADS-R message [F 3.3.2] C175 ASSAP/CDTI Equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI Equipment design fault [F 1.6, F1.3] C178 Traffic not ADS-B participant and not covered by ground surveillance system and broadcast on TIS-B C179 Data link interference C180 Insufficient quality ADS-B/TIS-B to support ASA application	Aircraft on final approach in marginal VMC at night The runway on which an approaching aircraft intends to land is occupied by a small airplane without bright lights ATC tower has limited visibility to runway due to marginal VMC and night time	Significant increase in pilot workload		Minor (4) If the pilot was looking out the window, he should see the runway occupant and be able to avoid collision. In an instrument approach scenario, a large aircraft may break out of a cloud layer at 200 ft decision height on an ILS. At a 200 ft decision height, there is not a lot of time to react and maneuver to avoid traffic. If the CDTI showed traffic on the runway and subsequently lost or dropped that traffic, the pilot on approach may believe the runway is clear. For a collision to occur, ATCT would have to not see that an aircraft is on the runway (Note: It may be difficult to tell whether an aircraft is holding short of or actually on a runway at night). A large aircraft coming in fast has less time to react; and it is hard to pull up due to aircraft weight and flap configuration. If the tail of the aircraft on the runway is facing the lander, it may be harder to the lander to see the runway occupant due to the lack of aircraft surface area to visualize.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H44] Pilots may use radio communications to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [H44] Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations [C9, C90, C91]. fPR 3.2.3.4 ADS-R Surveillance Service The LSP/BCS receives ADS-B on each approved data link and provides corresponding ADS-R Messages on the opposite datalinks. [C90] fPR 3.2.3.4.4 ADS-R Surveillance Service Coverage a ADS-R shall be user-accessible within the coverage volumes designated for this service. b. ADS-R coverage shall include, but not be limited to the following: • In en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3 G(3) and (4) • The aircraft movement area at airports with a control tower. [C90]	D The likelihood of design error related causes (in particular, random failure in ASSAP) in combination with the system state (i.e., conflict exists for an a/c on final approach in marginal VMC at night) is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								fPR 3.1.5.2 Maintenance Function Processing [C91] fPR 3.2.4.1.6 Automation System Capacity a. The ATC Automation Function shall have sufficient capacity to process the ADS-B peak and steady state target capacity loading. [C9] fPR 3.2.3.2.6 Capacity a. The LSP/BCS shall process all ADS-B Messages received from aircraft/vehicles within ADS-B surveillance coverage (Reference section 3.2.3.2.5). [C9] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176] Pilots may use radio communications to monitor other pilots announce their intentions (e.g., approach to / landing at an airport) to other traffic. [C178] ML 46: Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations [C179] fPR 3.2.3.4 ADS-R Surveillance Service c. The ADS-R service *shall* meet the performance requirements for ASSA. [C180]				

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H45	Erroneous Traffic Position on In-Cockpit Display	Traffic positions shown on the CDTI are wrong relative to ownship and/or to the runway map.	C175 ASSAP/ CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3] C31 GPS / navigation positioning error for single aircraft [F1.1] C78 STP failure to process ownship data [F1.1] C181 Airport map database is incorrect	Uncontrolled airport Marginal VMC Aircraft or other traffic present on runway	Large reduction in safety margin Significant traffic position errors could make it difficult to correlate traffic with other information and lead crew to making incorrect decisions.		2 (Hazardous) Traffic positions are relative to runways on a displayed map. If the position of an aircraft that is really on a runway is incorrectly shown elsewhere, the hazard severity is hazardous (2). An incursion may occur between a lander and ground traffic on the same runway, particularly if the airport is uncontrolled. Ground traffic may judge that there is sufficient time to cross an active runway based on the displayed position of an aircraft on final approach.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H45] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C78, C175, C176] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31] The Flight Information Publication (FLIP) is updated every 56 days to account for airport map changes such as those due to magnetic drift. [C181] Airports must be resurveyed whenever there is an Airport Movement Area change. [C181] fPR 3.2.2.2.3.2 Airport Map a. AMDB airport data <u>*shall*</u> be formatted in accordance with RTCA DO-291, *Interchange Standards for Terrain, Obstacle, and Aerodrome Mapping Data.* b. The AMDB <u>*shall*</u> be in accordance with RTCA DO-272, *User Requirements for Aerodrome Mapping Information,* and DO 200-A, *Standards for Processing Aeronautical Data.* c. The Aircraft/Vehicle <u>*shall*</u> include airport map databases for intended United States, civil and joint-use, towered-airports within the areas of operation. *d. AMDB production and*	D The likelihood of design error related causes (in particular, random failure in ASSAP/CDTI) in combination with the system state (i.e., conflict exists between a/c on final approach and an a/v on the ground in marginal VMC at uncontrolled airport) is qualitatively expected to occur several times in the life cycle of the avionics.	2D (Medium)	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H45]	2E (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								maintenance capability shall be expandable and scalable to accommodate the airports at which the operator desires to employ the Airport Surface Situational Awareness and Final Approach and Runway Occupancy Awareness applications. [C181]				
H32	Erroneous Traffic ID is Shown with One or More Traffic Symbols on In-Cockpit Display	Incorrect Traffic ID is shown with one or more traffic symbols.	C175 ASSAP/CDTI equipment random failure [F 1.6, F1.3] C176 ASSAP/CDTI design fault [F 1.6, F1.3]	Controlled airport Night time Marginal VMC Rainy conditions Poor airport lighting Ground traffic moving at slow speeds	None	This could cause confusion when trying to correlate traffic with other information.	5 (No effect) Traffic identification is not a required part of this procedure per DO-289 Table F-1.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H32] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C175, C176]]	C The likelihood of design error related causes (in particular, random failure in ASSAP/CDTI) in combination with the system state (i.e., conflict exists between a/c on final approach and a/v on the ground in marginal VMC) is qualitatively expected to occur several times in the life cycle of the avionics	5C (Low)		5C (Low)
H34	Erroneous Traffic Horizontal Velocity on In-Cockpit Display	The velocity vector does not correctly indicate the direction or movement of flight.	C150 Aircraft avionics / ADS-B transmitter provides inaccurate horizontal velocity (other a/c) C31 GPS / navigation positioning error for single aircraft C151 Aircraft avionics / ADS-B receiver provides inaccurate horizontal velocity	Aircraft on final approach in marginal VMC at night Traffic on runway occupied	May increase workload slightly		4 (Minor) Horizontal velocity is not a required element for this procedure per DO-289 Table F-1	fPR 3.2.2.2.2.4.2 Horizontal Velocity a. The Aircraft/Vehicle *shall* provide a horizontal velocity with a maximum error of less than or equal to 9.8 feet per second with a 95% probability to support the Conflict Detection, Airport Surface Situational Awareness, and Final Approach and Runway Occupancy applications. [C150,	D The likelihood of design error related causes (in particular, random failure in ASSAP/CDTI) in combination with the system state (i.e., conflict exists with a non-stationary a/v in marginal	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			(own a/c)					C151] On-board GPS integrity monitoring per TSO-C129 or TSO-C145 [C31]	VMC) is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle			
H39	Erroneous Air / Ground Status on In-Cockpit Display	Display indicates traffic is on the ground when it is really airborne or vice versa.	C59 Aircraft avionics / ADS-B transmitter provides inaccurate Air / Ground Status	Aircraft on final approach in marginal VMC at night	Slight increase in pilot workload.		4 (Minor) Erroneous air / ground status may result in a slight pilot work load increase. If an aircraft is shown as on the ground, but the displayed speed is 120 kts, for example, then the erroneous air / ground status is readily detectable. This applies to aircraft shown as airborne but with a speed that is too low.	DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C59]	C The likelihood of design error related to providing an incorrect air / ground status in combination with the system state (i.e., conflict exists for an a/c on final approach in marginal VMC at night) is qualitatively expected to occur several times in the life cycle of the avionics.	4C (Low)		4C (Low)
H47	Incorrect Airport Map on In-Cockpit Display	Airport map is out-of-date or otherwise inaccurate (e.g., taxiways and / or runways may be mis-labeled or the wrong map is shown for a particular airport).	C181 Airport map database is incorrect	Snow on ground which obstructs runway signage Aircraft on final approach in marginal VMC at night Runway occupied	potential minor increase in workload for crew		4 (Minor) Airport maps that are out-of-date may not show modifications to runway length or runway closures. Also, if runways are labeled incorrectly (e.g., 21L is labeled as 21R), a pilot may head toward or land on the wrong runway.	Airport signage, paper maps, and other visual cues to discern ownship location on airport [H47] The Flight Information Publication (FLIP) is updated every 56 days to account for airport map changes such as those due to magnetic drift. [C181] Airports must be resurveyed whenever there is an Airport Movement Area change. [C181] fPR 3.2.2.2.3.2 Airport Map [C181]	D The likelihood of an error in airport map in combination with the system state and existing controls is qualitatively estimated as unlikely to occur, but possible in an avionics life cycle	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								a. AMDB airport data shall be formatted in accordance with RTCA DO-291, *Interchange Standards for Terrain, Obstacle, and Aerodrome Mapping Data.* b. The AMDB shall be in accordance with RTCA DO-272, *User Requirements for Aerodrome Mapping Information*, and DO 200-A, *Standards for Processing Aeronautical Data.* c. The Aircraft/Vehicle shall include airport map databases for intended United States, civil and joint-use, towered-airports within the areas of operation. d. AMDB production and maintenance capability shall be expandable and scalable to accommodate the airports at which the operator desires to employ the Airport Surface Situational Awareness and Final Approach and Runway Occupancy Awareness applications.				
H41	Display Range to Airport Inaccurate on In-Cockpit Display	An auto-zoom function automatically adjusts the display range based on aircraft distance from airport. As the aircraft approaches the airport, the runway appears larger and larger on the display. In this scenario, the auto-zoom malfunctions or was designed incorrectly, causing	C85 CDTI malfunction [F1.3]	Aircraft on final approach in marginal VMC at night	Slight increase in pilot workload.		4 (Minor) A pilot may believe he is closer to the airport than he actually is if the display range to airport is wrong. The problem is readily detectable via visual observation. Pilot work load may increase slightly to manually adjust the display based on range to airport.	VAPIs (red and white visual approach indicator lights) indicate when an aircraft is too low or high for a safe approach On an ILS approach, instrumentation will indicate a discrepancy if the pilot descends based on wrong auto zoom.	D The likelihood of design error related causes (i.e., CDTI display malfunction) in combination with the system state (i.e., in final approach under marginal VMC) is qualitatively	4D (Low)		4D (Low)

No	Hazard Title	Hazard Description	Causes	Worst Case System State	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
		the display range to be inaccurate.							estimated as unlikely to occur, but possible in an avionics life cycle			

5.2.6 Conflict Detection

Definitions

The following application terminology is excerpted from the RTCA DO-289 ASA MASPS, Appendix D (Page D-121):

- Collision Avoidance Zone (CAZ): Zone used by the system to predict a collision or dangerously close spacing. The CAZ is defined by the sum of Assured Collision Avoidance Distance (ACAD) and position uncertainties. Collision Avoidance Zone (CAZ) alert: Notifies aircraft crew that a CAZ penetration will occur if immediate action is not taken. Aggressive avoidance action is essential.
- Conflict: A predicted violation of parameterized minimum separation criteria for adverse weather, aircraft traffic, special use airspace, other airspace, turbulence, noise sensitive areas, terrain and obstacles, etc. There can be different "levels" or "types" of conflict based on how the parameters are defined. Criteria can be either geometry-based or time- based. This document only addresses aircraft traffic. See Traffic Conflict below.
- Conflict Avoidance: The act of detecting a conflict and executing a resolution to avoid that conflict.
- Conflict Detection: The discovery of a conflict as a result of a computation and comparison of the predicted flight paths of two or more aircraft for the purpose of determining conflicts. (ICAO)
- Conflict Detection Zone (CDZ): Zone used by the system to detect conflicts. The CDZ is defined by the sum of ANSD, position uncertainties, and trajectory uncertainties. By attempting to maintain a measured separation no smaller than the CDZ, the system assures that the actual separation is no smaller than the ANSD.
- Conflict Detection Zone (CDZ) alert: An alert issued at the specified look ahead time prior to CDZ penetration if timely action is not taken. Timely avoidance action is required.
- Low Level Alert: An optional alert issued when CDZ penetration is predicted outside of the CDZ alert boundary.

Ground Rules and Assumptions:

- The Conflict Detection (CD) application is not a collision avoidance system (i.e., it does not provide instructions to the pilot regarding how to avoid potential collision). Instead, CD alerts the pilot to potential conflicts.
- CD is not the sole means of detecting predicted conflicts between aircraft (e.g., pilots, controllers, and TCAS provide other means of detecting conflicts)
- Optional outputs for this application are excluded from this safety assessment (Note: These optional outputs are denoted by "d" (for desired) in Table XX in Volume I)
- Additionally, the Low Level Alert, designated as an optional alert in DO-289 Vol. 1, section D.2.2.2, is also excluded from this analysis
- In accordance with the ASA MASPS, no changes to procedures, separation responsibilities, or clearances are expected based on the implementation of this application.
- The pilot is not supposed to maneuver on the sole basis of alerts from the CD application.
- Section D.1.3.2.2 of the ASA MASPS indicates that the CD application may be integrated into the aircraft's navigation display. Impacts to navigation system display functionality and performance based on integrating CD functionality within the display are not evaluated in this analysis.
- Conflict Avoidance Zone (CAZ) alerts have visual and aural components, whereas Conflict Detection Zone (CDZ) alerts have only a visual component. It is assumed that CDZ alerts cannot be mistaken for CAZ alerts and vice versa. See ASA MASPS Section D.1.3.1 for requirements to uniquely annunciate CAZ alerts.
- Mid-air collision likelihood is greater for VFR traffic at non-towered airports or towered airports during hours when the tower is closed.
- Per the ASA MASPS, this application can transition from a "no alert" state to a CAZ alert without first issuing a CDZ alert. A CAZ alert may be issued without a preceding CDZ alert when an aircraft makes a sudden turn out of one traffic stream toward an adjacent parallel stream, for example.
- Section D.1.2.2.1 of the ASA MASPS indicates that failures and malfunctions in the CD application will result in a "return to the current level of safety for the appropriate environment, which is considered acceptable." This premise was not assumed in this PHA. Instead, safety effects and pilot workload effects due to misleading or erroneous information from the CD application were considered.

Table 5-7: Conflict Detection Preliminary Hazards

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H49	CDZ Alert Not Issued Although a Conflict Exists	A Conflict Detection Zone (CDZ) alert is not issued although a conflict exists. Traffic is still shown correctly.	C182 - Number of aircraft exceeds CD application processing capacity (e.g., altitude / range filters may be set such that too many aircraft are processed for this application to handle) [F1.6] C183 - Alert not issued for conflict existing with traffic outside of selected display area. [F1.6] C184 - Visual component of CDZ alert does not work [F1.3] C304 Alert is lost in selecting the de-clutter function. [F1.6] C305 Alerts have been disabled. [F1.6] C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.6]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped High traffic volume due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert		The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is unlikely to maintain a collision course toward traffic which is shown on the display	5 (No effect) Using the see and avoid procedure, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. Unless the pilot is distracted, they should observe nearby traffic without relying on alerts from the CD application. The same potential for collision exists with and without the CD application in this case.	DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols[C182] DO-289 3.3.3.1.6.2 CDTI Installations that support the CD application … shall (R3.268) provide off-display alerted traffic bearing indicator [C183] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C184, C187] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures – (AIM) [H49]	C Existing requirements already cover the most likely causes of this failure and design assurance covers potential latent problems. The likelihood of design error related causes (in particular exceeding processing capacity) in combination with the system state (i.e., a conflict that should have generated an alert) is qualitatively expected to occur several times in the life cycle of the avionics.	5C (Low)	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H49, Update AIM] The Conflict Detection Application shall provide an indication that alerts have been disabled [F1.6]	5C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H50	CAZ Alert Not Issued Although a Potential Collision Exists	A Collision Avoidance Zone (CAZ) alert is not issued although a conflict exists. Traffic is still shown correctly.	C182 - Number of aircraft exceeds CD application processing capacity (e.g., altitude / range filters may be set such that too many aircraft are processed for this application to handle) [F1.6] C183 - Alert not issued for conflict existing with traffic outside of selected display area. [F1.6] C184 - Visual component of CDZ alert does not work [F1.3] C304 Alert is lost in selecting the de-clutter function. [F1.6] C305 Alerts have been disabled. [F1.6] C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.6]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped High traffic volume due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert		The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is unlikely to maintain a collision course toward traffic which is shown on the display	5 (No effect) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. Unless the pilot is distracted, they should observe nearby traffic without relying on alerts from the CD application. The same potential for collision exists with and without the CD application in this case. If the aircraft are TCAS equipped, then the hazard severity entails no safety effect (5).	DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols[C182] DO-289 3.3.3.1.6.2 CDTI Installations that support the CD application … shall (R3.268) provide off-display alerted traffic bearing indicator [C183] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C184, C187] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures – (AIM) [H50]	C Existing requirements already cover the most likely causes of this failure and design assurance covers potential latent problems. The likelihood of design error related causes (in particular exceeding processing capacity) in combination with the system state (i.e., a conflict that should have generated an alert) is qualitatively expected to occur several times in the life cycle of the avionics.	5C (Low)	The Conflict Detection Application shall provide an indication that alerts have been disabled. [F1.6]	5C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H51	CDZ Alert Issued Late	A Conflict Detection Zone (CDZ) alert is issued late	C185 Conflict Detection Processor/Alert soft failure [F1.3]. C308 End-to-end system latency is excessive. [F1.1 – F1.6] C186 CDZ and/or CAZ alert thresholds set incorrectly. [F1.3.12] C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.3.12]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert	Slight increase in workload.	Airlines are mostly TCAS equipped and fly IFR, under air traffic control. IFR traffic has potentially less risk for loss of separation and associated wake turbulence upsets. Smaller aircraft flying VFR may be more likely to lose separation, but wake turbulence upsets are not as likely among VFR traffic due to aircraft size. The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is unlikely to maintain a collision course toward traffic which is shown on the display	4 (Minor) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. The pilot will detect the potential loss of separation and maneuver to correct the situation without the aid of the CD alerts. If the alert is issued too late in this scenario, the pilot may wonder if there is a new conflict and visually scan for it (unnecessarily). The hazard severity is minor (4) due to this slight increase in workload.	fPR 3.2.2.2.1.1 Latency a. The maximum latency from measurement of position and velocity information in the transmitting aircraft/vehicle and display of this position / velocity information in the receiving a/v shall be less than 3 seconds to support the CD application [C308] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C185, C186] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures – (AIM) [H51]	C The hazard is substantially controlled by existing requirements and see-and-avoid procedures.	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H52	CAZ Alert Issued Late	A Collision Avoidance Zone (CAZ) alert is issued too late for a pilot to take action to avoid potential impending collision	C185 Conflict Detection Processor/Alert soft failure [F1.3]. C308 End-to-end system latency is excessive. [F1.1 – F1.6] C186 CDZ and/or CAZ alert thresholds set incorrectly. [F1.3.12] C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.3.12]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert	Slight increase in workload.	The Enhanced Visual Acquisition application still shows the location of traffic relative to ownship – The pilot is less likely to maintain a collision course toward traffic which is shown on the display. See and avoid procedures are still in effect.	4 (Minor) Using the see and avoid procedures, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. The pilot may detect the loss of separation and maneuver to correct the situation without the aid of the CD alerts. If the alert is issued too late in this scenario, the pilot may wonder if there is a new conflict and visually scan for it (unnecessarily). The hazard severity is minor (4) due to an increase in workload.	fPR 3.2.2.2.1.1 Latency a. The maximum latency from measurement of position and velocity information in the transmitting aircraft/vehicle and display of this position / velocity information in the receiving a/v shall be less than 3 seconds to support the CD application. [C308] DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C185, C186] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures – (AIM) [H52]	C The hazard is substantially controlled by existing requirements and see-and-avoid procedures.	4C (Low)		4C (Low)
H53	False CDZ Alert Issued	A Conflict Detection Zone (CDZ) alert is issued when no conflict exists. An alert may be issued too early or when no predicted conflict exists.	C185 Conflict Detection Processor/Alert soft failure [F1.3.12] C176 ASSAP/CDTI design fault [F1.3, F1.6]. C186 CDZ and/or CAZ alert thresholds set incorrectly [F1.3.12]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists	A false CDZ alert could result in a slight workload increase.	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maneuver toward real traffic which is shown on the display	4 (Minor) A CDZ alert is strategic; i.e., there is adequate time for the pilot to assess traffic for potential conflicts. A false CDZ alert will prompt the pilot to visually scan for traffic, potentially resulting in a slight workload increase. The hazard severity is minor in this case (4).	DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C176, C185, C186] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures –	C The hazard is substantially controlled by existing requirements and see-and-avoid procedures.	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.3.12]	that would ordinarily result in a CDZ alert				(AIM) [H53]				
H54	False CAZ Alert Issued	A Collision Avoidance Zone (CAZ) alert is issued when no conflict exists. An alert may be issued too early or when no predicted conflict exists.	C185 Conflict Detection Processor/Alert soft failure [F1.3.12] C176 ASSAP/CDTI design fault [F1.3, F1.6]. C186 CDZ and/or CAZ alert thresholds set incorrectly [F1.3.12] C187 CDZ and/or CAZ alert thresholds do not change as a function of the phase of flight. [F1.3.12]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert	A false CAZ alert could result in a slight workload increase.	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maneuver toward real traffic which is shown on the display	4 (Minor) A CAZ alert will prompt the pilot to visually scan for traffic, potentially resulting in a slight workload increase. Using see and avoid procedures, the pilot should be able to confirm that no traffic conflict exists (i.e., the alert was false). The hazard severity is minor in this case (4).	DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C176, C185, C186] DO-289 Table D-2 specifies alert zones depending on phase of flight [C187] See and avoid procedures – (AIM) [H54]	C The hazard is substantially controlled by existing requirements and see-and-avoid procedures.	4C (Low)		4C (Low)
H55	Erroneous Alerted Traffic Symbol for CDZ Alert	The target highlighted as causing or contributing to the conflict condition is wrong. Conflict with a different target has led to the alert.	C64 CDTI malfunction causing erroneous traffic symbol associated with an alert	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would	Slight workload increase may be incurred in having to determine that the CD application was in error.	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maneuver toward real traffic which is shown on the display	4 (Minor) The CDZ alert applies to potential loss of separation. Given the nature of the CDZ alert, the pilot will have time to detect that the wrong traffic symbol was highlighted as having caused the alert condition. Some workload increase may be incurred in having to determine that the CD application was in error. Nevertheless, the	DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C64] See and avoid procedures – (AIM) [H55]	C The hazard is substantially controlled by design requirements and see-and-avoid procedures	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
				ordinarily result in a CDZ alert			application provides the pilot a cue to look for traffic conflicts. It is presumed that the pilot will notice the correct aircraft which contributed to the alert condition.					
H56	Erroneous Alerted Traffic Symbol for CAZ Alert	The CAZ alert includes both aural and visual components. In this scenario, the aural alert is issued correctly, but the wrong traffic symbol is highlighted as having caused or contributed to the conflict condition. Conflict with a different target has led to the alert.	C64 CDTI malfunction causing erroneous traffic symbol associated with an alert [F 1.6]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert	Pilot time to detect which aircraft is in conflict is increased due to wrong highlighted traffic symbol Significant reduction in safety margin.	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maneuver toward real traffic which is shown on the display	2 (Hazardous) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. In this hazard scenario, the pilot either fails to observe the pending traffic conflict or the conflict was of a "sudden" nature. Based on the CAZ aural alert, the pilot may look at the display to determine which traffic is in conflict. The pilot should visually scan out the window for the traffic conflict based on the location of the highlighted traffic symbol. If the wrong symbol is highlighted, the pilot may look in the wrong area for the conflict. The pilot may not detect which aircraft is in conflict as quickly. A significant reduction in safety margin may result; the hazard severity is hazardous (2) in this	DO-289 Table 3-20 Subsystem integrity and availability risk requirements [C64] See and avoid procedures – (AIM) [H56]	C Design assurance pre DO-289 (minor) and procedures limit the likelihood to remote.	2C (High)	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI [H55] Software for the Aircraft/Vehicle function shall satisfy the objectives for Software Level C defined in RTCA DO-178B or an equivalent software design assurance standard.	2D (Medium)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
							case.					
H57	CDZ Visual Alert Not Noticeable	CDZ visual alerts not discernable or not noticeable	C65 The CDTI display is too cluttered.	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CDZ alert	A slight increase in workload.	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maintain a collision course toward traffic which is shown on the display	4 (Minor) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. If the CDZ alert is not visible or noticeable, it is equivalent to not having the CD application to aid in detecting potential loss of separation.	DO-289 §3.3.3.1.3.1 suggests filtering criteria for the CDTI. [C65]	A Clutter filtering is suggested in existing documentation but is not required.	4A (Medium)	Make filtering criteria standard in the CDTI MOPS [C65]	4C (Low) Addition of required control will reduce this hazard likelihood to an acceptable level.
H58	CAZ Visual or Aural Alert Not Noticeable	CAZ visual alerts not discernable or not noticeable, or aural alert can not be heard.	C65 The CDTI display is too cluttered. C67 The volume setting does not match the flight deck ambient noise setting (volume too low) C69 CD alerts not consistent or not integrated or not given proper priority with	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would	A slight increase in workload	The Enhanced Visual Acquisition application shows the location of traffic relative to ownship – The pilot is less likely to maintain a collision course toward traffic which is shown on the display	4 (Minor) Using the see and avoid principle, visual out-the-window scans for traffic should still be performed regardless of whether the CD application is present. If the CDZ alert is not visible or noticeable, it is equivalent to not having the CD application to aid in detecting potential loss of separation.	DO-289 §3.3.3.1.3.1 suggests filtering criteria for the CDTI. [C65]	A Clutter filtering is suggested in existing documentation but is not required. No requirements for audio controls for alerting in existing documentation.	4A (Medium)	Make filtering criteria standard in the CDTI MOPS [C65] The CDTI shall provide volume control to adjust for ambient noise in the cockpit. [C67, C69] The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for	4C (Low) Addition of required controls will reduce this hazard likelihood to an acceptable level.

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			existing flight deck alerting system. [F1.6]	ordinarily result in a CDZ alert							ADS-B avionics and ancillary equipment. [C69]	
H60	CAZ Alert Audio Interferes with Air Crew Ability to Hear Radio Communications	The CAZ alert audio component interferes with the pilot's ability to hear and understand radio communications	C68 The volume setting does not match the flight deck ambient noise setting (volume too high) C69 CD alerts not consistent or not integrated or not given proper priority with existing flight deck alerting system. [F1.6]	Either controlled airspace or airspace where ATC is giving advisories OR uncontrolled airspace where pilots are using radio communications to advise other traffic of their maneuvers Night time Marginal VMC Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CAZ alert	ATC workload may increase due to repeating radio communications missed by the pilot. Similarly, the pilot's workload may increase if they realize they missed a radio communication and have to ask ATC to repeat.	The TCAS MOPS recommends that the volume level of the automatic adjustment provide a range of 0 to 4 watts RMS at 1000 Hz into 8 ohms for a speaker output and the automatic adjustment provide a range of 0 to 40 milliwatts at 1000 Hz into a 600 ohm audio distribution system.	3 (Major) If the alert audio obscures the pilot's ability to hear and understand radio communications, a significant reduction in safety margin may occur based on the nature of the communication. In controlled airspace, ATC may issue breakout instructions to a pilot to avoid an aircraft which has unexpectedly deviated from its planned course. If the pilot does not hear the instructions, it may take some time until ATC or the pilot realizes instructions were not received. In this case, the window for the pilot to safely maneuvering the aircraft to avoid a conflict is reduced. In uncontrolled airspace, GA pilots may use radio communications to announce their intentions (e.g., approach to / landing at	AIM, 7110.65: Pilot read-back of ATC instructions (ATC will detect pilot has not heard instructions if there is no read-back) [H60]	C Pilot read-back will detect this problem with high probability; other controls necessary to limit likelihood of the event in the first place.	3C (Medium)	The CDTI shall provide volume control to adjust for ambient noise in the cockpit. [C68. C69] The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B avionics and ancillary equipment. [C69]	3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
							an airport) to other traffic. If a pilot does not hear the radio communications from another pilot, they may not realize that the other pilot expects to begin descending to land at an airport which they may also be approaching. Also, ATC workload may increase due to repeating radio communications missed by the pilot. Similarly, the pilot's workload may increase if they realize they missed a radio communication and have to ask ATC to repeat.					
H61	Multiple, Successive CDZ and/or CAZ Alerts Issued	Multiple conflicts result in multiple simultaneous or successive alerts. The pilot may become confused as to which alert to react upon.	C310 More than one alert is allowed to be issued at a time [F1.3.12]	Night time Marginal VMC Uncontrolled airspace Aircraft are not TCAS equipped Traffic is busy due to a seasonal event at a GA airport A conflict between two aircraft exists that would ordinarily result in a CAZ alert	The pilot's time to react to a conflict may be reduced if they are occupied with mentally processing multiple alerts or manipulating the CDTI to suspend the alerts. Significant reduction in safety margin.		2 (Hazardous) Multiple, successive alerts may confuse the pilot and lead to a workload problem. Depending on the actual conflict situation, this could be minor to hazardous in severity. In the latter case, the pilot's time to react to a conflict may be reduced if they are occupied with mentally processing multiple alerts or manipulating the CDTI to suspend the alerts.	There is only one alert present for the total system at any time and that is the highest alert. (ASA MASPS section D.2.2.2, pg D-24 for requirement preventing issuance of simultaneous alerts) [C310]	D Design requirements specifically prevent this. See and avoid procedures still in place. Likelihood of multiple simultaneous conflicts is low to begin with.	2D (Medium)	The Conflict Detection application shall present only one alert level at a time. (Note: Verify that corresponding ASA MASPS statement in section D.2.2.2 pg D-24 for preventing issuance of simultaneous alerts is carried through in MOPS) [C310]	2E (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H62	TCAS Resolution Advisory (RA) Followed by CDZ or CAZ Alert	A TCAS Resolution Advisory (RA) is issued and followed by CDZ or CAZ alert.	C69 CD alerts not consistent or not integrated or not given proper priority with existing flight deck alerting system. [F1.3.12]	Aircraft are equipped with TCAS II and the CD application Mixture of IFR and VFR traffic in terminal airspace VFR aircraft may get within a mile of an IFR aircraft.	This may lead to pilot confusion and increased workload.		4 (Minor) TCAS RAs include instructions to climb or descend to resolve a conflict. Once an RA is issued, the pilot will comply with the RA instructions. A successive CAZ alert may be a function of the new maneuver or the initial conflict which also caused the TCAS RA. This may lead to pilot confusion and increased workload. If the CAZ alert was due to same cause as that of the TCAS RA, then pilot workload may increase slightly to verify that the causes are the same. Also, the pilot may be looking back and forth between separate TCAS and CDTI displays, distracting them from visually scanning for traffic out the window.	DO-289 3.3.1.6.4 TCAS/ACAS alerts shall have priority over all ASA alerts [C69].	C The fact that the TCAS alert is over indicates that the situation is resolved. If CAZ is designed properly, it is considered remote that the CAZ alert will run contrary to the TCAS alert. A CDZ alert after the RA would not be unexpected.	4C (Low)		4C (Low)
H63	CDZ or CAZ Alert Followed by a TCAS Resolution Advisory (RA)	A CDZ or CAZ alert is issued and followed by a TCAS Resolution Advisory (RA).	C69 CD alerts not consistent or not integrated or not given proper priority with existing flight deck alerting system. [F1.3.12]	Aircraft are equipped with TCAS II and the CD application Mixture of IFR and VFR traffic in terminal airspace VFR aircraft may get within a mile of an IFR aircraft.	Pilot inappropriately maneuvers based on CD alert; maneuver conflicts with subsequent TCAS RA instructions Reaction time to resolve traffic conflict is reduced significantly See and avoid compromised due to head down time (e.g., pilot may be looking back and forth between separate TCAS and CDTI displays)		2 (Hazardous) If a CDZ alert is issued followed by a TCAS RA, the pilot will respond to the RA which takes precedence over the CD application alerts. If a CAZ alert is generated, the pilot may begin to maneuver (climb for example) based on the alert. If a TCAS RA is issued subsequently, and the RA instruction is to descend, reaction time to resolve the conflict is reduced significantly. I.e., the pilot / aircraft are descending when the TCAS RA	DO-289 §3.3.1.6.4 "TCAS alerts shall have priority over ASA alerts." [C69] DO-289 specifies that flight crews are not to maneuver solely on the basis of a CD alert. [H63]	D Implementation of specified procedures and requirements in DO-289 make this extremely remote, and the likelihood is that in most cases the CDZ and CAZ alert will make the RA more, not less effective, because it gives the flight crews an earlier warning.	2D (Medium)	The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B avionics and ancillary equipment. [C69] The Aircraft Flight Manual shall indicate that the pilot shall not maneuver on the sole basis of CD application alerts. [H63]	2E (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
					Significant reduction in safety margin.		instructions are to climb. Also, the pilot may be looking back and forth between separate TCAS and CDTI displays, distracting them from visually scanning for traffic out the window.					
H64	TCAS Traffic Advisory (TA) Followed by a CDZ or CAZ Alert	A TCAS Traffic Advisory (TA) is issued and followed by a CDZ or CAZ alert.	C69 CD alerts not consistent or not integrated or not given proper priority with existing flight deck alerting system. [F1.3.12]	Aircraft are equipped with TCAS II and the CD application Mixture of IFR and VFR traffic in terminal airspace VFR aircraft may get within a mile of an IFR aircraft.	The pilot's workload may increase in order to verify that the TA applied to the same traffic conflict	TCAS TA will precede RA. The pilot has time to examine and resolve the traffic situation given the nature of the conflict leading to a TCAS TA. Once a TA issued, the pilot may examine the TCAS display to see what is causing the TA. If a CDZ or CAZ is then issued, the pilot's workload may increase in order to verify that the TA applied to the same traffic conflict. Also, the pilot may be looking back and forth between separate TCAS and CDTI displays, distracting them from visually scanning for traffic out the window.	4 (Minor) The pilot has time to examine and resolve the traffic situation given the nature of the conflict leading to a TCAS TA. Once a TA issued, the pilot may examine the TCAS display to see what is causing the TA. If a CDZ or CAZ is then issued, the pilot's workload may increase in order to verify that the TA applied to the same traffic conflict. Also, the pilot may be looking back and forth between separate TCAS and CDTI displays, distracting them from visually scanning for traffic out the window.	DO-289 §3.3.1.6.4 "TCAS alerts shall have priority over ASA alerts." [C69] DO-289 specifies that flight crews are not to maneuver solely on the basis of a CD alert. [H63]	C Implementation of specified procedures and requirements in DO-289 make this remote	4C (Low)		4C (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H65	CDZ or CAZ Alert Followed by a TCAS Traffic Advisory (TA)	A CDZ or CAZ alert is issued and followed by a TCAS Traffic Advisory (TA).	C69 CD alerts not consistent or not integrated or not given proper priority with existing flight deck alerting system. [F1.3.12]	Aircraft are equipped with TCAS II and the CD application Mixture of IFR and VFR traffic in terminal airspace VFR aircraft may get within a mile of an IFR aircraft.	Pilot workload may increase slightly due to mentally processing and resolving two separate alerts.		3 (Major) If a CDZ alert is followed by TA, the pilot has time to examine and resolve the traffic situation given the nature of the conflicts leading to TA and CDZ alerts. Pilot workload may increase slightly due to mentally processing and resolving two separate alerts. If a CAZ alert is issued and the pilot maneuvers based on the alert, a TCAS TA may lead to pilot confusion. Either the TA was issued for the initial conflict or for a new conflict created when the pilot maneuvered to resolve the traffic situation which generated the CAZ alert. Also, the pilot may be looking back and forth between separate TCAS and CDTI displays, distracting them from visually scanning for traffic out the window.	DO-289 §3.3.1.6.4 "TCAS alerts shall have priority over ASA alerts." [C69] DO-289 specifies that flight crews are not to maneuver solely on the basis of a CD alert. [H63]	D Implementation of specified procedures and requirements in DO-289 make this extremely remote, In most cases, the alerts will be consistent. The CDZ alert will give the pilot additional warning time that a conflict is pending. The existing control of shutting down the ASA alert when there is a TCAS alert will minimize pilot confusion as there will be only one alert active at a time.	3D (Low)		3D (Low)

5.2.7 Weather and NAS Status Situational Awareness

Ground Rules and Assumptions

- Because specific sources for FIS-B products were not identified during the PHA, a recommended risk mitigation to "Identify built in safety controls from external systems" is included in hazard H66. This mitigation will occur during the SSHA after contract award and toward the system design review timeframe when specific external weather and aeronautical information systems are identified.
- Flight rules for pilots to obtain applicable weather reports and forecasts prior to takeoff are referenced frequently as an existing control. These rules are abbreviated in the hazard tables for brevity; the complete rule is contained in the following excerpt from the Federal Aviation Regulations (FAR):

> Title 14: Aeronautics and Space
> PART 91—GENERAL OPERATING AND FLIGHT RULES
> Subpart B—Flight Rules
> Source: Docket No. 18334, 54 FR 34294, Aug. 18, 1989, unless otherwise noted.
> § 91.103 Preflight action.
> Each pilot in command shall, before beginning a flight, become familiar with all available information concerning that flight. This information must include—
> (a) For a flight under IFR or a flight not in the vicinity of an airport, **weather reports and forecasts**, fuel requirements, alternatives available if the planned flight cannot be completed, and any known traffic delays of which the pilot in command has been advised by ATC;
> (b) For any flight, **runway lengths at airports of intended use**, and the following takeoff and landing distance information:
> (1) For civil aircraft for which an approved Airplane or Rotorcraft Flight Manual containing takeoff and landing distance data is required, the takeoff and landing distance data contained therein; and
> (2) For civil aircraft other than those specified in paragraph (b)(1) of this section, other reliable information appropriate to the aircraft, relating to aircraft performance under expected values of airport elevation and runway slope, aircraft gross weight, and wind and temperature.

Table 5-8: Weather and NAS Status Situational Awareness Preliminary Hazards

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H66	Loss of or Erroneous AIRMET	An AIRMET, or Airmen's Meteorological Information, is a weather advisory for aircraft that is potentially hazardous to aircraft with limited capability because of lack of equipment, instrumentation, or pilot qualification. AIRMETs cover: moderate turbulence and icing, surface winds of 30 knots, or widespread restricted visibility. AIRMETs are issued only to amend the area forecast concerning weather phenomena. AIRMETs concern weather of less severity than that covered by SIGMETs or convective SIGMETs. AIRMETS must affect at least a 3,000 square mile area and are valid for six hours. In this hazard, the application does not provide or provides erroneous AIRMET messages.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot encounters wide area of limited visibility (e.g., smoke present)	Significant increase in workload.		3 (Major) A pilot may fly into an areas with turbulence or widespread limited visibility (as with smoke), if AIRMET information is wrong or missing. When there is limited visibility, it may be difficult to remain on VFR, and a pilot who is not instrument-rated may not fly IFR. Given the pilot's lack of ability to switch from VFR to IFR and / or the possibility of encountering moderate turbulence, the hazard severity is major (3).	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources. (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]	D Extremely remote probability due to pilot ability to cross-check information	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H67	Loss of or Erroneous METAR and SPECI	METAR, or METeorological Aerodrome Report, is predominantly used by pilots in fulfillment of a part of a pre-flight weather briefing. METAR reports usually come from airports. Typically, reports are generated once an hour; however, if conditions change significantly, they may be updated in special reports called SPECIs. A typical METAR report contains data for the temperature, dew point, wind, precipitation, cloud cover, cloud heights, visibility, and barometric pressure. A METAR report may also contain information on precipitation amounts, lightning, and other information that would be of interest to pilots. In this hazard, the application does not provide or provides erroneous METAR or SPECI reports.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot unexpectedly encounters low visibility conditions	Significant increase in workload.		3 (Major) A pilot could unexpectedly encounter low visibility conditions in either case where METAR information is missing or erroneous.	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency a. The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]	D Extremely remote probability per due to pilot ability to cross-check information hourly. Also information source should be highly reliable; difficult to corrupt information in a way that is non-obvious.	3D (Low)		3D (Low)
H68	Loss of AWW and WW	Severe Weather Forecast Alert (AWW). AWW is a preliminary message used to alert airmen that a Severe Weather Bulletin (WW) is being issued. AWW defines an area of possible severe thunderstorms or tornado activity. This hazard is about the loss of AWW or WW.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot encounters a severe thunderstorm	Significant increase in workload.	This scenario exists today without the aid of information provided by this application.	3 (Major) In this scenario, severe weather suddenly occurs, but a pilot received no AWW or WW messages. At night, a pilot may not readily detect that severe weather is ahead. However, pilots may obtain severe weather forecasts pre-flight and check for updates via HI WAS in-flight. In addition, the pilot should eventually detect that severe weather is ahead while in-flight based on visual and	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] If tuned into ATIS or flight service station could get same information [C73, C71, C70] For IFR flights, ATC is required to provide AWW related information to aircraft on frequency [C73, C71, C70]	D Extremely remote probability per due to pilot ability to cross-check information, source information should be highly reliable and corruption in a non-	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]				physical cues, including high clouds and winds. Given alternative severe weather information sources and physical and visual cues that provide an opportunity to avoid hazardous weather, hazard severity is, at most, major (3).	Visual and physical cues to the pilot that severe weather is in the vicinity (e.g., high clouds associated with tornadic activity, high winds) [C73, C71, C70] Pilots may obtain weather updates via the HI WAS frequency off of VORs [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]	obvious manner difficult.			
H69	Loss of or Erroneous Ceiling	The ceiling is the height of the lowest layer of broken or overcast clouds. Although clouds are present, the application does not provide ceiling, or the application provides erroneous ceiling information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment	Small GA aircraft equipped with UAT Pilot on VFR flight plan	Significant increase in workload.	Pilots interviewed for this hazard scenario indicated that ceiling height	3 (Major) Pilots may obtain weather terminal forecasts along their intended course pre-flight.	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] Pilots may obtain terminal forecasts along intended	D Extremely remote probability per due to pilot	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3] .	Pilot not instrument-rated A cloud deck is present ahead of and below the aircraft		information provided by AWOS is known to be unreliable. This is due to the localized nature of cloud height measurement which does not account for variations across a wide area.	In-flight, cloud decks that develop underneath an aircraft can be problematic if a pilot is not instrument-rated. A pilot may not be able to safely navigate below a cloud deck to land without instrument training. However, pilots should visually detect clouds ahead and maneuver around them even without the aid of this application. Even if a pilot unexpectedly flies into a cloud layer, there is an opportunity to turn around and select an alternate route.	course of flight to get an indication of clouds layers pre-flight [C73, C71, C70] Pilots will visually detect clouds ahead and have an opportunity to avoid flying into a cloud layer [C73, C71, C70] Upon encountering a cloud layer, pilots may turn around and choose an alternate course [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]	ability to cross-check information directly with visual info; information is difficult to corrupt in a non-obvious manner;			

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H70	Loss of or Erroneous Convective SIGMET	SIGMET, or Significant Meteorological Information, is a weather advisory that contains information concerning the safety of all aircraft. Typical SIGMETs contain information on severe turbulence and icing, or visibility restrictions such as dust, ash, or sandstorms. Convective SIGMETs (WST) are issued by time and region, and are associated with thunderstorms. WSTs are issued hourly as required. They are valid for two hours or until superseded. Bulletins consist of an observation and/or a forecast. In this hazard, the application does not provide a SIGMET when one should be issued, or the application provides erroneous information concerning time, region, observation, and / or forecast.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Icing conditions present	Significant increase in workload.		3(Major) If SIGMET information is erroneous, the pilot may believe that there are no severe weather or visibility restrictions in the vicinity. The pilot could unexpectedly encounter severe weather conditions, resulting in a significant reduction in safety margin.	Pilots obtain weather reports from external sources before takeoff[C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]	D Extremely remote probability per due to pilot ability to cross-check information, information being provided periodically, difficulty of corrupting information in a non-obvious manner.	3D (Low)		3D (Low)
H71	Loss of or Erroneous Echo tops	Echo tops are derived from NEXRAD data that indicates the highest altitude at which precipitation is falling. The higher the echo tops, the more powerful the storm. In this hazard, the application does not provide echo top information, or the application provides erroneous echo top altitude information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot encounters severe weather conditions		Significant increase in workload.	Major (3) Though echo tops are typically associated with higher altitudes where IFR applies, warm rain can result in echo tops at 9,000 – 10,000 ft. If a pilot believes he can fly VFR on top based on erroneous echo top information, he may not be able to safely navigate below the cloud deck to land. However, pilots should visually detect clouds ahead even without the aid of this application and maneuver around them. Even if a pilot	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] Pilots may obtain terminal forecasts along intended course of flight to get an indication of clouds layers pre-flight [C73, C71, C70] Pilots will visually detect clouds ahead and have an opportunity to avoid flying into a cloud layer [C73, C71, C70]	D Extremely remote probability per due to pilot ability to cross-check information visually, opportunities to divert to another path, difficulty of corrupting info in a non-	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]				unexpectedly flies into a cloud layer, there is an opportunity to turn around and select an alternate route.	Upon encountering a cloud layer, pilots may turn around and choose an alternate course [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]	obvious manner.			
H72	Loss of or Erroneous Lightning Strike Information	Lightning strikes are indicators of convective weather. The application does not provide information concerning lightning strikes (cloud-to-ground as opposed to cloud-to-aircraft), or the application provides erroneous lightning strike information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot unexpectedly encounters	Significant increase in workload.	Is there data on the frequency of lightning striking aircraft?	3 (Major) Lightning strike information supplements other weather products such as Severe Weather Forecast Alerts (AWWs), Significant Meteorological Information (SIGMET), and echo tops. If other weather products are not available and lightning strike information is not provided or	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics	D Extremely remote probability per due to pilot ability to cross-check information, ability to detect areas of lightning	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	lightning activity Other weather products indicative of storm activity are not available or not provided			is incorrect, there is a possibility that the pilot may fly into weather with lightning activity. Even if lightning strikes an aircraft, aircraft hull damage or loss of flight control are not expected given that the aircraft acts as an electrical conductor to ground. It is possible that electrical instruments may be affected by the lightning strike, however; hazard severity is considered major (3) in this case.	a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]	visually, unlikely to corrupt information in a way that is not obvious.			
H73	Loss of or Erroneous NEXRAD Reflectivity	The application does not provide or provides erroneous NEXRAD precipitation information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Pilot unexpectedly encounters moderate precipitation	Significant increase in workload.	GA pilots may land and wait for bad weather to pass. NEXRAD products are not intended for navigating around bad weather.	3 (Major) Pilots obtain weather forecasts pre-flight. In-flight, pilots may check with Flight Service Stations for updated weather information if the application fails to provide NEXRAD precipitation information. Alternatively, precipitation information is available in-flight via other weather products, including METeorological Aerodrome Reports (METARs), Severe Weather Forecast Alerts (AWWs), and echo tops, provided by this application. If the application provides erroneous information, the pilot should eventually detect that severe weather or precipitation is ahead based on visual and physical cues. Cues include presence of clouds, winds, and light rain. Given alternative	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] Other weather products such as Severe Weather Forecast Alerts (AWWs), Significant Meteorological Information (SIGMET), and echo tops are available in-flight [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73]	D Extremely remote probability per due to pilot ability to cross-check information and difficulty of corruption information in a way that is non-obvious.	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
							weather information sources and physical and visual cues that provide an opportunity to avoid hazardous weather, hazard severity is, at most, major (3).	b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]				
H74	Loss of or Erroneous PIREPs	A Pilot Report (PIREP) is a report of weather conditions encountered by an aircraft during a flight. The application does not provide or provides erroneous PIREP information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated Other weather products or information sources are available	Slight increase in workload.	The pilots interviewed for this hazard consider PIREPs to be supplemental / non-critical information.	4 (Minor) PIREPs apply to a localized area, and missing PIREP information may not be relevant to the pilot's intended course of flight. The pilot may contact ATC or flight service stations to obtain weather information. If other weather products were received, but a PIREP erroneously contradicted that information, the pilot would still be prompted to look for severe weather conditions.	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]	D Extremely remote probability per due to pilot ability to cross-check information, the possibility of other sources, and the fact that the information is not of high criticality to begin with.	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H75	Loss of or Erroneous TAF	TAF, or Terminal Aerodrome Forecast, is generally a 24 hour forecast; it complements and uses similar encoding to METAR reports and may be amended as needed.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot obtains TAF from external source prior to takeoff Pilot on VFR flight plan Pilot not instrument-rated Pilot unexpectedly encounters severe weather conditions	Significant increase in workload.	Assume TAF retrieved before takeoff is correct	3 (Major) TAF information is used for strategic planning purposes. As flight departure time approaches, pilots will have current weather forecasts from sources external to this application. If the TAF provided in this application indicates good weather conditions and the TAF obtained pre-flight agrees, the pilot may be less likely to check for weather updates in flight. Other weather products are available with current or more tactical weather information. Safety may be significantly reduced if the pilot fails to check for weather updates and unexpectedly encounters severe weather.	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]	D Extremely remote probability per due to pilot ability to cross-check information	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
H76	Loss of or Erroneous TWIP	TWIP, or Terminal Weather Information for Pilots, is local terminal Doppler weather radar severe weather information (around an airport)—including wind shear, storm cells, microbursts, gust fronts, and moderate-to-heavy precipitation. It is assumed TWIP reports are only available at controlled airports. The application does not provide or provides erroneous TWIP reports.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Controlled airport Large, GA aircraft on final approach Pilot on IFR flight plan Pilot unexpectedly encounters convective weather Other weather products indicative of storm activity are not available or not provided	Significant increase in workload.		3 (Major) If TWIP reports are not provided or indicate the wrong location for severe weather, a pilot may unexpectedly fly into severe weather. For example, the pilot may encounter a microburst at an airport. If a microburst is encountered, a possibility of stalling the aircraft exists considering that some larger aircraft cannot speed up quickly enough to avoid a stall.	ATC notifies pilots of severe weather [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]	D Extremely remote probability per due to pilot ability to cross-check information and difficulty of corrupting information in a way that is non-obvious.	3D (Low)	.	3D (Low)
H77	Loss of or Erroneous Winds Aloft	Winds Aloft is information about wind speed and direction at various levels in the atmosphere above the level reached by surface weather observations. The application does not provide or provides erroneous winds aloft information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C70 Data from external weather source is erroneous [External]	An aircraft has just enough fuel to reach a particular destination The pilot unexpectedly encounters a strong head wind which reduces ground speed	Slight increase in workload.		4 (Minor) An aircraft may have just enough fuel to reach a particular destination. With a strong head wind, ground speed is reduced, and the aircraft may have insufficient fuel to reach the intended airport. Even if the application does not provide winds aloft information, other aircraft instrumentation (e.g., speed indicator) enables the pilot to detect that head winds may be present. The pilot has the ability to change to a different altitude with better	Pilots obtain weather reports from external sources before takeoff [C73, C71, C70] Pilot may change to a different altitude with better wind conditions [C73, C71, C70] Pilot may land elsewhere in the event that fuel is insufficient to reach intended airport [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS	D Extremely remote probability per due to pilot ability to cross-check information; ability to change altitude, unlikely to corrupt information in a non-obvious way.	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]				wind conditions.	processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. .[C71, C72]				
H78	Loss of or Erroneous D-ATIS	D-ATIS, or Digital Automated Terminal Information Service, provides information on runway and taxiway instructions, avionics equipment, frequency outages, and local weather conditions. This hazard entails loss of or provision of erroneous D-ATIS information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C75 Data from external aeronautical information source is erroneous [External] C201 LSP/BCS processing of FIS-B	Class C or better airport	Slight increase in workload.	D-ATIS is expected at Class C or better airports	4 (Minor) If D-ATIS lost, a pilot may tune into "regular" ATIS radio broadcasts. Hazard severity is minor (4) given a slight increase in pilot workload.	Pilots obtain airport status and special instructions from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C75]	D Extremely remote probability per due to pilot ability to cross-check information, obtain information from other sources, and due to the minimal likelihood that the information is corrupted in a way that is not detectable.	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
			products is not timely.[F2,F3]					b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72] ATIS radio broadcasts				
H79	Loss of or Erroneous NOTAMs	A Local, Distant and Flight Data Center Notices to Airmen, or NOTAM, is filed with an aviation authority to alert aircraft pilots of any hazards en route or at a specific location. The authority through its Flight Service Stations in turn reports all relevant NOTAMs to pilots when a pilot files an intended flight plan. NOTAMs are issued (and reported) for a number of reasons, such as: hazards such as air-shows and parachute jumps, flights by important people such as heads of state, closed runways, inoperable radio navigational aids. military exercises with resulting airspace restrictions, inoperable lights on tall obstructions,temporary erection of obstacles near airfields (e.g. cranes). The application does not provide or provides erroneous NOTAM information.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C75 Data from external aeronautical information source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot not instrument-rated	Slight increase in workload.		4 (Minor) Pilots obtain NOTAMs before takeoff, and may check with ATC or Flight Service Stations for updates. If a NOTAM change was generated while the pilot was in-flight, and the NOTAM information was of significance to the pilot (e.g., Navaid outage at destination airport), the pilot may incur increased workload.	Pilots obtain airport status and special instructions from external sources before takeoff [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C73] b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C75] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a	D Extremely remote probability per due to pilot ability to cross-check information	4D (Low)		4D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]				
H80	Loss of or Erroneous SUA Indication	The application may fail to provide or provide erroneous information concerning active Special Use Airspace (SUA) associated with military operations. The active / non-active status may change while an aircraft in in-flight.	C71 LSP/BCS Equipment random failure [F2,F3] C72 LSP/BCS Equipment design flaw [F2,F3] C73 BCS incorrectly processes FIS data products [F3.2.3] C75 Data from external aeronautical information source is erroneous [External] C201 LSP/BCS processing of FIS-B products is not timely.[F2,F3]	Small GA aircraft equipped with UAT Pilot on VFR flight plan Pilot unexpectedly encounters an active artillery range	Significant increase in workload.		3 (Major) Pilots consult VFR charts to determine locations and altitudes of SUA and default times when they are active prior to takeoff. Also, the military notifies the FAA 24 hours in advance when there is a change to SUA default active times. Even if the application fails to provide SUA information or provides erroneous SUA information (e.g., active time is wrong), see and avoid procedures still apply. VFR GA pilots and military aircraft pilots should visually detect and avoid each other.	VFR charts provide locations and altitudes of SUA and default times when they are active [C73, C71, C70] The military notifies the FAA 24 hours in advance when there is a change to SUA default active times [C73, C71, C70] See and avoid procedures [C73, C71, C70] fPR 3.2.3.5.1 Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds. [C201] fPR 3.2.3.5.9 Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities. [C75]	D Extremely remote probability per due to pilot ability to cross-check information	3D (Low)		3D (Low)

No.	Hazard Title	Hazard Description	Causes	Worst Case System States	Possible Effects	Comments	Severity / Rationale	Existing Controls & Requirements	Likelihood / Rationale	Current / Initial Risk	Recommended Safety Reqs	Predicted Residual Risk
								b. All FIS products shall be based on government approved data sources (approved by FAA Order 8400.1) [C70] fPR 3.2.1.4 FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999. [C71, C72]				

SURVEILLANCE AND BROADCAST SERVICES PROGRAM
SEGMENT 1

SAFETY RISK MANAGEMENT DOCUMENT:
PRELIMINARY HAZARD ANALYSIS

VOLUME III - RESULTS & APPENDICES

SEPTEMBER 18, 2006

VERSION 1.0

DOCUMENT CHANGE HISTORY

VERSION	DATE	DESCRIPTION OF CHANGES

TABLE OF CONTENTS

6. LIST OF SAFETY REQUIREMENTS 4

6.1 EXISTING CONTROLS AND RECOMMENDED REQUIREMENTS 4
6.2 SAFETY REQUIREMENTS VERIFICATION 4

7. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS 12

8. REFERENCES / BIBLIOGRAPHY 16

APPENDIX A: ACRONYMS 17

LIST OF TABLES

TABLE 6-7: SAFETY REQUIREMENTS VERIFICATION TABLE (SRVT) 4

LIST OF FIGURES

FIGURE 7-1: CURRENT RISK SUMMARY 14
FIGURE 7-2: PREDICTED RESIDUAL RISK SUMMARY 15

6. LIST OF SAFETY REQUIREMENTS

6.1 Existing Controls and Recommended Requirements

Reserved.

6.2 Safety Requirements Verification

A Safety Requirements Verification Table (SRVT) is provided in Table 6-1. The SRVT indicates the validation status of existing controls and requirements and recommend safety requirements in addition to the recommended verification method. The controls and requirements listed in the SRVT are primarily extracted from the following sources:

(1) Surveillance and Broadcast Services Final Program Requirements Document
(2) DO-289 ASA MASPS
(3) TIS-B MASPS
(4) Air Traffic Control 7110.65R

Requirements validation and verification status will continue to be updated in the HTRR System.

Table 6-1: Safety Requirements Verification Table (SRVT)

Validation and Verification (V&V) Status: 0 = not validated or verified; 1 = validated only; 2 = validated & verified
Planned Verification Method: A = Analysis; T = Test; I = Inspection; D = Demonstration (see SBS Integrated Safety Plan for a description of each verification method)

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
fPR 3.1.6	ADS-B Backup a. ATC Surveillance application shall continue to operate in the event of GNSS failure.	1		X			
fPR 3.2.1.1	ADS-B Service Availability The ADS-B service is a safety-critical service as classified by NAS-SR-1000 for surveillance services. This requirement is driven by the ATC Surveillance application. a. The ADS-B service shall meet a minimum Availability of 0.99999.	1	X	X			
NAS-SR-1000 3.8.1	NAS equipment, systems, installations, and facilities shall be kept in an operable and committable state according to their criticality to safe operation of aircraft. A. 1. Critical – Functions or services which, if lost, would prevent the NAS from exercising safe separation and control over aircraft. 2. Essential – Functions or services which, if lost, would reduce the capability of the NAS to exercise safe separation and control over aircraft.	1	X		X	X	
fPR 4.9	Power Systems and Commercial Power 4.9.1 Electrical Power Electrical power shall be provided in accordance with NFPA 70, National Electric Code ®; FAA Order, Electrical Power Policy; FAA Order 6950.2, Electrical Power Policy Implementation, NAS Facilities; and FAA Order 6950.25, Power Conditioning Devices at FAA Facilities.	1	X		X		
Ctrl-1	Automation system displays coasted track when surveillance data is missing for an adaptable amount of time.	2					
fPR 3.1.5	Maintenance Function 3.1.5.2 Processing h. The Maintenance Function shall provide a centralized monitor and control capability to evaluate performance during operation, control the equipment, monitor system health, and identify faulted modules.	1				X	
fPR 3.1.5	i. The Maintenance Function shall generate Alerts and Alarms when monitored parameters exceed allowable tolerances.	1		X		X	
3.1.5.3	Outputs a. The Maintenance Function shall display system performance and	1				X	

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
	certification data to the operator to assess the status of the system.						
3.1.5.3	b. The Maintenance Function shall display Alerts and Alarms to the system operator.	1		X		X	
3.1.5.3	c. The Maintenance Function shall display the operating status of system functions and components.	1				X	
	FAA Order 7110.65 ATC non-radar separation procedures	2					
	ATC / pilot communications	2					
	TCAS	2					
	Pilot see and avoid rules	2					
fPR 3.2.3.2.5	Coverage a. ADS-B surveillance coverage shall include, but not be limited to the following: • in en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3.G (3) and (4)	1	X				
fPR 3.2.3.2.3	Update Rate Each aircraft/vehicle will transmit ADS-B Messages with a position and velocity at least once every second. Aircraft/vehicle identification data may be transmitted less often. The ADS-B update rate as seen by the LSP/BCS is a function of operating environment and transmission range.	1		X			
fPR 3.2.3.2.3	a. The LSP/BCS shall provide position and velocity data from each aircraft/vehicle in terminal airspace coverage with an update rate sufficient to support 3nm separation standards.	1		X			
fPR 3.2.4.1. 5	Coverage a. The ATC Automation Function *shall* process and display ADS-B target data within the coverage volumes of the LSP Function and the BCS Function.	1		X			
fPR 3.1.5.3	Outputs g. The Maintenance Function shall provide analysis results indicating areas where coverage is predicted to exist, where actual coverage is acceptable, where actual coverage is not acceptable, and areas where coverage is unknown due to lack of targets of opportunity.	1				X	
fPR 3.2.3.2.6	Capacity a. The LSP/BCS shall process all ADS-B Messages received from aircraft/vehicles within ADS-B surveillance coverage (Reference section 3.2.3.2.5).	1		X			
fPR 3.2.4.1	ADS-B Surveillance Service (Terminal and En Route Airspace) 3.2.4.1.6 Automation System Capacity a. The ATC Automation Function shall have sufficient capacity to process the ADS-B peak and steady state target capacity loading	1		X			
fPR 3.2.2.2.2	Aircraft/Vehicle ADS-B Transmission The Aircraft/Vehicle transmits ADS-B Messages in support of all applications. The requirements in this section apply to all applications, unless a specific application is listed in the requirement text.	1		X			
3.2.2.2.2.6	Availability a. Aircraft/Vehicle function shall provide a minimum availability of 0.9995 for non-redundant installations.	1		X			
J 51	Provide on-board position source integrity monitoring per DO-242A, DO-260A, DO-282A	2		X			
fPR 3.2.2.2.2.4	Position and Velocity Information Accuracy Vertical and horizontal position and velocity uncertainty is a 95% accuracy limit on the position and velocity, respectively	1		X			
fPR 3.2.2.2.2.4	f.The Aircraft/Vehicle shall provide position information with a 95% probability of a maximum error less than or equal to 0.1NM to support the ATC Surveillance application in the terminal environment.	1		X			
	[RTCA DO-160D, Environmental Testing, DO -178B, Software	2			X		

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
	Assurance, DO-200, database processes]						
fPR 3.2.3.2.2	Position Accuracy The aircraft navigation source and avionics are contributors to ADS-B Report position and velocity accuracy. The ADS-B Report also includes quality parameters for the reported position and velocity. a. The LSP/BCS Function shall preserve the target position and velocity accuracy represented in each ADS-B Report.	1		X			
fPR 3.2.3.2.4	Integrity ADS-B Messages are received, processed and transported by the LSP/BCS function to the ATC Automation Function. The integrity of ADS-B Reports cannot be compromised by the LSP/BCS as a result of software or hardware failures. a. The probability that LSP/BCS introduces hazardously misleading information into an ADS-B Report while being processed shall be 10-5 or better per hour.	1		X			
3.2.4.1.2	Accuracy a. The ATC Automation Function shall preserve the airborne horizontal position accuracy of ADS-B Reports.	1		X			
3.2.4.1.2	b. The ATC Automation Function tracking performance with ADS-B data shall be equal or exceed tracking performance with radar in automation systems.	1		X			
3.2.4.1.2	c. The ATC Automation Function shall only use ADS-B Reports with accuracy and integrity values that meet configured/adapted thresholds as inputs to tracking, safety alert and display functions.	1		X			
3.2.4.1.4	Integrity a. The ATC Automation Function shall preserve the integrity of reported airborne horizontal positions.	1		X			
	b. The ATC Automation Function probability that Automation fails to detect large jumps in an aircraft position in an ADS-B Report that is outside the probable position shall be better than or equal to 10-3.	1		X			
	c. The ATC Automation Function allowable rate of false (self) conflict alerts due to non-correlation of ADS-B and radar targets in overlapping ADS-B/radar airspace shall not impact ATC's ability to control air traffic.	1		X			
fPR 3.1.5	Maintenance Function 3.1.5.1 Inputs d. The Maintenance Function shall receive GNSS status from external sources to assess the operational status of the GNSS sources in the Aircraft/Vehicle Function.	1		X			
fPR 3.1.5	b. The Maintenance Function shall display Alerts and Alarms to the system operator.	1		X			
fPR 3.1.5	c. The Maintenance Function shall display the operating status of system functions and components.	1		X			
fPR 3.2.1.5	System Latency for ATC Surveillance Application The System Latency is the sum of the aircraft/vehicle latency from the time of applicability, the LSP/BCS latency with telecommunications, and the ATC Automation latency. a. The latency from time of applicability of the ADS-B Message data until display by ATC Automation shall be less than or equal to 2.7 seconds to provide ATC Surveillance in Terminal airspace.	1		X			
fPR 3.1.4	ATC Automation Function 3.1.4.2 Processing d. The ATC Automation Function shall link valid ADS-B Reports with other surveillance sources to avoid duplicate tracks on a single target from being displayed.	1		X			
3.1.4.2	Processing j. The ATC Automation Function shall provide registration between ADS-B and radar.	1		X			
JH 55	Use error detecting and correction codes in ADS-B transmissions	1	X				
	AIM Section 7-2-2 Altimeter Setting Procedures	2					

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
ML 3	ATCT use of 7110.65 procedures for validating aircraft ID, position, and altitude	2					
fPR 3.1.1	Aircraft/Vehicle Function 3.1.1.1 ADS-B Transmission 3.1.1.1.1 Inputs b. The Aircraft/Vehicle Function shall include an FAA approved pressure altitude sensor as the primary barometric altitude data source.	1	X				
fPR 3.2.2.2.2.4.4	fPR 3.2.2.2.2.4.4 Vertical Position b. The Aircraft/Vehicle shall provide barometric altitude with an accuracy commensurate with the pressure altitude source to support the ATC Surveillance application.	1	X				
fPR 3.2.2.2.2.5.4	Identification and Altitude Integrity b. The likelihood that the Aircraft/Vehicle transmits an incorrect altitude shall be less than 10-3 per flight hour for aircraft without an RVSM altimetry system to support the ATC Surveillance application.	1	X				
	c. The likelihood that the Aircraft/Vehicle transmits an incorrect altitude shall be less than 10-5 per flight hour for aircraft with RVSM altimetry systems to support the ATC Surveillance application.	1	X				
	TAWS	2					
	1090 MHz and UAT MOPS provide requirements for message formats	2					
	1090 MHz and UAT MOPS provide requirements for spectrum requirements	2					
fPR 3.2.2.2.2	Aircraft/Vehicle ADS-B Transmission The Aircraft/Vehicle transmits ADS-B Messages in support of all applications. The requirements in this section apply to all applications, unless a specific application is listed in the requirement text.	1	X				
3.2.2.2.2.6	Availability a. Aircraft/Vehicle function shall provide a minimum availability of 0.9995 for non-redundant installations.	1	X				
fPR 3.1.5	Maintenance Function 3.1.5.3 Outputs h. The Maintenance Function shall provide a list of ADS-B equipped aircraft/vehicles that are not in compliance with the datalink standards.	1			X		
fPR 3.1.4.2	Processing j. The ATC Automation Function shall provide registration between ADS-B and radar.	1	X				
	Aircraft use “flying lights” (aids visibility to and from other traffic)	2					
	Radio communication to announce intentions upon approach to uncontrolled airport	2					
	DO-289 Table 3-20 Subsystem integrity and availability risk requirements	2					
JH 50	Provide a backup system for surveillance or navigation	2					
DO-289 3.3.3.2	The CDTI shall R3.270 support the display of at least 30 traffic symbols	1		X			
fPR 3.2.3.4	ADS-R Surveillance Service The LSP/BCS receives ADS-B on each approved data link and provides corresponding ADS-R Messages on the opposite datalinks. a. The LSP/BCS *shall* provide ADS-R data on those aircraft/vehicles actively transmitting ADS-B only on UAT to aircraft able to receive on 1090ES.	1	X				
	b. The LSP/BCS *shall* provide ADS-R data on those aircraft/vehicles actively transmitting ADS-B only on 1090ES to aircraft able to receive on UAT.	1		X			
	c. The ADS-R service *shall* meet the performance requirements for the Enhanced Visual Acquisition	1		X			
	DO-289 3.3.3.2 The CDTI shall R3.270 support the display of at least 30 traffic symbols	1		X			
	DO-289 Table 3-20 Subsystem integrity and availability risk requirements	1		X			
ML 46	Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations.	1		X			

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
fPR 3.2.3.3	TIS-B Surveillance Service: a. The TIS-B Service *shall* support the following application: Enhanced Visual Acquisition.	1		X			
fPR 3.2.3.3.9	False Report Rate The LSP/BCS *shall* not increase the false TIS-B Report rate relative to the false measurement rate of the contributing sensor or sensors used to produce the TIS-B Reports.	1		X			
ASA MAPS R3.172	The ASSAP ***shall*** include a correlation function that associates traffic data from different surveillance sources that relate to the same a/v track	1	X				
fPR 3.1.3.2	Processing g. The BCS shall associate ADS-B equipped targets with TIS-B Tracks.	1		X			
	h. The BCS Function shall filter TIS-B Reports that have a corresponding ADS-B track on the same target.	1		X			
	Pilot training includes guidance to scan for other traffic at VOR intersections	2					
fPR 3.2.3.3.4	Integrity a. The probability that the LSP/BCS introduces hazardously misleading information into a TIS-B Report while being processed shall not exceed 10^{-3} per hour of operation.	1		X			
fPR 3.2.3.3.2	Position Accuracy c. The LSP/BCS *shall* provide TIS-B Reports with altitude accuracy of 148 feet with a 95% probability.	1		X			
	On-board GPS integrity monitoring per TSO-C129 or TSO-C145	1		X			
7110.65 (Section 7-2-1):	Once aircraft are cleared for visual approaches, ATC must advise the pilot if the radar targets appear likely to converge. If aircraft are on converging courses, ATC must inform the other aircraft of the traffic and that visual separation is being applied.	2					
	Pilot may stop to ask ATC direction [H42]	2					
	Crew cross check with other redundant info. (e.g., visual, paper maps, mental model).	2					
	Airport Movement Area signage	2					
	Design ADS-B to be hardened against electromagnetic interference to the standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-46D and FCC Regulations	1	X		X		
fPR 3.2.3.4.4	ADS-R Surveillance Service Coverage a. ADS-R shall be user-accessible within the coverage volumes designated for this service.	1	X				
	b. ADS-R coverage shall include, but not be limited to the following: • In en route, terminal and air sovereignty airspace per NAS-SR-1000, section 3.2.3 G(3) and (4) • The aircraft movement area at airports with a control tower.	1	X				
	The Flight Information Publication (FLIP) is updated every 56 days to account for airport map changes such as those due to magnetic drift.	2					
	Airports must be resurveyed whenever there is an Airport Movement Area change.	2					
fPR 3.2.2.2.3.2	Airport Map: a. AMDB airport data *shall* be formatted in accordance with RTCA DO-291, *Interchange Standards for Terrain, Obstacle, and Aerodrome Mapping Data.*	1		X			
	b. The AMDB *shall* be in accordance with RTCA DO-272, *User Requirements for Aerodrome Mapping Information,* and DO 200-A, *Standards for Processing Aeronautical Data.*			X			
	c. The Aircraft/Vehicle *shall* include airport map databases for intended			X			

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
	United States, civil and joint-use, towered-airports within the areas of operation. *AMDB production and maintenance capability* shall *be expandable and scalable to accommodate the airports at which the operator desires to employ the Airport Surface Situational Awareness and Final Approach and Runway Occupancy Awareness applications.*						
fPR 3.2.2.2.2.4.2	Horizontal Velocity The Aircraft/Vehicle *shall* provide a horizontal velocity with a maximum error of less than or equal to 9.8 feet per second with a 95% probability to support the Conflict Detection, Airport Surface Situational Awareness, and Final Approach and Runway Occupancy applications.			X			
	VAPIs (red and white visual approach indicator lights) indicate when an aircraft is too low or high for a safe approach	2					
	On an ILS approach, instrumentation will indicate a discrepancy if the pilot descends based on wrong auto zoom.	2					
fPR 3.2.2.2.1.1	Latency a. The maximum latency from measurement of position and velocity information in the transmitting aircraft/vehicle and display of this position / velocity information in the receiving a/v shall be less than 3 seconds to support the CD application	1		X			
DO-289	§3.3.3.1.3.1 suggests filtering criteria for the CDTI.	2					
AIM, 7110.65	Pilot read-back of ATC instructions (ATC will detect pilot has not heard instructions if there is no read-back)	2					
DO-289 3.3.1.6.4	TCAS/ACAS alerts shall have priority over all ASA alerts	2					
DO-289 §3.3.1.6.4	"TCAS alerts shall have priority over ASA alerts."	2					
DO-289	DO-289 specifies that flight crews are not to maneuver solely on the basis of a CD alert.	2					
fPR 3.2.3.5.1	Latency The delay for LSP/BCS processing of FIS-B products shall be less than 10 seconds.	1		X			
fPR 3.2.3.5.9	Product Characteristics a. The FIS-B products shall be consistent in content and extent with FIS information used by Flight Service and Air Traffic Specialists at NAS ground facilities.	1				X	
	b. All FIS products shall be based on government approved data sources. (approved by FAA Order 8400.1)	1				X	
fPR 3.2.1.4	FIS-B Service Availability The FIS-B service is a safety-essential service as classified by NAS-SR-1000. a. The service availability for FIS-B shall be 0.999.	2					
	Pilots obtain weather reports from external sources before takeoff	2					
	If tuned into ATIS or flight service station could get same information	2					
	For IFR flights, ATC is required to provide AWW related information to aircraft on frequency	2					
	Visual and physical cues to the pilot that severe weather is in the vicinity (e.g., high clouds associated with tornadic activity, high winds)	2					
	Pilots will visually detect clouds ahead and have an opportunity to avoid flying into a cloud layer	2					
	Upon encountering a cloud layer, pilots may turn around and choose an alternate course	2					
	VFR charts provide locations and altitudes of SUA and default times when they are active	2					
	The military notifies the FAA 24 hours in advance when there is a change to SUA default active times	2					
	The FAA shall define and implement requirements for an independent automated safety monitoring capability that monitors inputs and outputs at interfaces between SBS subsystems and provides fault diagnostics, failure control and correction, and configurable status monitoring and alarm annunciation. Software for the automated safety monitoring capability shall satisfy the objectives for Assurance Level 2 defined in	0					X

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
	RTCA DO-278 or an equivalent software design assurance standard.						
	The SBS Contractor shall adhere to industry best practices for software development.	0					X
	The ADS-B system shall be designed to meet Mil-STD-461 requirements for electromagnetic susceptibility and interference.	0	X				
	The combined probability that ADS-B primary and backup surveillance fails shall be no more than extremely remote (i.e., 10^{-7})	0	X				
	The FAA shall develop and implement certification procedures to verify that SBS ground equipment performance is within tolerance.	0					X
	The FAA shall perform an analysis of 1090 MHz spectrum utilization impacts given peak ADS-B, Mode S, and Mode A/C target loads and densities and the worst-case potential combination of ATC surveillance systems which utilize the 1090 MHz spectrum in the same service area. The spectrum analysis shall evaluate the impacts to aircraft transponder occupancy, TCAS performance, and the probability of target detection for each ATC surveillance system considered above. If deemed necessary based on the results of the spectrum analysis, the FAA shall develop a mitigation strategy to minimize the risk to maintaining required ATC surveillance systems' performance and required TCAS performance.	0					X
	The system shall provide a notification to maintenance operators prior to reaching a computer processing utilization threshold at which target data may be lost or dropped.	0				X	
	The system shall provide a notification to maintenance operators prior to reaching a telecommunications loading threshold at which target data may be lost or dropped.	0				X	
	The system shall provide a notification to maintenance operators prior to reaching a computer memory utilization threshold at which target data may be lost or dropped.	0				X	
	The probability that the system fails to notify ATC when surveillance data is missing for an adaptable amount of time shall be no more than 10^{-7}.	0	X				
	When selecting locations for ADS-B ground stations, the FAA shall perform a coverage / siting analysis that considers aircraft bank angles which may result in line-of-sight coverage problems (e.g., the aircraft banks such that the transmit / receive antenna is angled away from the ground station antenna).	0					X
	The FAA shall perform a collision risk analysis in accordance with Flight Standards guidelines to determine the required availability of the Aircraft/Vehicle function given terminal separation standards and end-to-end (i.e., air / ground) system performance parameters	0					X
	Hardware for the Aircraft/Vehicle function shall comply with RTCA DO-160D Environmental Conditions and Test Procedures for Airborne Equipment.	0			X		
	The approval process for design, production, installation, and operation of ADS-B equipment onboard civil aircraft shall comply with "The FAA and Industry Guide to Product Certification" and "The FAA and Industry Guide to Avionics Approvals."	0					X
	The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B and ancillary equipment.	0					X
	The end-to-end system latency shall not exceed the maximum acceptable latency based on Flight Standards collision risk analysis.	0		X			
ML 32:	The FAA shall ensure accuracy of the terrain/airfield map displayed to ATC.	0					X
	The FAA shall develop and implement procedures to verify alignment of surveillance sensor data to the automation system display map.	0					X
	The FAA shall develop and implement certification procedures to verify that barometric pressure correction applied at the automation system is accurate.	0					X
	The FAA shall maintain legacy surveillance systems until ADS-B equipage level deemed sufficient to remove legacy systems and transition to NRA.	0					X
	Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI	0					X
	Train pilots to check for updated weather information pre-flight and in-flight and to refrain from over-relying on the CDTI	0					X
	The FAA shall provide NOTAMS or other pilot notification to indicate	0					X

ID	Requirement or Objective	V&V Status	Planned Verification Method * applies to objectives / non-system reqmts only				
			A	T	I	D	Assess*
	that not all traffic are participants in CDTI- based applications [C418]						
	Provide warnings and cautions regarding over-reliance on CDTI in avionics equipment manuals, pilot training manuals, and AIM [C416, C418]	0					X
	Provide placard on CDTI to indicate application / display only for situational awareness / advisory use	0					X
	The CDTI shall provide indication when the status is such that (a) Inadequate or invalid surveillance data would cause unacceptable traffic information display. (b) Inadequate or invalid own-ship data would cause unacceptable traffic information display (c) Application processing is not functioning normally.	0					X
	Processing and interface capacities shall be specified to accommodate the traffic densities and operating ranges for the most demanding application(s).	0					X
	The enhanced visual application shall notify the air crew when altitude information is missing.	0					X
	The Conflict Detection Application shall provide an indication that alerts have been disabled	0		X			
	Software for the Aircraft/Vehicle function shall satisfy the objectives for Software Level C defined in RTCA DO-178B or an equivalent software design assurance standard.	0					X
	Make filtering criteria standard in the CDTI MOPS	0					X
	The CDTI shall provide volume control to adjust for ambient noise in the cockpit.	0		X			
	The Conflict Detection application shall present only one alert level at a time. (Note: Verify that corresponding ASA MASPS statement in section D.2.2.2 pg D-24 for preventing issuance of simultaneous alerts is carried through in MOPS)	0		X			
	The FAA shall analyze and characterize the separation errors at the ATC display between each combination of ADS-B and radar-only targets.	0					X
	The FAA shall perform a collision risk analysis to validate separation standards.	0					X
	ATIS radio broadcasts	2					X
	The probability that the system displays an incorrect target ID to the controller shall be less than 10-6.	0	X				
	The FAA shall develop and publish procedures for pilots to implement when concerned with ATC instructions based on traffic and / or weather information presented on the CDTI (Note: This recommended requirement does not preclude defining procedures in which the pilot must comply with ATC instructions regardless of information presented on the CDTI).	0					X

7. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

A total of 80 hazards were identified as part of the preliminary hazard analysis. Of these hazards, 8 are assessed as having high initial risk, 15 as having medium initial risk, and 57 as having low initial risk. Current and predicted residual risks are plotted in the risk matrices in Figures 8-1 and 8-2, respectively.

With the verification of the following recommended safety requirements, the assessed risks for each alternative all fall in the medium to low range:

- The FAA shall define and implement requirements for an independent automated safety monitoring capability that monitors inputs and outputs at interfaces between SBS subsystems and provides fault diagnostics, failure control and correction, and configurable status monitoring and alarm annunciation. Software for the automated safety monitoring capability shall satisfy the objectives for Assurance Level 2 defined in RTCA DO-278 or an equivalent software design assurance standard.
- The SBS Contractor shall adhere to industry best practices for software development.
- The ADS-B system shall be designed to meet Mil-STD-461 requirements for electromagnetic susceptibility and interference.
- The combined probability that ADS-B primary and backup surveillance fails shall be no more than extremely remote (i.e., 10^{-7})
- The FAA shall develop and implement certification procedures to verify that SBS ground equipment performance is within tolerance.
- The FAA shall perform an analysis of 1090 MHz spectrum utilization impacts given peak ADS-B, Mode S, and Mode A/C target loads and densities and the worst-case potential combination of ATC surveillance systems which utilize the 1090 MHz spectrum in the same service area. The spectrum analysis shall evaluate the impacts to aircraft transponder occupancy, TCAS performance, and the probability of target detection for each ATC surveillance system considered above. If deemed necessary based on the results of the spectrum analysis, the FAA shall develop a mitigation strategy to minimize the risk to maintaining required ATC surveillance systems' performance and required TCAS performance.
- The system shall provide a notification to maintenance operators prior to reaching a computer processing utilization threshold at which target data may be lost or dropped.
- The system shall provide a notification to maintenance operators prior to reaching a telecommunications loading threshold at which target data may be lost or dropped.
- The system shall provide a notification to maintenance operators prior to reaching a computer memory utilization threshold at which target data may be lost or dropped.
- The probability that the system fails to notify ATC when surveillance data is missing for an adaptable amount of time shall be no more than 10^{-7}.
- When selecting locations for ADS-B ground stations, the FAA shall perform a coverage / siting analysis that considers aircraft bank angles which may result in line-of-sight coverage problems (e.g., the aircraft banks such that the transmit / receive antenna is angled away from the ground station antenna).
- The FAA shall perform a collision risk analysis in accordance with Flight Standards guidelines to determine the required availability of the Aircraft/Vehicle function given terminal separation standards and end-to-end (i.e., air / ground) system performance parameters
- Hardware for the Aircraft/Vehicle function shall comply with RTCA DO-160D Environmental Conditions and Test Procedures for Airborne Equipment.
- The approval process for design, production, installation, and operation of ADS-B equipment onboard civil aircraft shall comply with "The FAA and Industry Guide to Product Certification" and "The FAA and Industry Guide to Avionics Approvals."
- The FAA shall develop and publish AC 20-XX to establish installation and operational approval criteria for ADS-B and ancillary equipment.
- The end-to-end system latency shall not exceed the maximum acceptable latency based on Flight Standards collision risk analysis.
- The FAA shall ensure accuracy of the terrain/airfield map displayed to ATC.

- The FAA shall develop and implement procedures to verify alignment of surveillance sensor data to the automation system display map.
- The probability that the system displays an incorrect target ID to the controller shall be less than 10^{-6}.
- The FAA shall develop and implement certification procedures to verify that barometric pressure correction applied at the automation system is accurate.
- The FAA shall maintain legacy surveillance systems until ADS-B equipage level deemed sufficient to remove legacy systems and transition to NRA.
- The FAA shall analyze and characterize the separation errors at the ATC display between each combination of ADS-B and radar-only targets.
- The FAA shall perform a collision risk analysis to validate separation standards.
- The FAA shall develop and publish procedures for pilots to implement when concerned with ATC instructions based on traffic and / or weather information presented on the CDTI (Note: This recommended requirement does not preclude defining procedures in which the pilot must comply with ATC instructions regardless of information presented on the CDTI).
- Train pilots to be vigilant in executing see and avoid procedures and to refrain from over-relying on the CDTI.
- Train pilots to check for updated weather information pre-flight and in-flight and to refrain from over-relying on the CDTI.
- The FAA shall provide NOTAMS or other pilot notification to indicate that not all traffic are participants in CDTI- based applications.
- Provide warnings and cautions regarding over-reliance on CDTI in avionics equipment manuals, pilot training manuals, and AIM.
- Provide placard on CDTI to indicate application / display only for situational awareness / advisory use.
- The CDTI shall provide the air crew with an indication when: (a) Inadequate or invalid surveillance data would cause unacceptable traffic information display. (b) Inadequate or invalid own-ship data would cause unacceptable traffic information display. (c) Application processing is not functioning normally. The RTCA shall define specific performance requirements for acceptable traffic information display.
- Processing and interface capacities shall be specified to accommodate the traffic densities and operating ranges for the most demanding application(s).
- The enhanced visual application shall notify the air crew when altitude information is missing.
- The Conflict Detection Application shall provide an indication that alerts have been disabled
- Software for the Aircraft/Vehicle function shall satisfy the objectives for Software Level C defined in RTCA DO-178B or an equivalent software design assurance standard.
- The CDTI shall provide volume control to adjust for ambient noise in the cockpit.
- The Conflict Detection application shall present only one alert level at a time. (Note: Verify that corresponding ASA MASPS statement in section D.2.2.2 pg D-24 for preventing issuance of simultaneous alerts is carried through in MOPS)

Figure 7-1: Current Risk Summary

TOTAL COUNT = 80

	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A		CD: H57, H58			
Frequent B		App: H19 Acq: H19	ATC: H85		
Remote C	FAR: H32 CD: H49, H50	Acq: H23, H24 App: H23,H24 Apt: H32, H45 FA: H34, H39 CD: H51, H52, H53, H54, H55, H62, H64	Acq: H25, H29 CD: H60	ATC: H1, H82 CD: H56	ATC: H2 Gen: H81
Extremely Remote D	FAR: H33	Acq: H26, H37 App: H26, H33, H34, H36, H37 Apt: H42, H43, H44, H22, H47 FAR: H22, H44, H41 FIS: H74, H77, H78, H79	ATC: H6 Acq: H22, H44 App: H22, H25, H29, H44, H35 FIS: H66-H73, H75, H76, H80 CD: H65	ATC: H8, H17, H7, H9, H83 FAR: H45 CD: H61, H63	ATC: H4, H5
Extremely Improbable E					

High	8
Medium	15
Low	57

Note: Hazards associated with the ATC Surveillance application are designated by "ATC." For in-cockpit applications, Gen = General, Acq = Enhanced Visual Acquisition, App = Enhanced Visual Approach, CD = Conflict Detection, Apt = Airport Surface Situational Awareness, FAR = Final Approach and Runway Occupancy Awareness, and FIS = Weather and NAS Status Situational Awareness.

Figure 7-2: Predicted Residual Risk Summary

TOTAL COUNT = 80

	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A					
Frequent B					
Remote C	FAR: H32 CD: H49, H50	Acq: H24 App: H24 Apt: H45, H32 FAR: H34, H39 CD: H51-H55, H57, H58, H62, H64			
Extremely Remote D	FAR: H33	Acq: H19, H23, H26 App: H19, H23, H26, H33, H34, H36, H37 Apt: H42, H43, H44, H22, H47; FAR: H22, H44, H41; FIS: H74, H77, H78, H79	ATC: H6, H85 Acq: H22, H25, H29 App: H22, H25, H29, H35, H44 CD: H60, H65 FIS: H66-H73, H75, H76	ATC: H1 CD: H56	
Extremely Improbable E		Acq: H37	Acq: H44	ATC: H7, H8, H9, H17, H83 FAR: H45 CD: H61, H63	ATC: H2, H4, H5, H82 Gen: H81

High	0
Medium	7
Low	73

Note: Hazards associated with the ATC Surveillance application are designated by "ATC." For in-cockpit applications, Gen = General, Acq = Enhanced Visual Acquisition, App = Enhanced Visual Approach, CD = Conflict Detection, Apt = Airport Surface Situational Awareness, FAR = Final Approach and Runway Occupancy Awareness, and FIS = Weather and NAS Status Situational Awareness.

8. REFERENCES / BIBLIOGRAPHY

The primary source documents for this preliminary hazard analysis are:

- "National Airspace System Surveillance and Broadcast Services Concept of Operations," FAA, May 11, 2006
- "National Minimum Aviation System Performance Standards for Aircraft Surveillance Applications (ASA)," (DO-289 Volume 1 and 2), RTCA, Inc. 2003.
- "Exhibit 300, Attachment 1 Final Program Requirements for Surveillance and Broadcast Services," version 1.0, May 9, 2006

Other source documents are included below:

1. Automatic Dependant Surveillance – Broadcast (ADS-B) Design Analysis Report: ADS-B Operational Safety Assessment Operational Services and Environment Description (OSED), Operational Hazard Assessment (OHA), Allocation of Safety Objectives and Requirements (ASOR)," September 6, 2005, Report No. 010927-01

2. "Automatic Dependant Surveillance – Broadcast (ADS-B) Safety Engineering Report #1 Volume I Initial Hazard Analysis," January 21, 2000, Report No. 991215-01

3. "Automatic Dependant Surveillance – Broadcast (ADS-B) Safety Engineering Report #1 Volume II ADS-B End-to-End system Initial Hazard Analysis Matrix of Scenarios MIL-STD-882C Methodology," January 21, 2000, Report No. 991215-01

4. Automatic Dependant Surveillance – Broadcast (ADS-B) Safety Engineering Report #1 Volume III ADS-B Application-Driven Initial Hazard Analysis RTCA SC189 WG 53 CNS/ATM Safety Assessment Methodology," January 21, 2000, Report No. 991215-01

5. "Automatic Dependant Surveillance – Broadcast (ADS-B) Final Draft Design Analysis Report: ADS-B Preliminary Hazard Analysis Volume I Findings and Recommended Safety Requirements, September 20, 2001, Report No. 010920-01

A subset of controls from [5] that met the scope of this document was incorporated.

APPENDIX A: ACRONYMS

ADL	Aeronautical Data Link
ADS-B	Automation Dependent Surveillance - Broadcast
ADS-R	Automatic Dependent Surveillance-Rebroadcast
ASA	Aircraft Surveillance Applications
ATC	Air Traffic Control
ATO SSWG	Air Traffic Organization System Safety Working Group
CDR	Critical Design Review
CDTI	Cockpit Display of Traffic Information
COTS	Commercial Off-the-Shelf
FAA	Federal Aviation Administration
F&E	Facilities and Equipment
FIS-B	Flight Information Service – Broadcast
HTRR	Hazard Tracking and Risk Resolution
HTS	Hazard Tracking System
ISD	In-Service Decision
ISP	Integrated Safety Plan
JRC	Joint Resources Council
LOB	Line of Business
MNS	Mission Need Statement
NAS	National Airspace System
NPRM	Notice of Proposed Rulemaking
O&SHA	Operating and Support Hazard Analysis
OPS	Operations
P	Probability
PHA	Preliminary Hazard Analysis
PMO	Program Management Office
POC	Point of Contact
NOTAM	Notice to Airmen
RAC	Risk Assessment Code
RFO	Request for Offer
SAR	Safety Action Record
SBS	Surveillance and Broadcast Services
SEM	Systems Engineering Manual
SHA	System Hazard Analysis
SLS	System Level Specification
SMS	Safety Management System
SOW	Statement of Work
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SRMP	Safety Risk Management Panel
SRVT	Safety Requirements Verification Table
SSAR	System Safety Assessment Report
SSE	System Safety Engineers
SSHA	Sub-System Hazard Analysis
SSMP	System Safety Management Program
SSP	System Safety Program
SSPP	System Safety Program Plan
TIS-B	Traffic Information Service – Broadcast
V&V	Validation and Verification
VP	Vice President
WJHTC	William J. Hughes Technical Center

SURVEILLANCE AND BROADCAST SERVICES PROGRAM
SEGMENT 1

SAFETY RISK MANAGEMENT DOCUMENT:
PRELIMINARY HAZARD ANALYSIS

VOLUME IV - FAULT TREES AND EVENT TREES

SEPTEMBER 18, 2006

VERSION 1.0

DOCUMENT CHANGE HISTORY

VERSION	DATE	DESCRIPTION OF CHANGES

TABLE OF CONTENTS

APPENDIX B FAULT TREES **1**

B.1 ATC SURVEILLANCE APPLICATION 1
B.2 IN-COCKPIT APPLICATIONS 20
B.2.1 General *20*
B.2.2 Enhanced Visual Acquisition and Approach *22*
B.2.3 Final Approach and Runway Occupancy Awareness (FAROA) and Airport Surface Situational Awareness (ASSA) *27*
B.2.4 Conflict Detection *35*
B.2.5 Weather and NAS Status Situational Awareness *52*

LIST OF FIGURES

FIGURE 1: FAULT TREE FOR H1 1
FIGURE 2: EVENT TREE FOR H1, H17, AND H2 2
FIGURE 3: FAULT TREE FOR H17 3
FIGURE 4: FAULT TREE FOR H2 4
FIGURE 5: FAULT TREE FOR H4 5
FIGURE 6: EVENT TREE FOR H4 AND H5 6
FIGURE 7: FAULT TREE FOR H5 7
FIGURE 8: FAULT TREE FOR H6 8
FIGURE 9: EVENT TREE FOR H6 9
FIGURE 10: FAULT TREE FOR H7 10
FIGURE 11: EVENT TREE FOR H7 11
FIGURE 12: FAULT TREE FOR H8 12
FIGURE 13: EVENT TREE FOR H8 13
FIGURE 14: FAULT TREE FOR H9 14
FIGURE 15: EVENT TREE FOR H9 15
FIGURE 16: FAULT TREE FOR H82 16
FIGURE 17: EVENT TREE FOR H82 17
FIGURE 18: FAULT TREE FOR H83 18
FIGURE 19: EVENT TREE FOR H83 19
FIGURE 20: FAULT TREE FOR H81 20
FIGURE 21: EVENT TREE FOR H81 21
FIGURE 22: EVENT TREE FOR H19 22
FIGURE 23: EVENT TREE FOR H44 23
FIGURE 24: EVENT TREE FOR H22 24
FIGURE 25: EVENT TREE FOR H23 25
FIGURE 26: EVENT TREE FOR H24 26
FIGURE 27: FAULT TREE FOR H32 AND H22 27
FIGURE 28: FAULT TREE FOR H43 28
FIGURE 29: FAULT TREE FOR H44 29
FIGURE 30: FAULT TREE FOR H45 30
FIGURE 31: EVENT TREE FOR H45 (FAROA ONLY) 31
FIGURE 32: FAULT TREE FOR H48 32
FIGURE 33: EVENT TREE FOR H42, H43, H44, H45 (ASSA ONLY), H48, AND H32 33
FIGURE 34: EVENT TREE FOR H22 (ASSA), H34, H39, H41, H44, AND H47 34
FIGURE 35: FAULT TREE FOR H49 AND H50 35
FIGURE 36: FAULT TREE FOR H51 AND H50 36
FIGURE 37: EVENT TREE FOR H51 AND H52 37
FIGURE 38: FAULT TREE FOR H55 AND H56 38
FIGURE 39: EVENT TREE FOR H55 AND H56 39
FIGURE 40: FAULT TREE FOR H53 AND H54 40

FIGURE 41: EVENT TREE FOR H53 AND H54 41
FIGURE 42: FAULT TREE FOR H57 42
FIGURE 43: EVENT TREE FOR H57 43
FIGURE 44: EVENT TREE FOR H58 44
FIGURE 45: EVENT TREE FOR H58 45
FIGURE 46: FAULT TREE FOR H60 46
FIGURE 47: EVENT TREE FOR H60 47
FIGURE 48: FAULT TREE FOR H61 48
FIGURE 49: EVENT TREE FOR H61 49
FIGURE 50: FAULT TREE FOR H61 – H65 50
FIGURE 51: EVENT TREE FOR H61 – H65 51

APPENDIX B FAULT TREES

B.1 ATC Surveillance Application

Figure 1: Fault Tree for H1

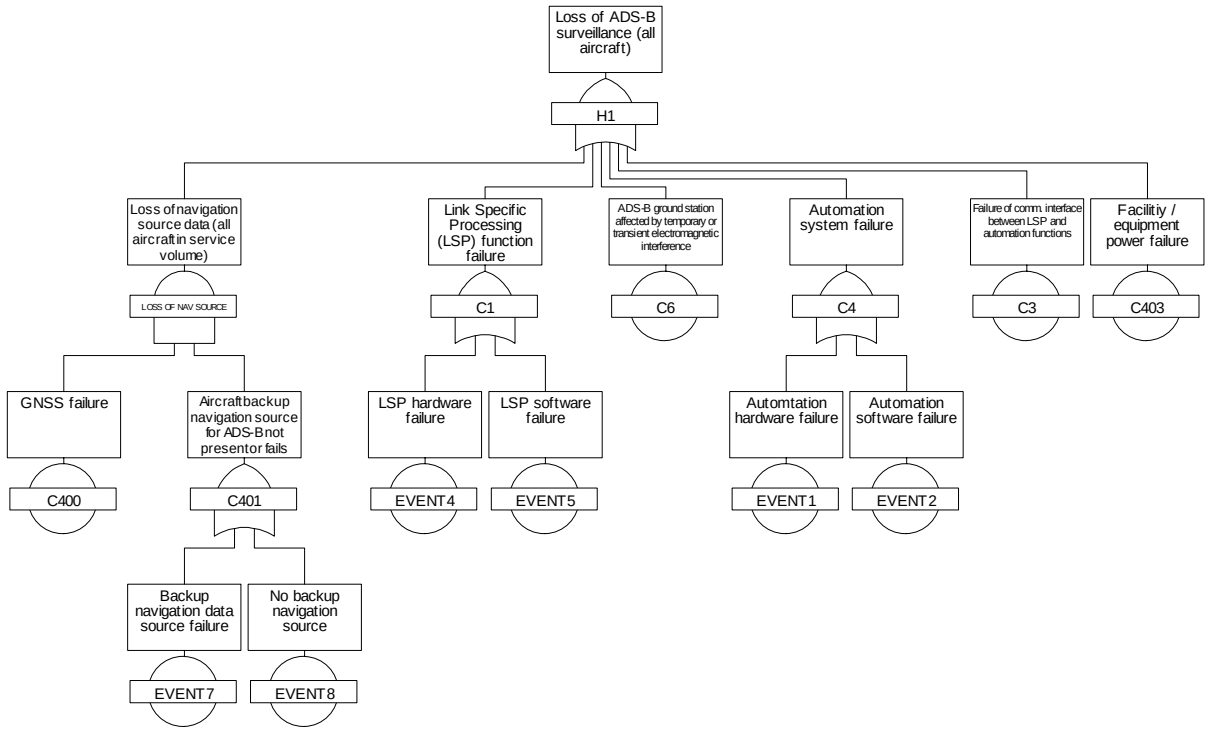


Figure 2: Event Tree for H1, H17, and H2

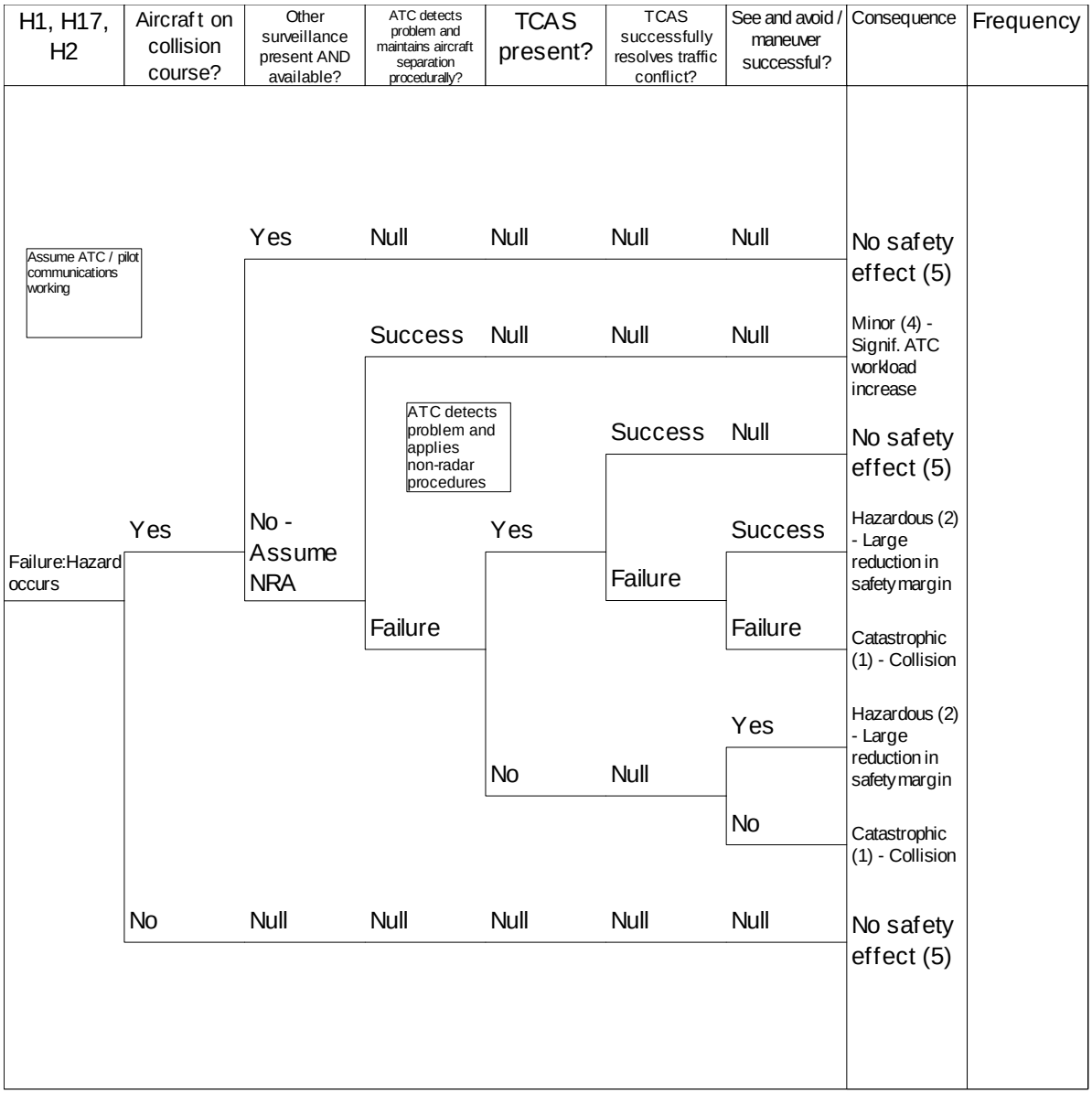


Figure 3: Fault Tree for H17

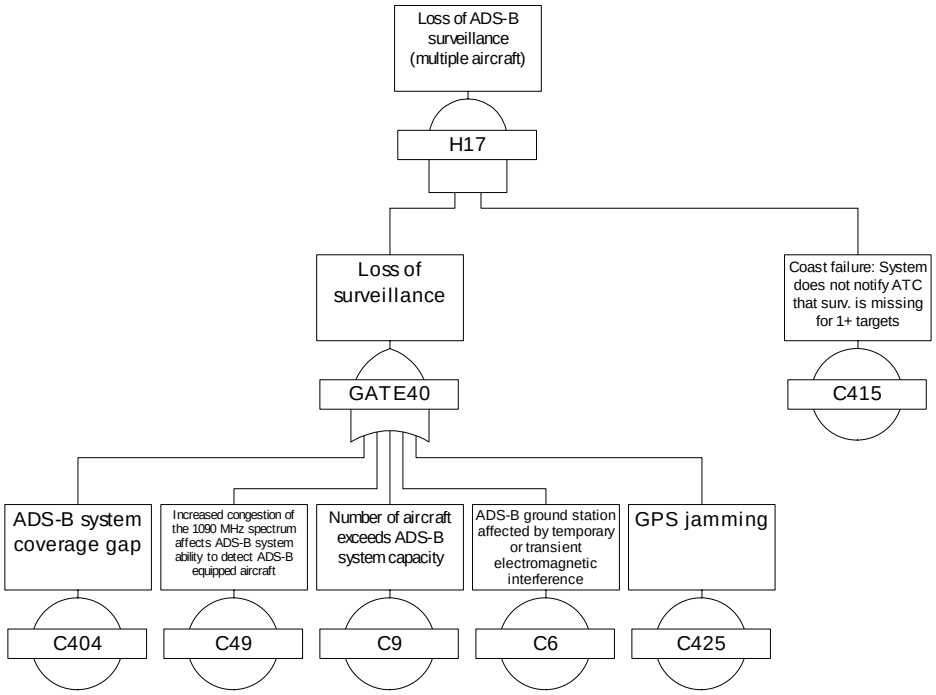


Figure 4: Fault Tree for H2

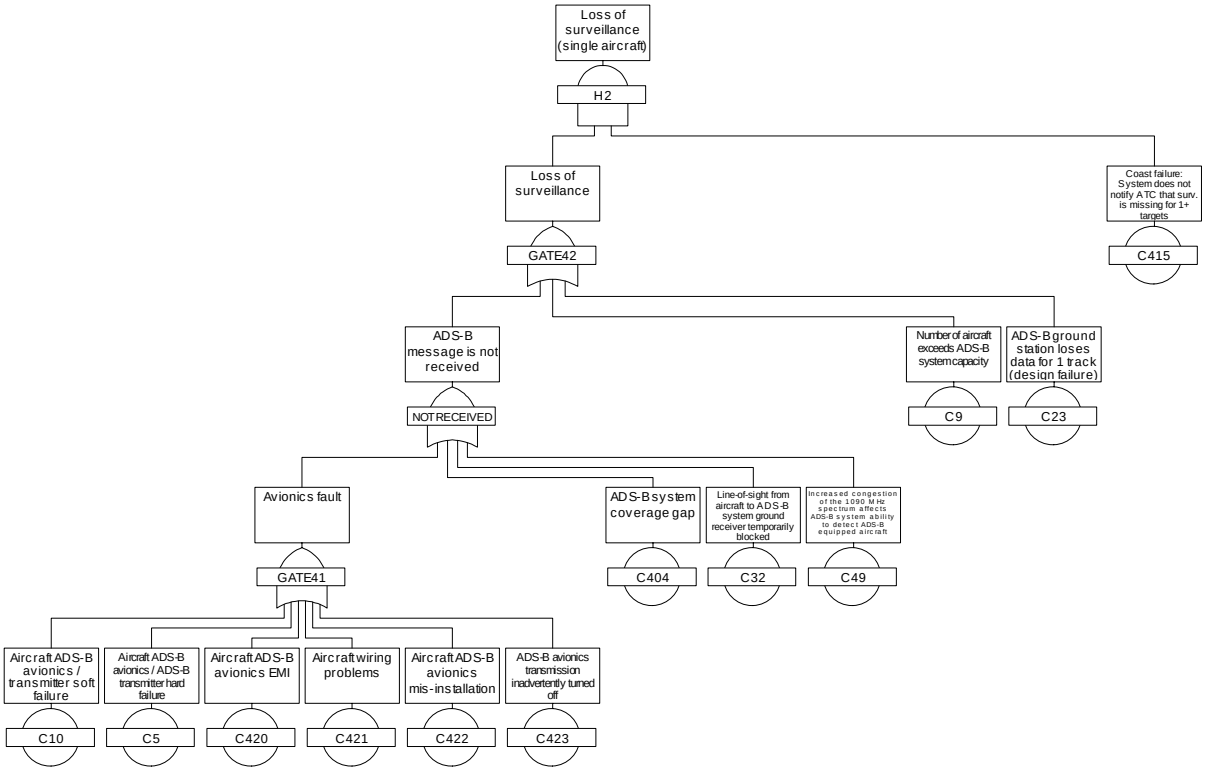


Figure 5: Fault Tree for H4

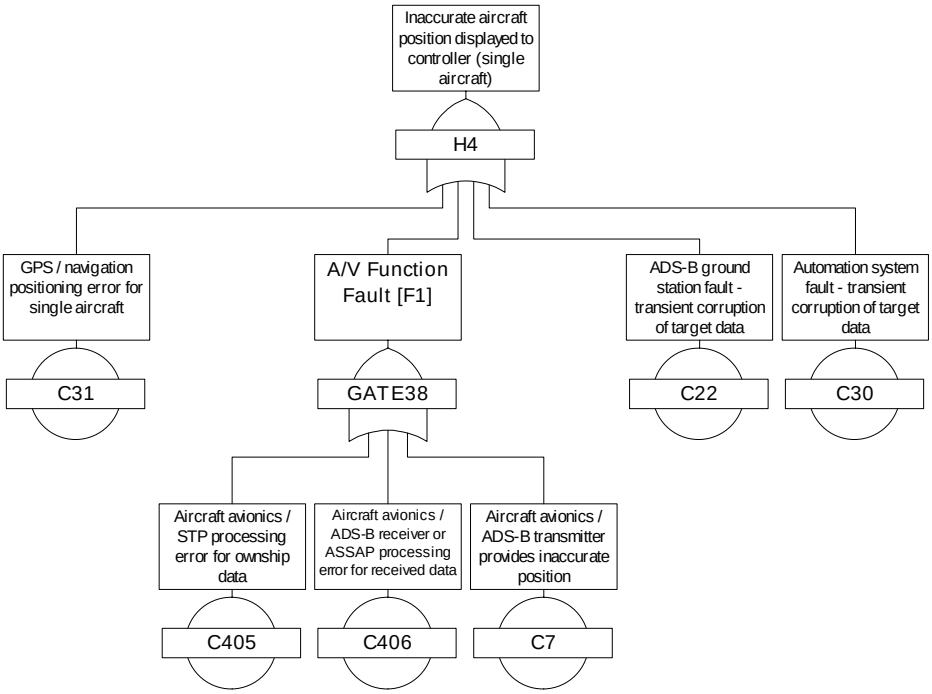


Figure 6: Event Tree for H4 and H5

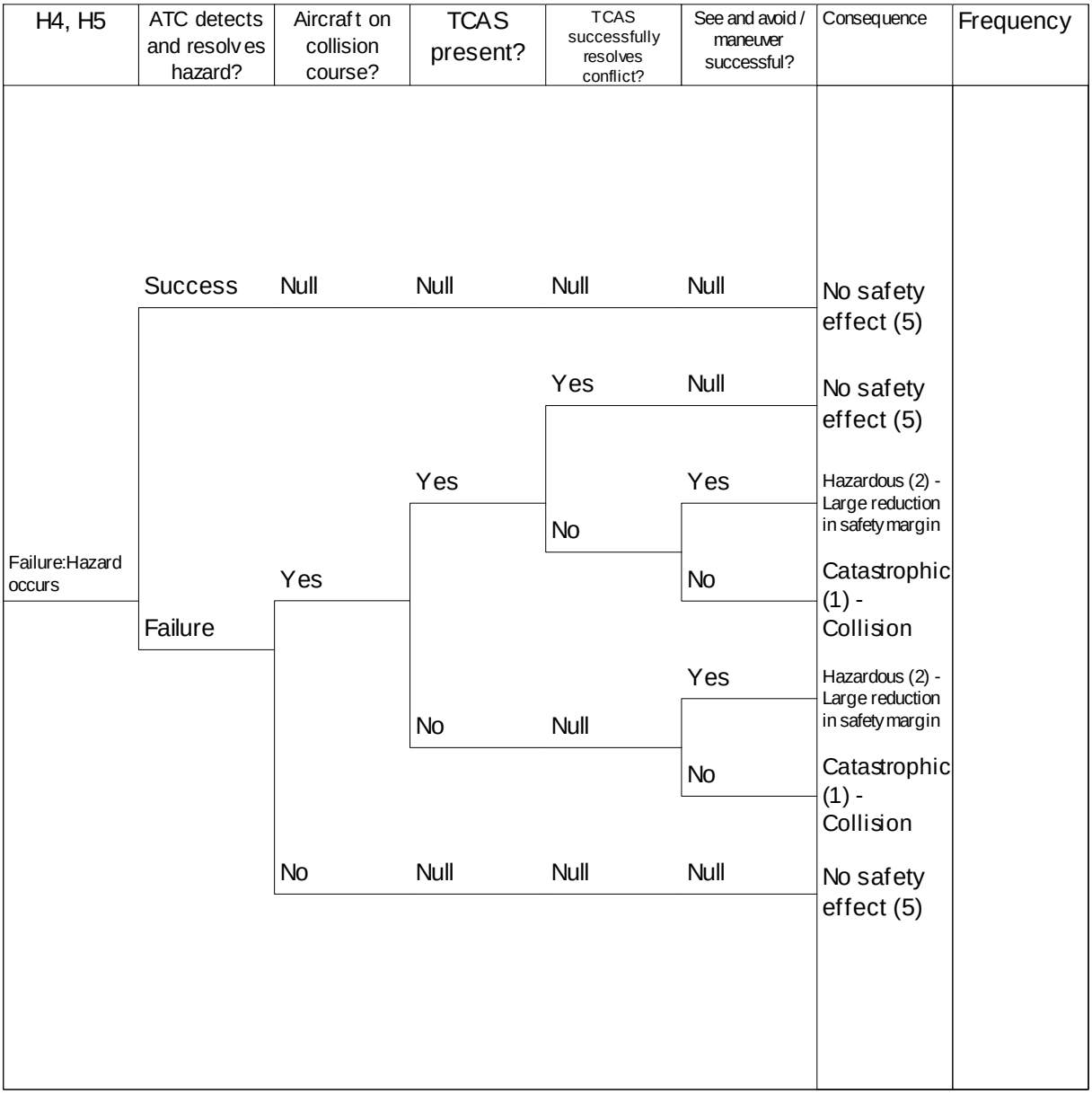


Figure 7: Fault Tree for H5

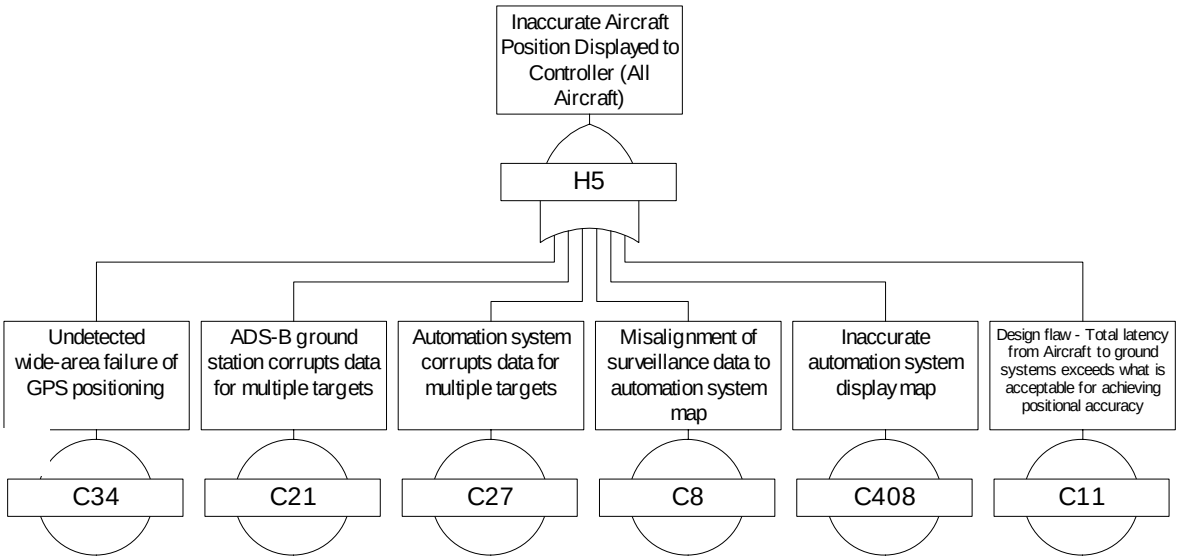


Figure 8: Fault Tree for H6

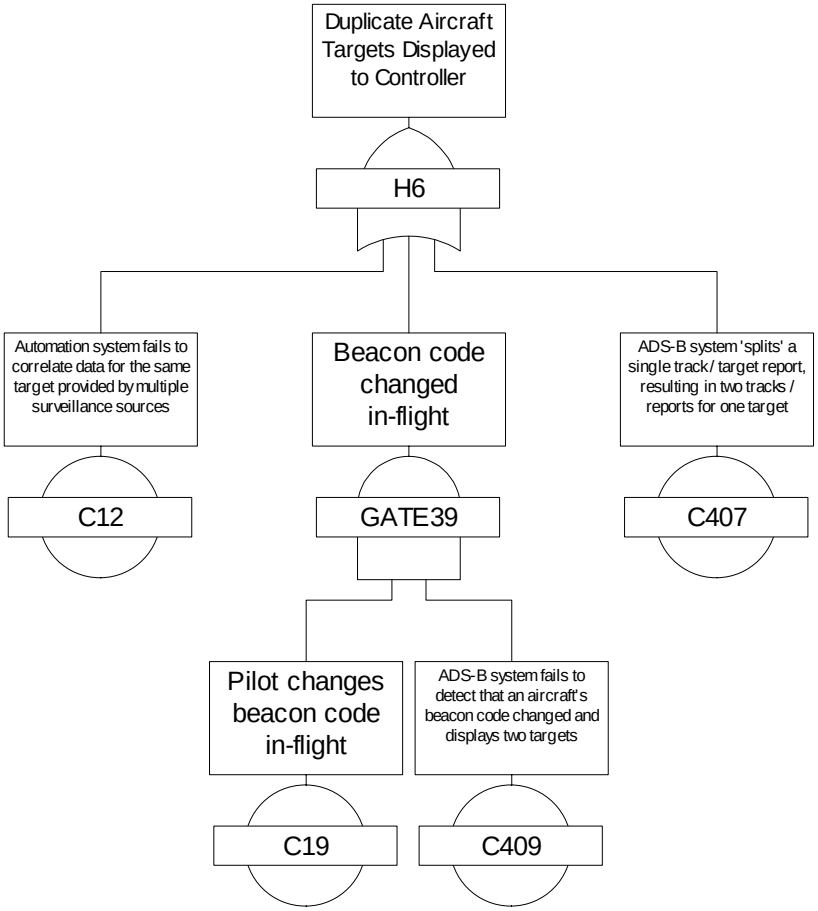


Figure 9: Event Tree for H6

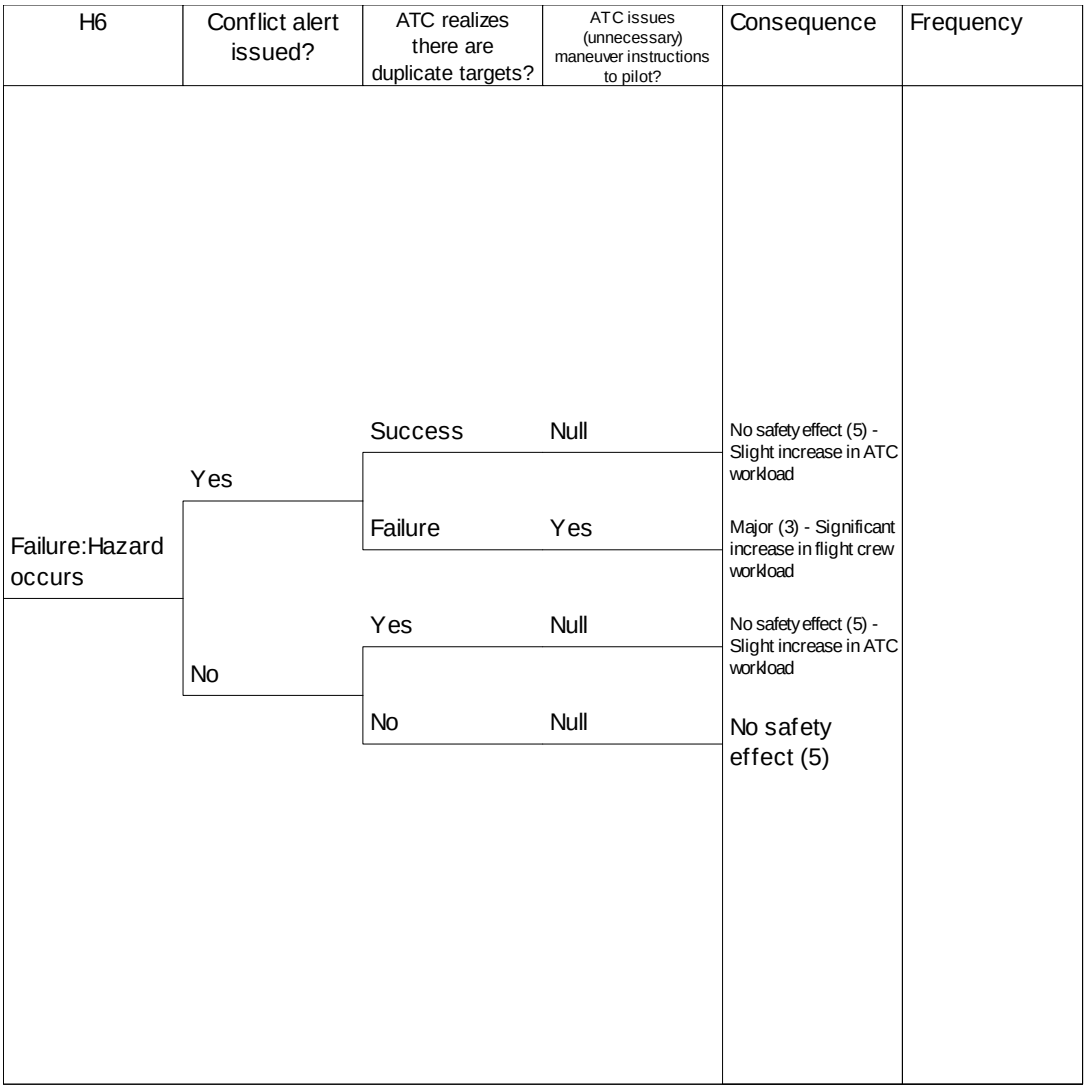


Figure 10: Fault Tree for H7

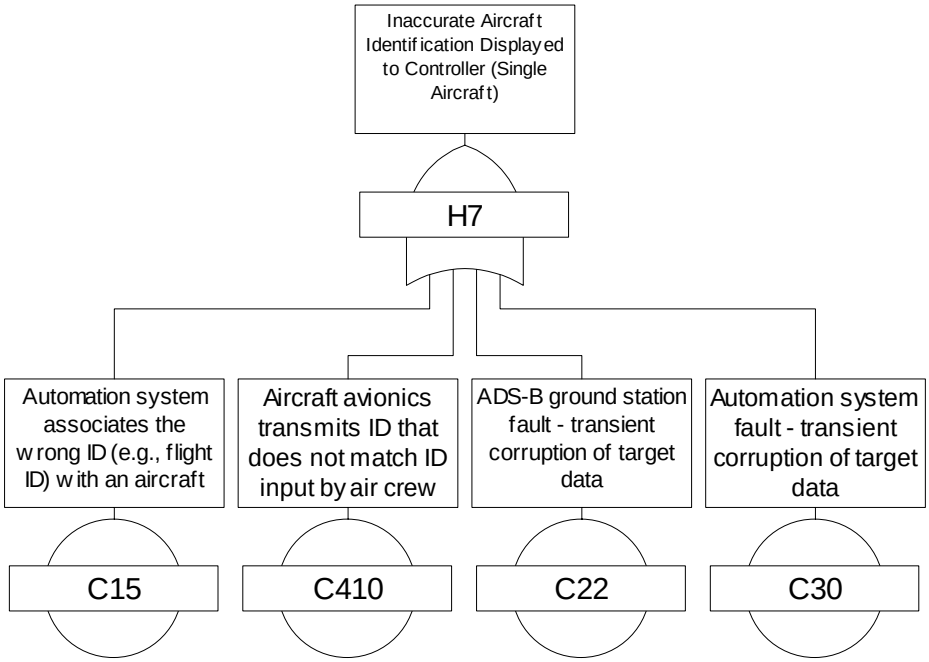


Figure 11: Event Tree for H7

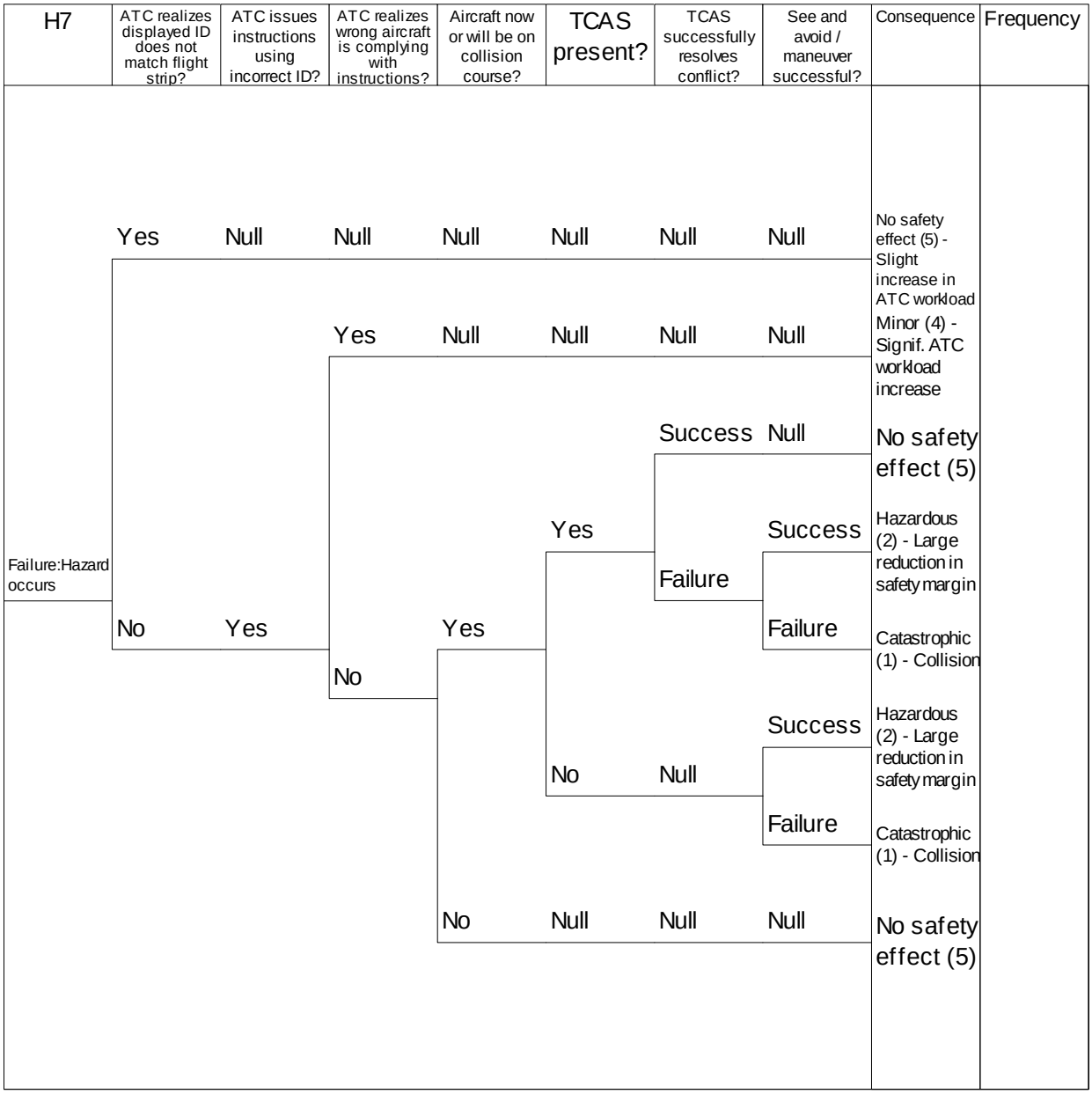


Figure 12: Fault Tree for H8

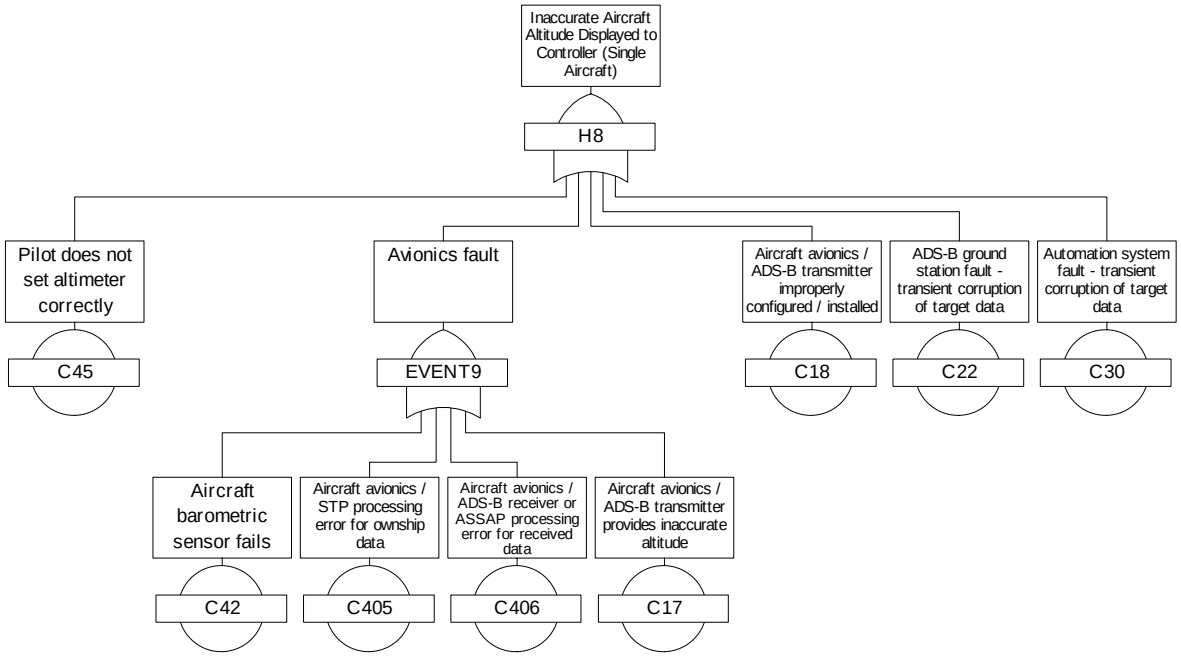


Figure 13: Event Tree for H8

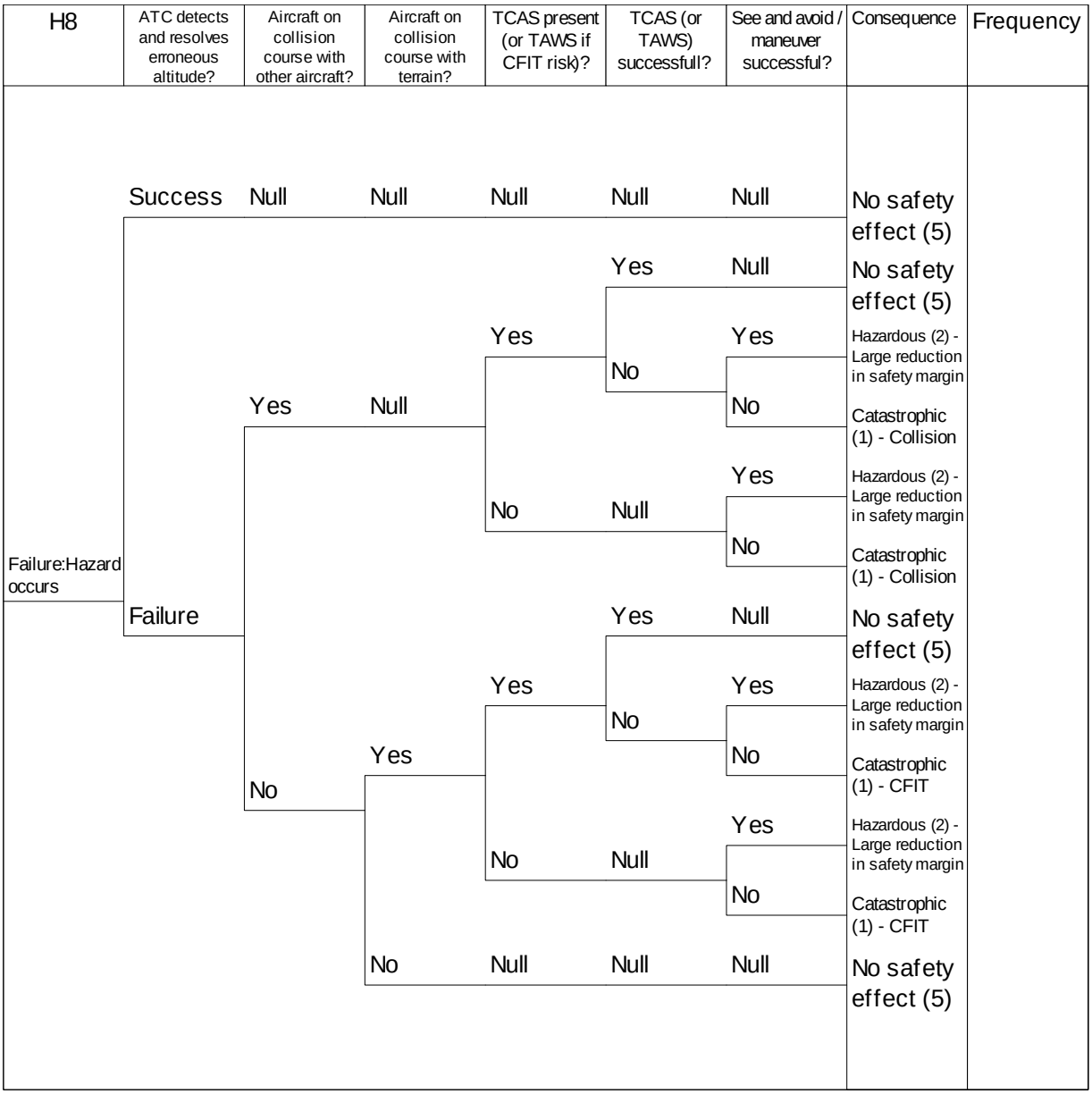


Figure 14: Fault Tree for H9

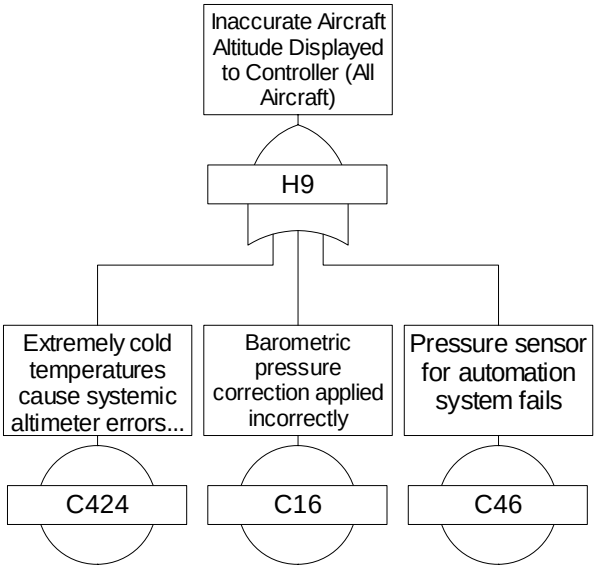


Figure 15: Event Tree for H9

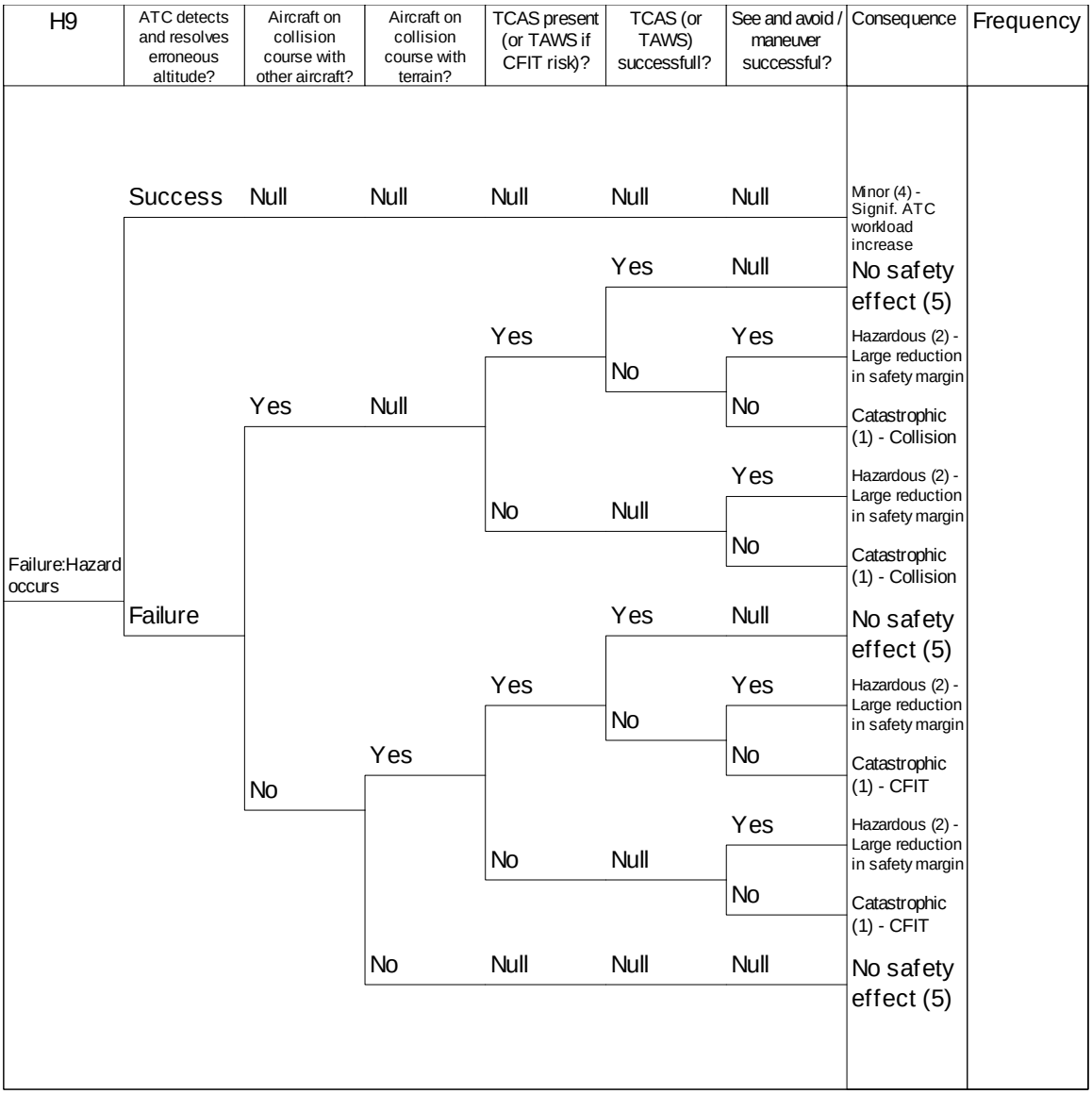


Figure 16: Fault Tree for H82

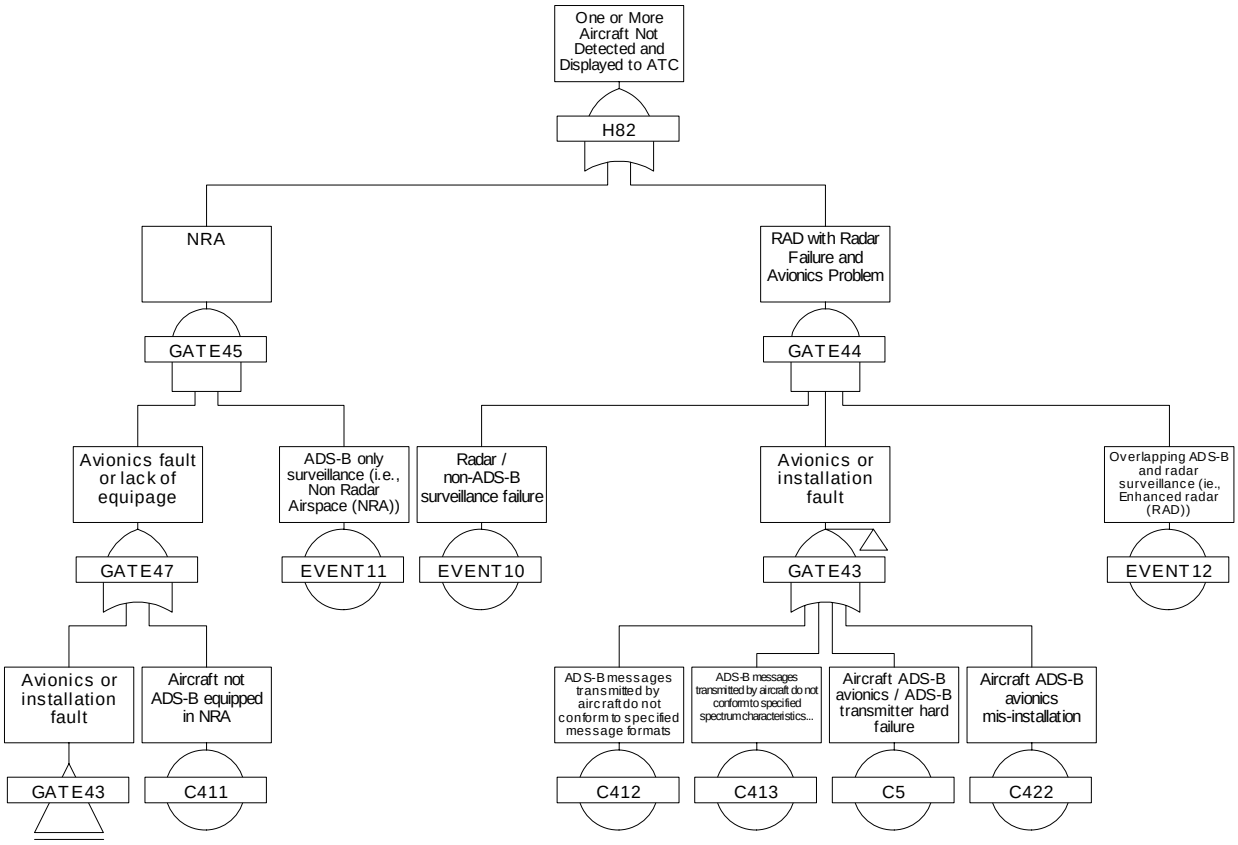


Figure 17: Event Tree for H82

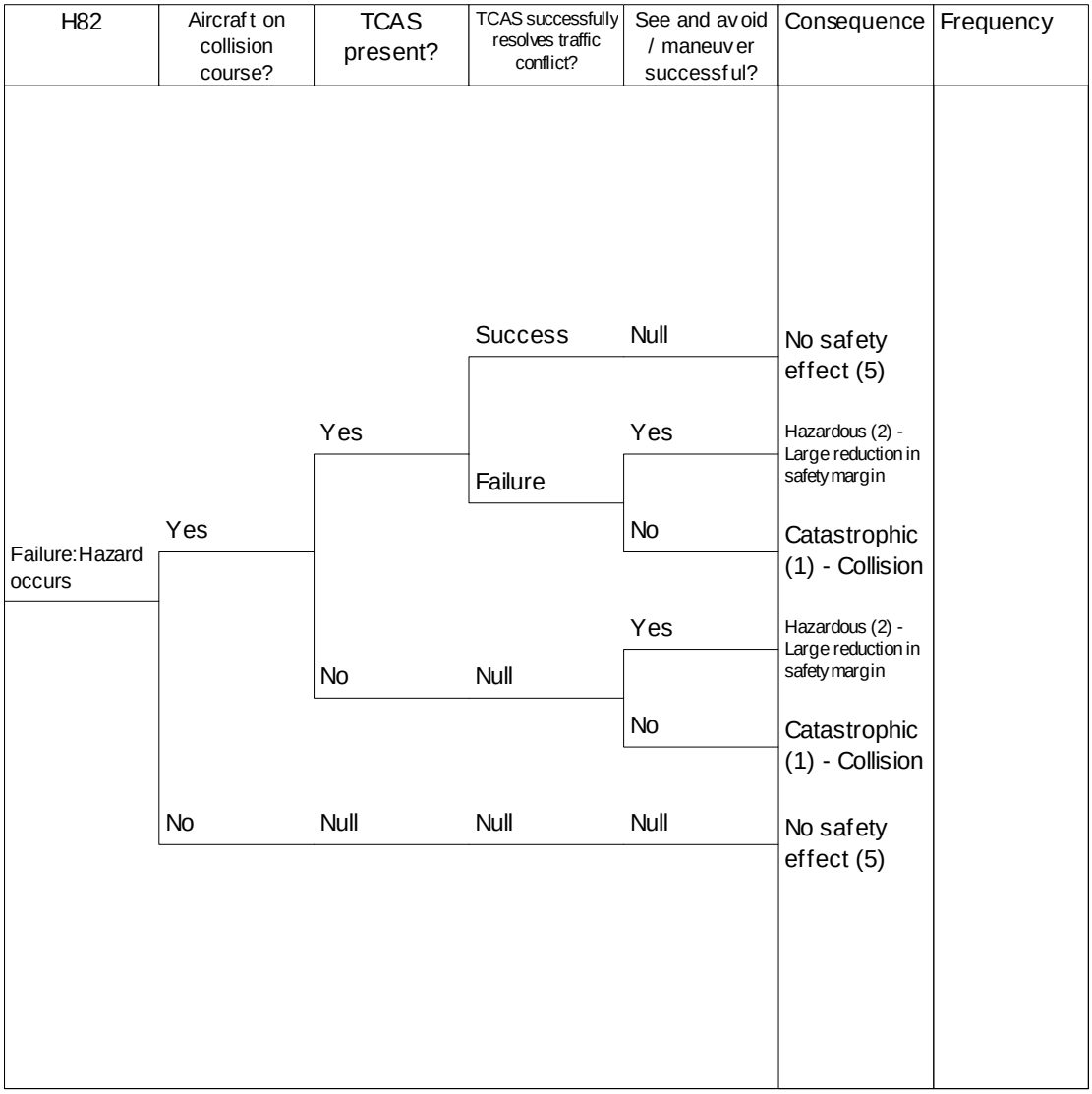


Figure 18: Fault Tree for H83

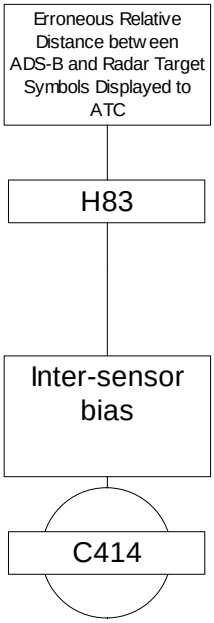
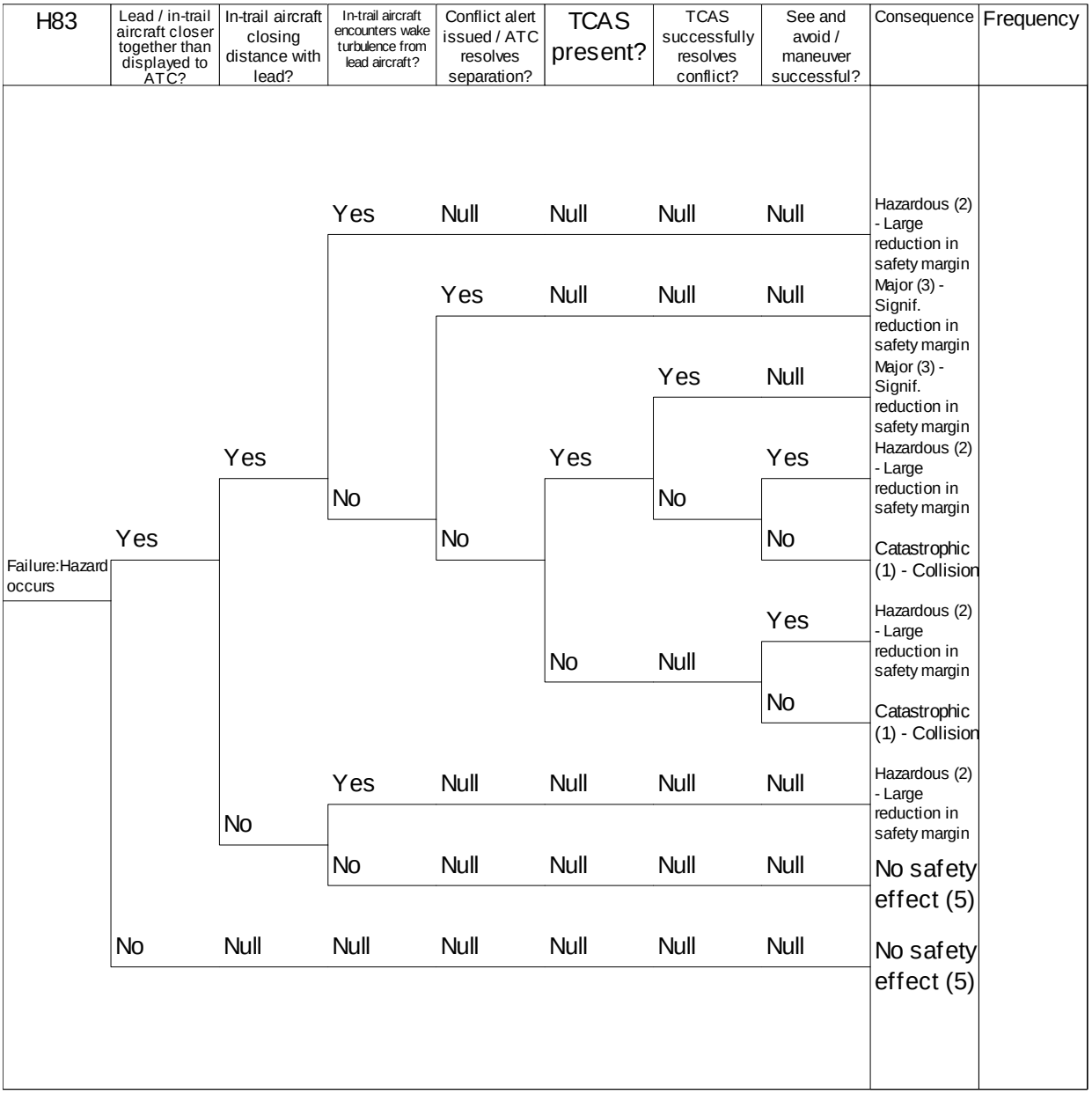


Figure 19: Event Tree for H83



B.2 In-Cockpit Applications

B.2.1 General

Figure 20: Fault Tree for H81

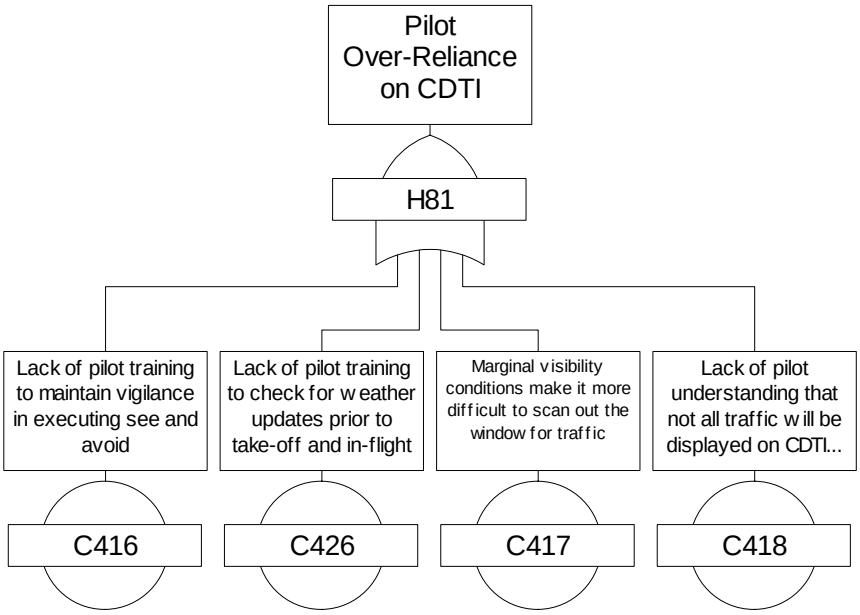
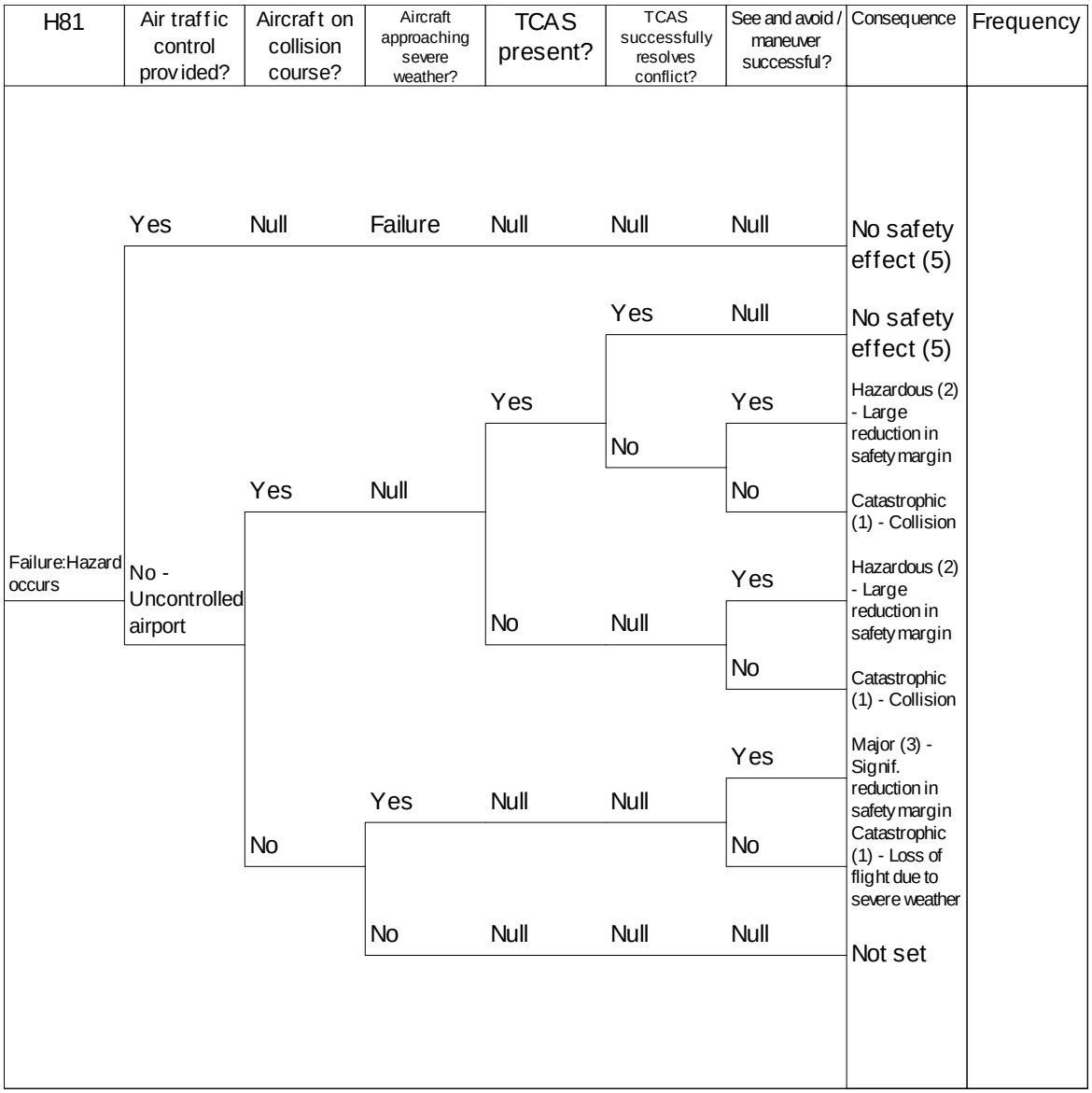


Figure 21: Event Tree for H81



B.2.2 Enhanced Visual Acquisition and Approach

Note: Fault trees are not presented for the enhanced visual acquisition or approach applications, because causes for each hazard are combined by "OR" gates.

Figure 22: Event Tree for H19

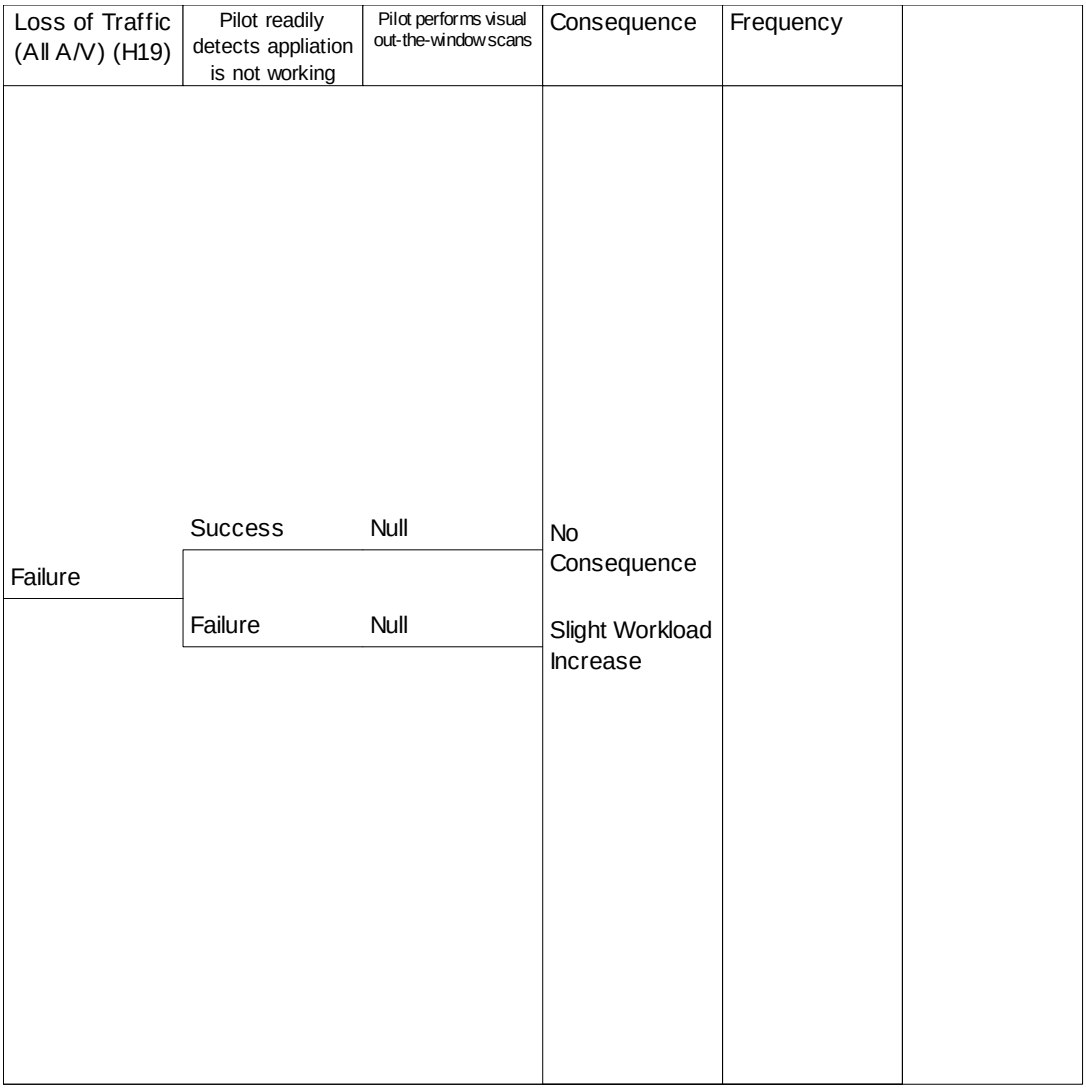


Figure 23: Event Tree for H44

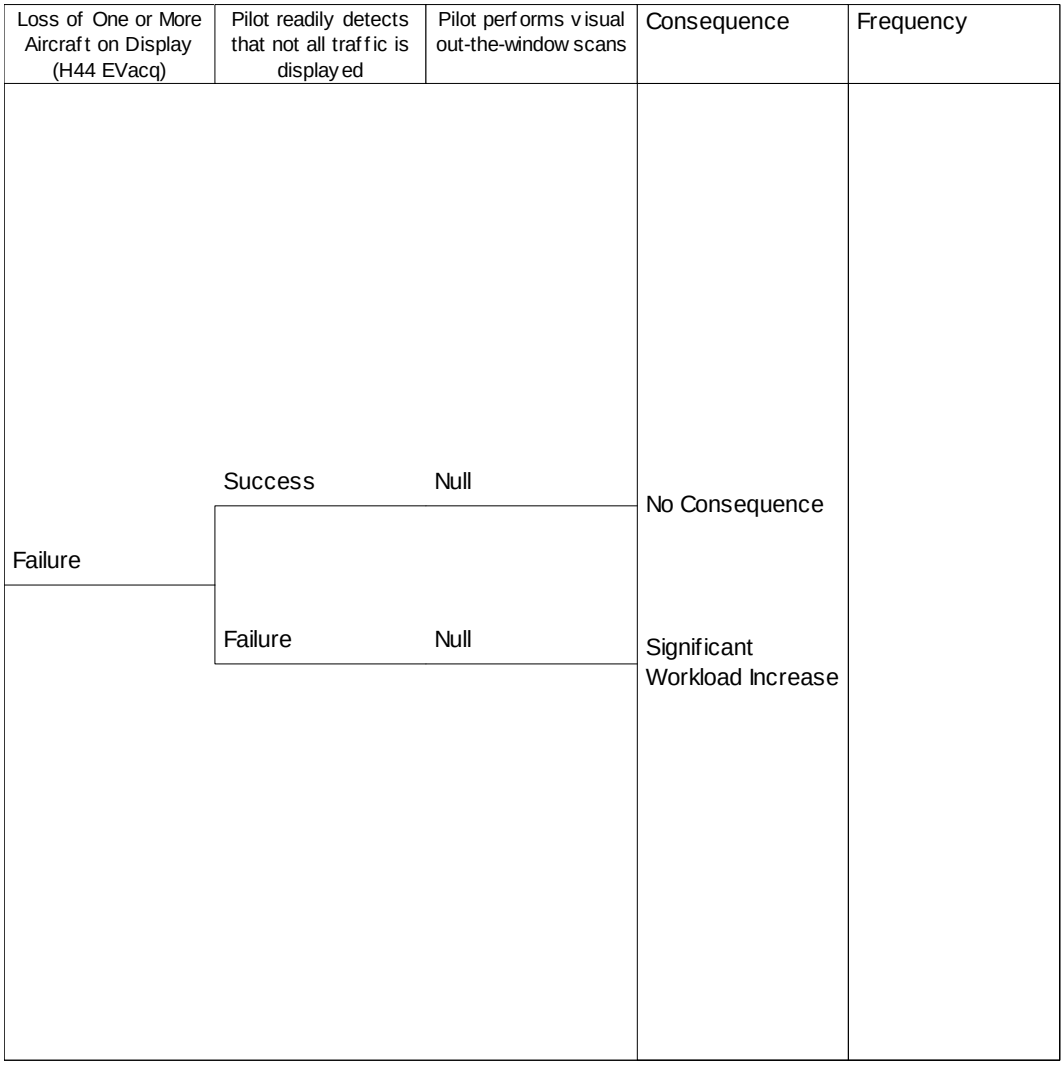


Figure 24: Event Tree for H22

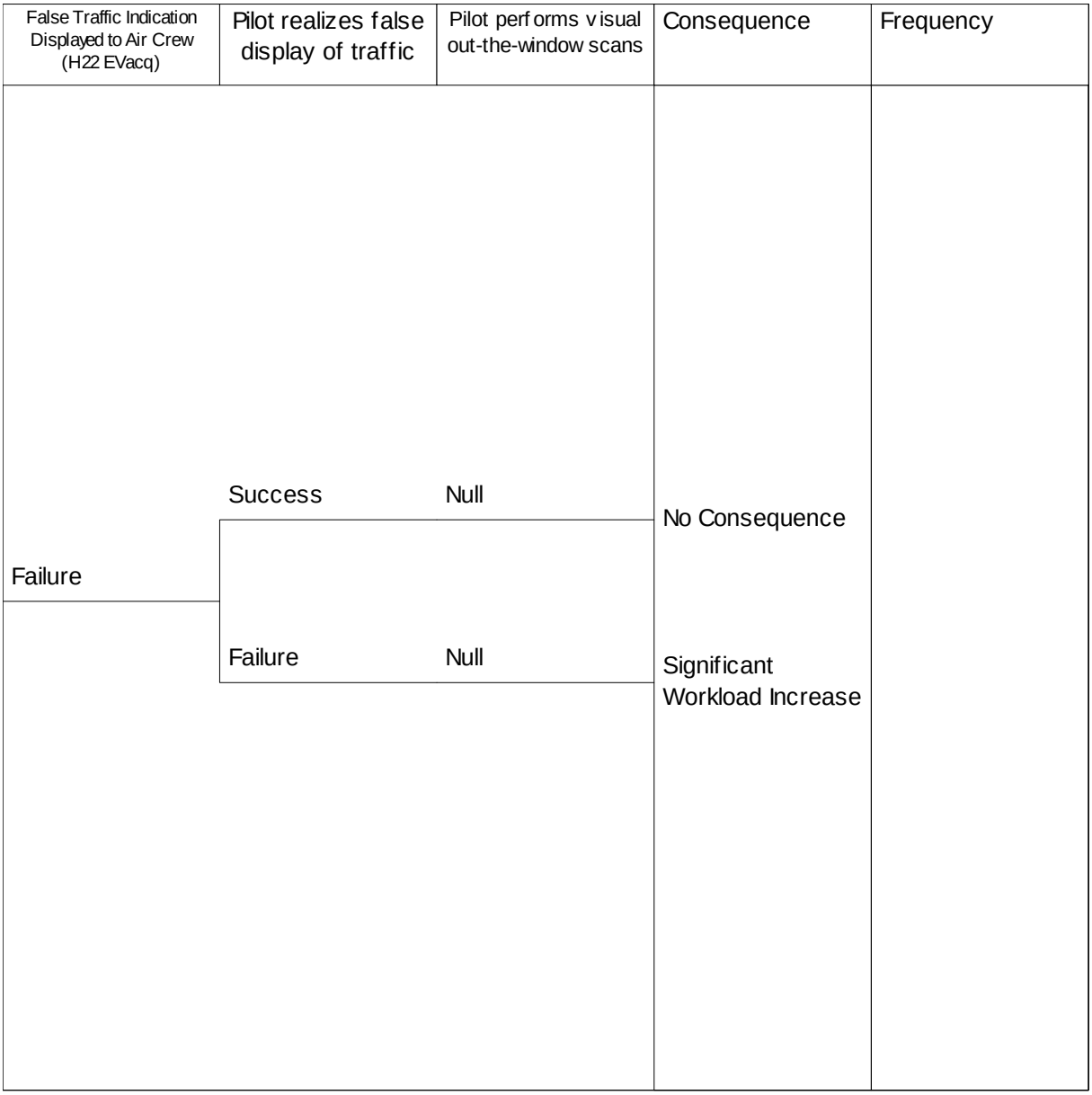


Figure 25: Event Tree for H23

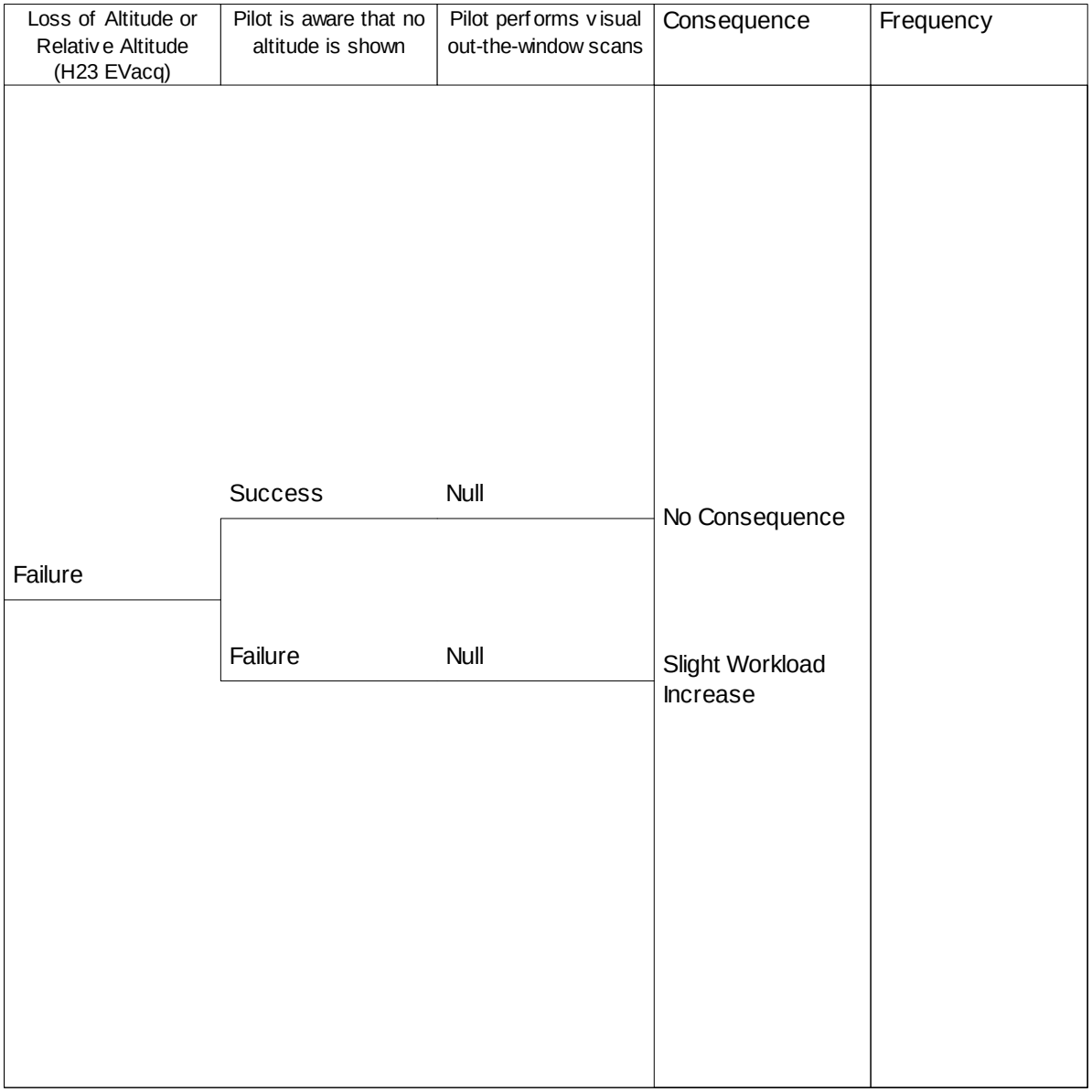
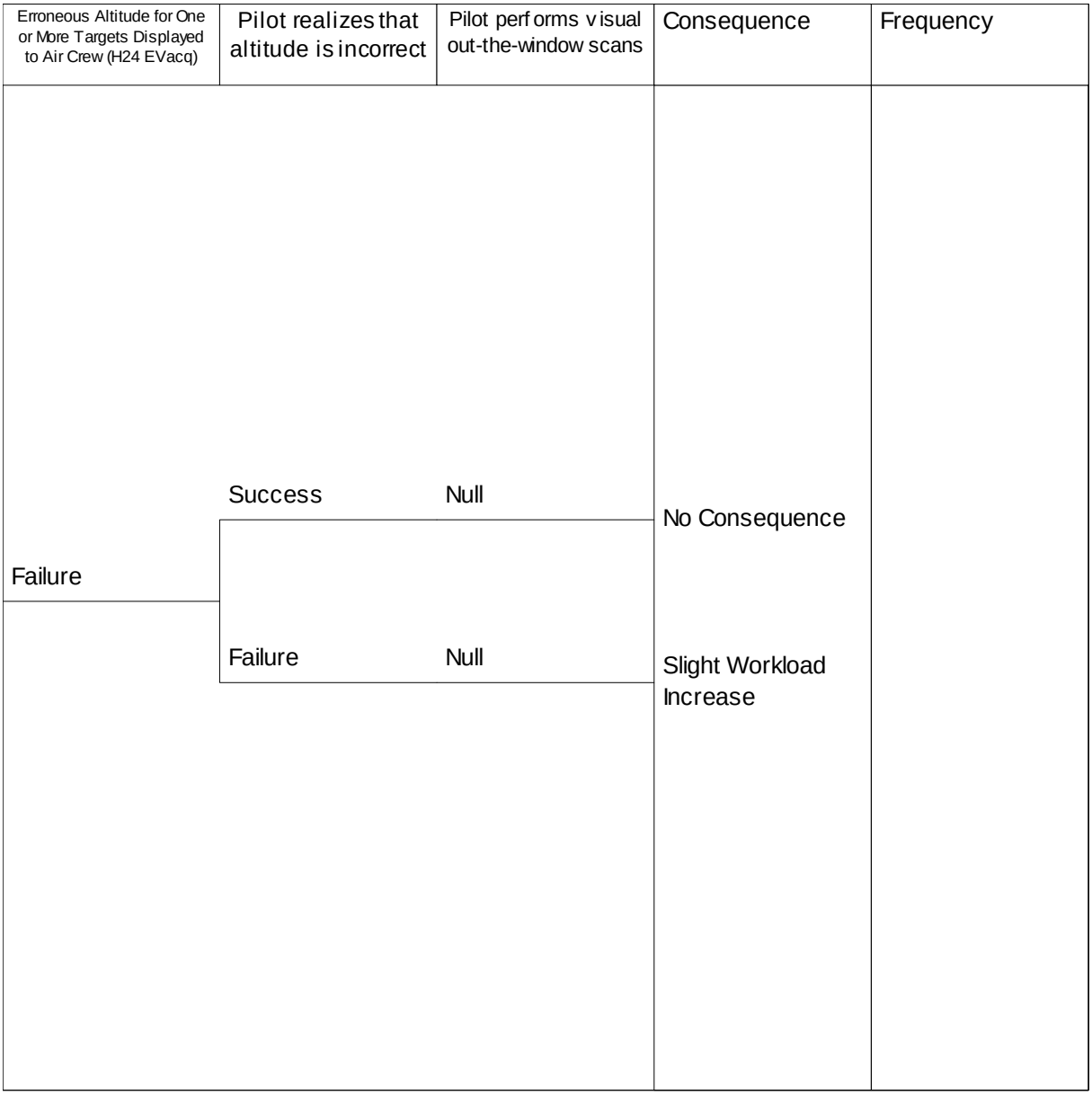


Figure 26: Event Tree for H24



B.2.3 Final Approach and Runway Occupancy Awareness (FAROA) and Airport Surface Situational Awareness (ASSA)

Figure 27: Fault Tree for H32 and H22

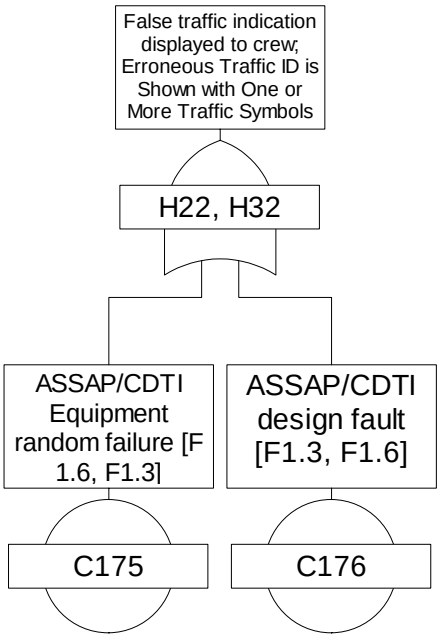


Figure 28: Fault Tree for H43

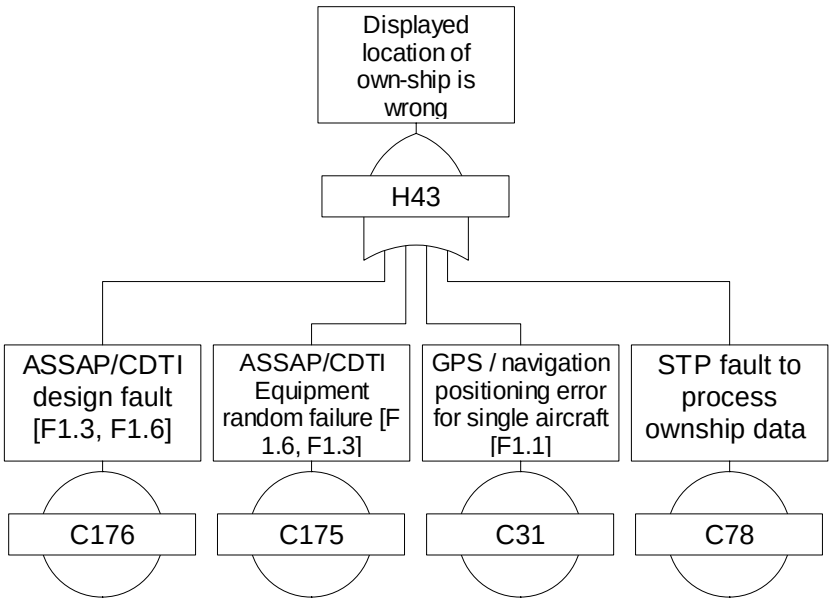


Figure 29: Fault Tree for H44

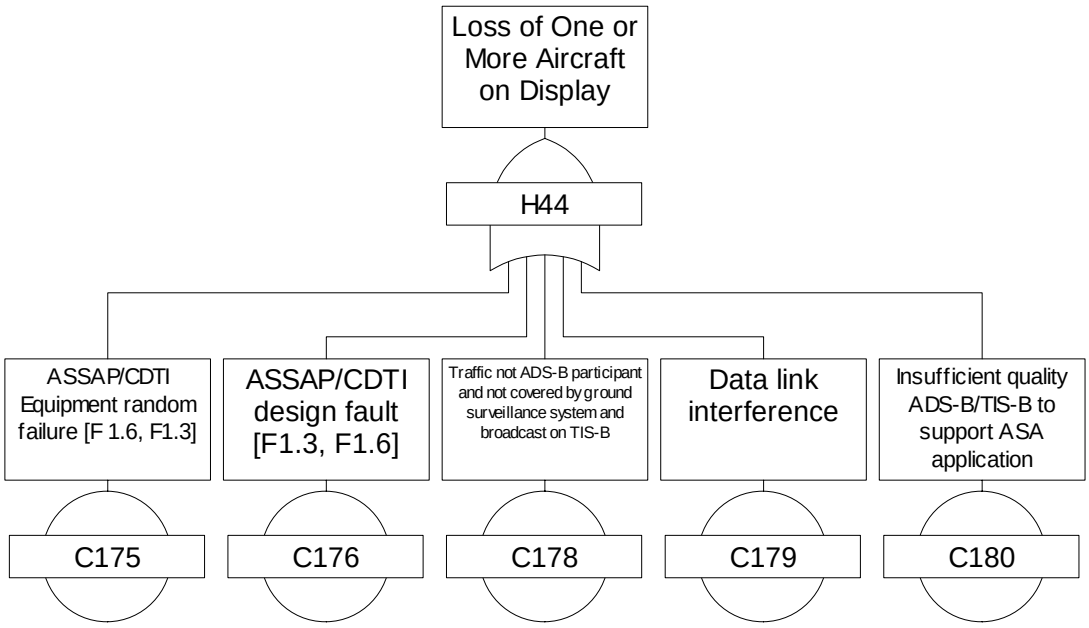


Figure 30: Fault Tree for H45

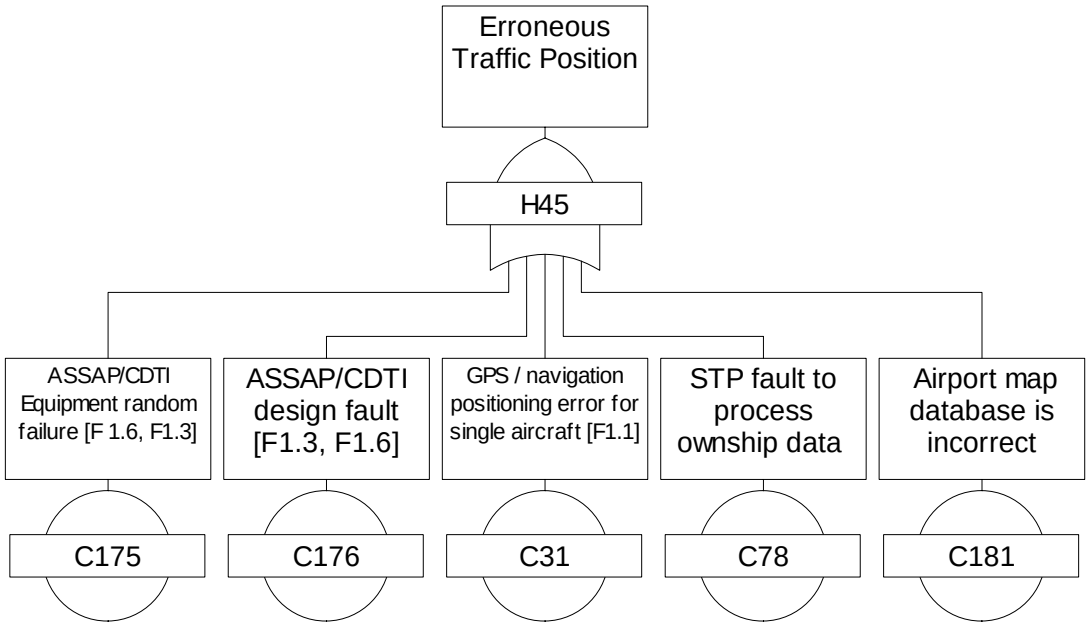


Figure 31: Event Tree for H45 (FAROA Only)

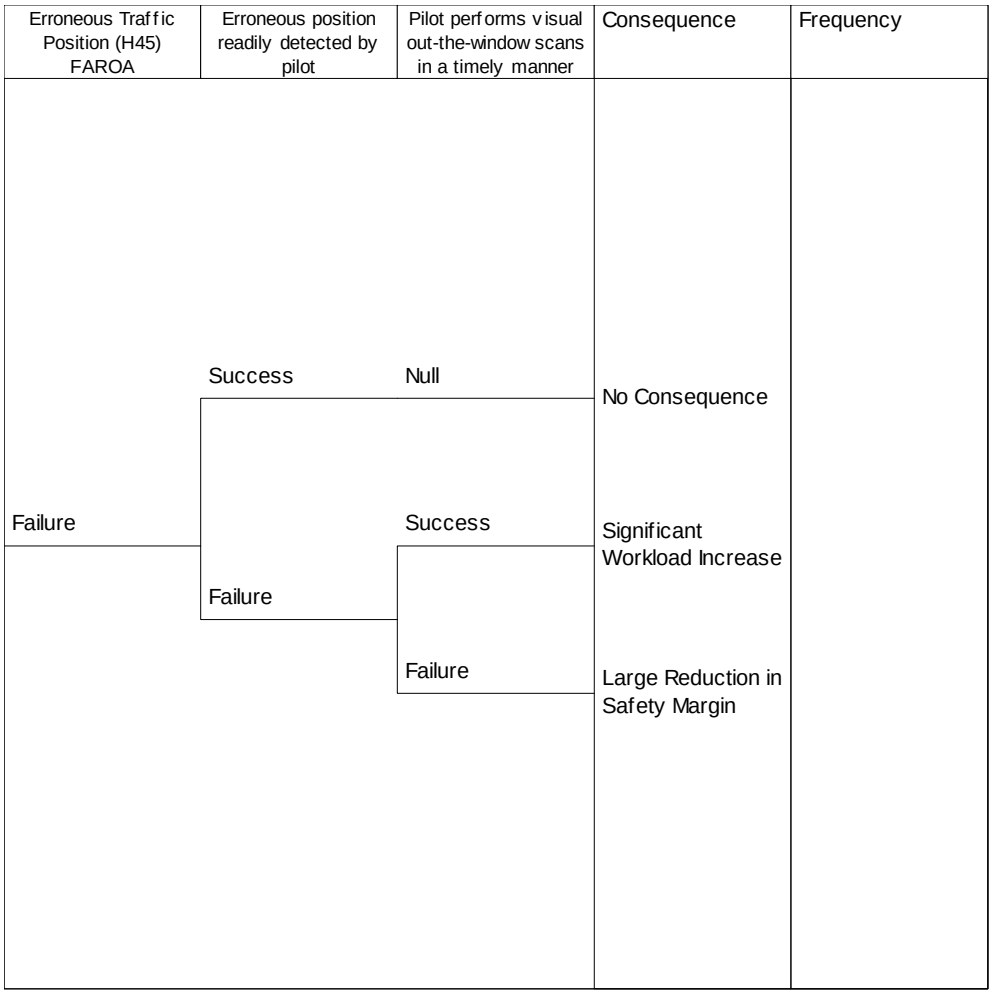


Figure 32: Fault Tree for H48

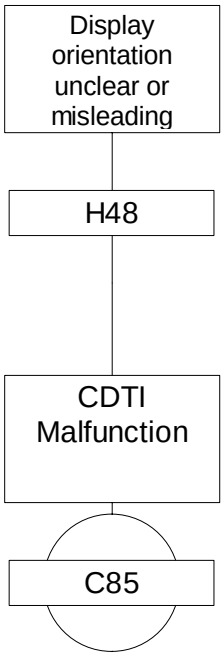


Figure 33: Event Tree for H42, H43, H44, H45 (ASSA Only), H48, and H32

<table>
<tr><td>H42, H43, H44, H45, H48, H32,</td><td>Cross-check maps, ATC</td><td>Consequence</td><td>Frequency</td></tr>
<tr><td>Failure</td><td>Normal surface procedures</td><td rowspan="2">Increase in workload</td><td rowspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
</table>

Figure 34: Event Tree for H22 (ASSA), H34, H39, H41, H44, and H47

<table>
<tr><td>H22, H34, H39, H41, H44, H47</td><td>Cross-check maps, ATC, visual situation</td><td>Consequence</td><td>Frequency</td></tr>
<tr><td rowspan="2">Failure</td><td>Normal surface or landing procedures</td><td rowspan="2">Slight Increase in workload</td><td rowspan="2"></td></tr>
<tr><td></td></tr>
</table>

B.2.4 Conflict Detection

Figure 35: Fault Tree for H49 and H50

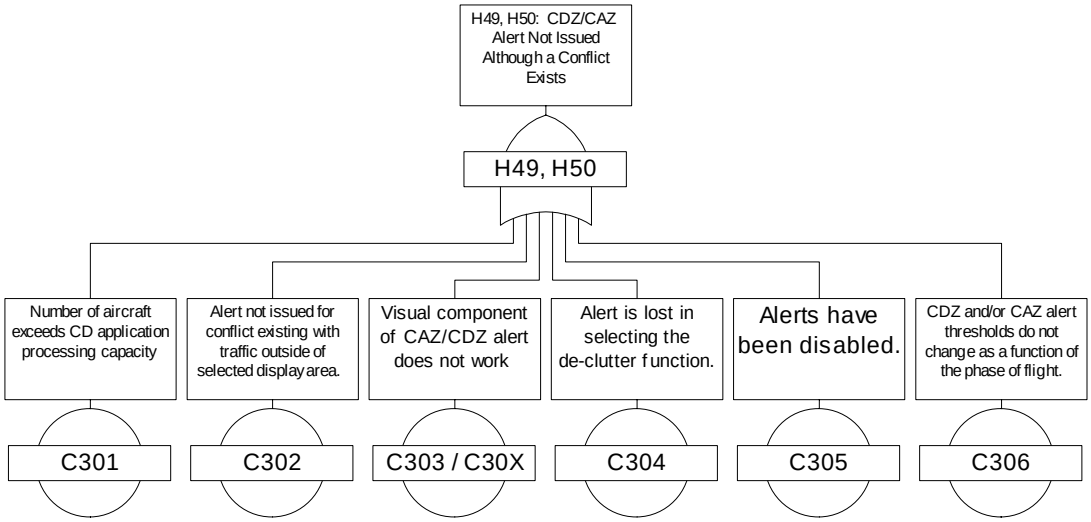


Figure 36: Fault Tree for H51 and H50

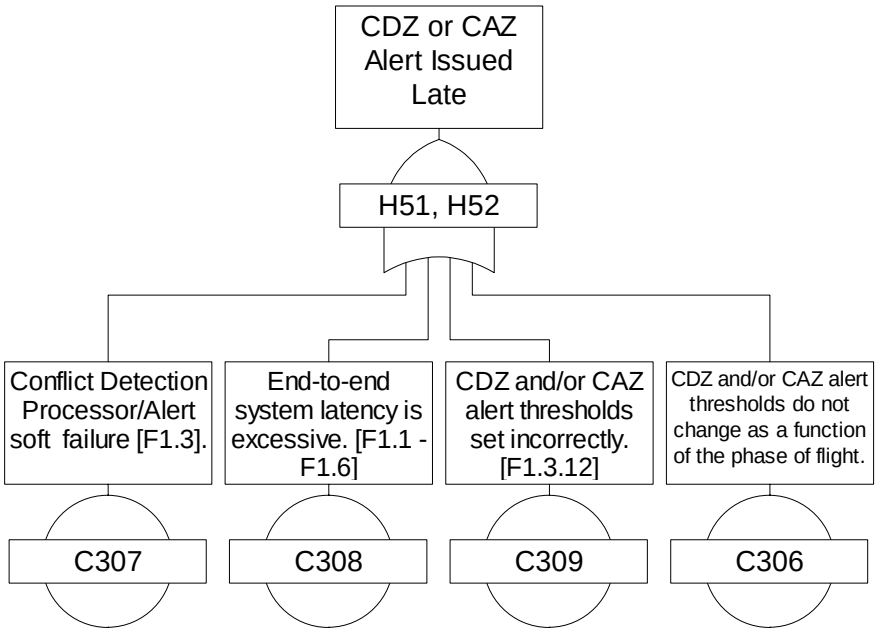


Figure 37: Event Tree for H51 and H52

H51, H52 CDZ or CAZ alert issued late	See and avoid procedures	Consequence	Frequency
Failure	Invoked	Slight Increase in workload (Pilot may scan for another conflict)	

Figure 38: Fault Tree for H55 and H56

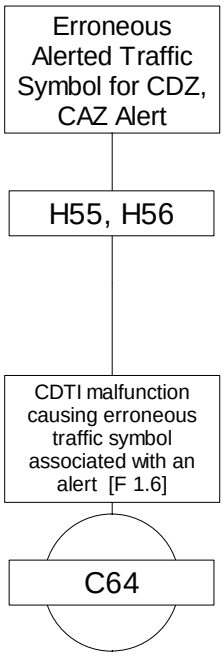


Figure 39: Event Tree for H55 and H56

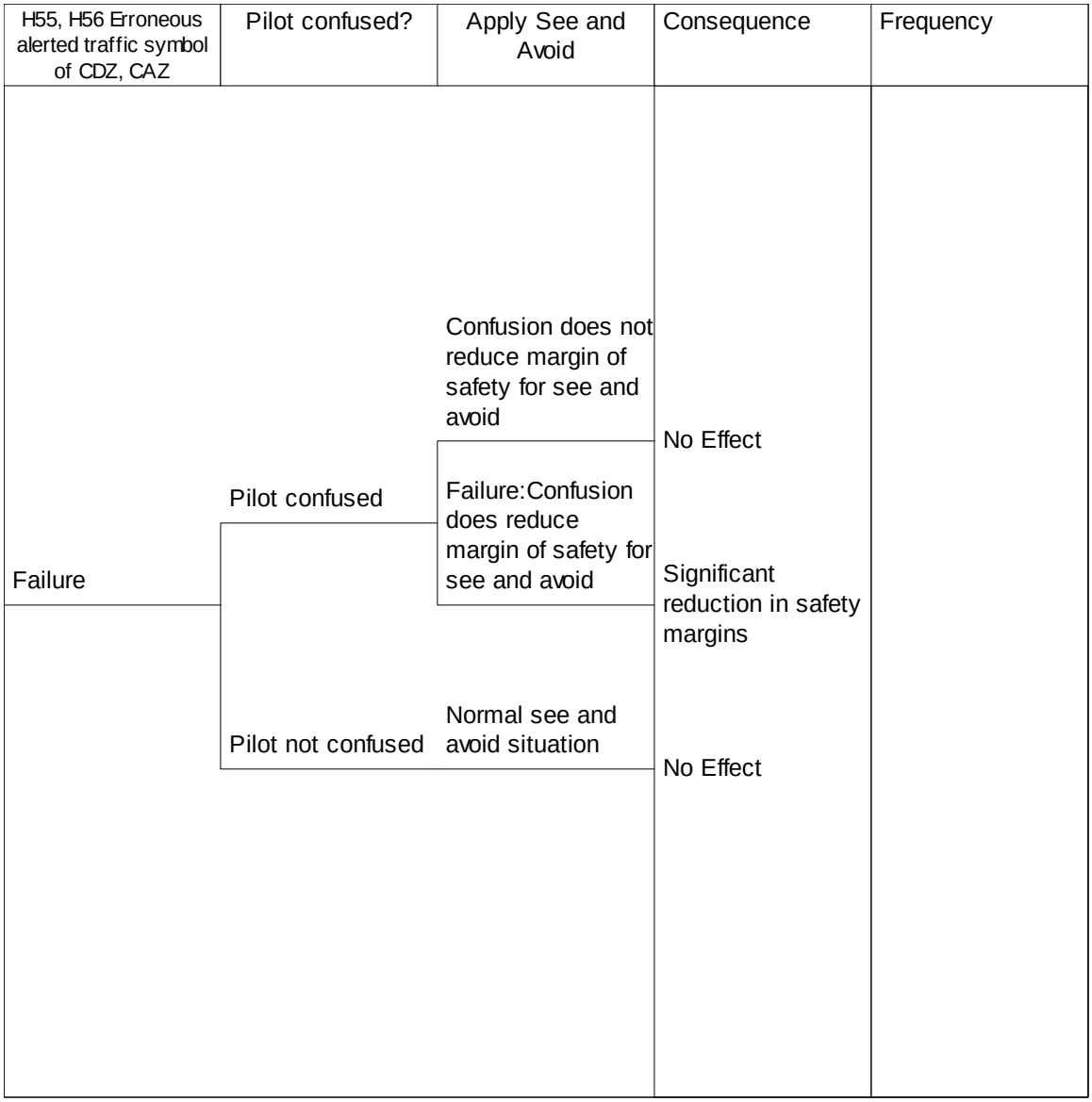


Figure 40: Fault Tree for H53 and H54

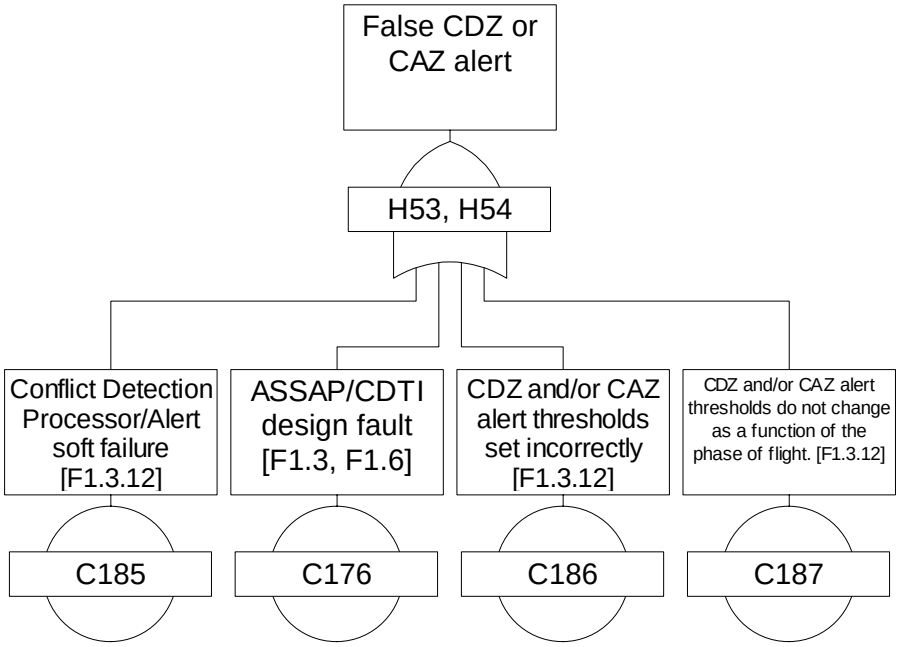


Figure 41: Event Tree for H53 and H54

H53, H54 False CDZ or CAZ alert	Pilot detects alarm is false	Consequence	Frequency
Failure:false alarm	Success	Slight Increase in workload	
	Failure	Slight Increase in workload	

Figure 42: Fault Tree for H57

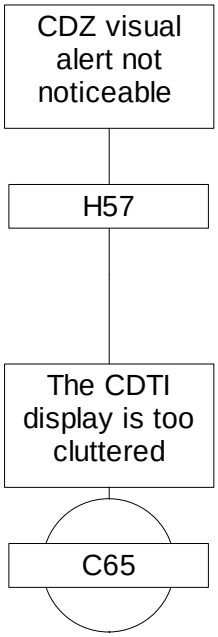


Figure 43: Event Tree for H57

H57: CDZ visual alert not noticeable	See and Avoid Procedures	Consequence	Frequency
Failure	invoked	No Effect	

Figure 44: Event Tree for H58

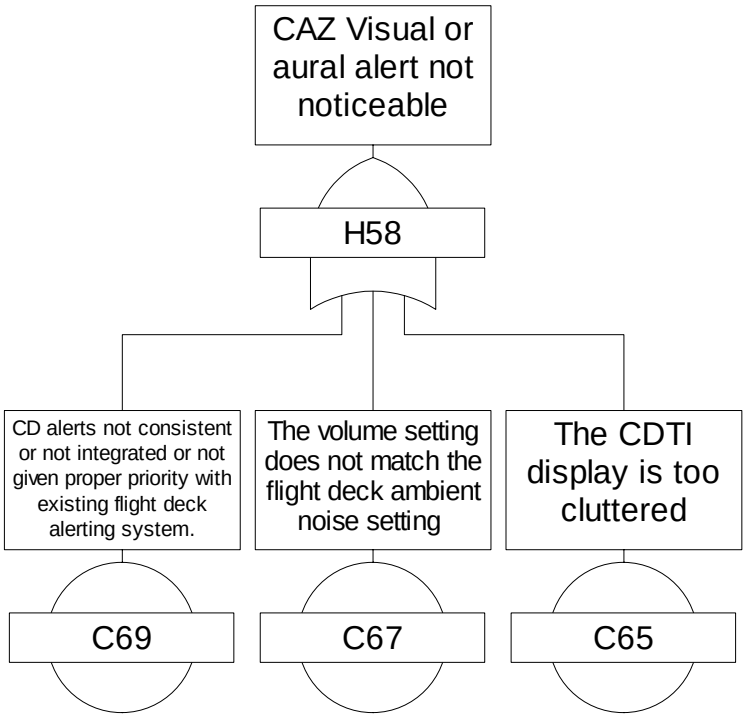


Figure 45: Event Tree for H58

H58: CAZ Visual or aural alert not noticeable	See and avoid procedures	Consequence	Frequency
Failure	invoked	No Effect	

Figure 46: Fault Tree for H60

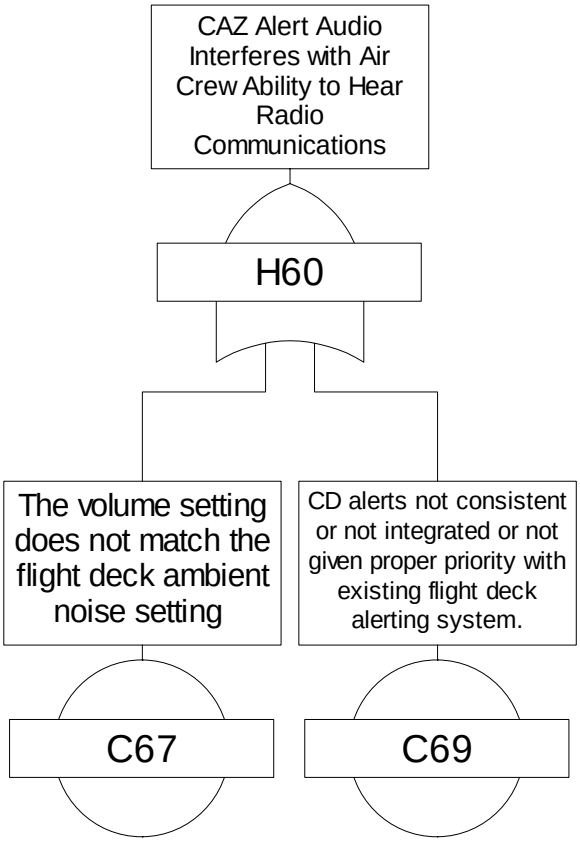


Figure 47: Event Tree for H60

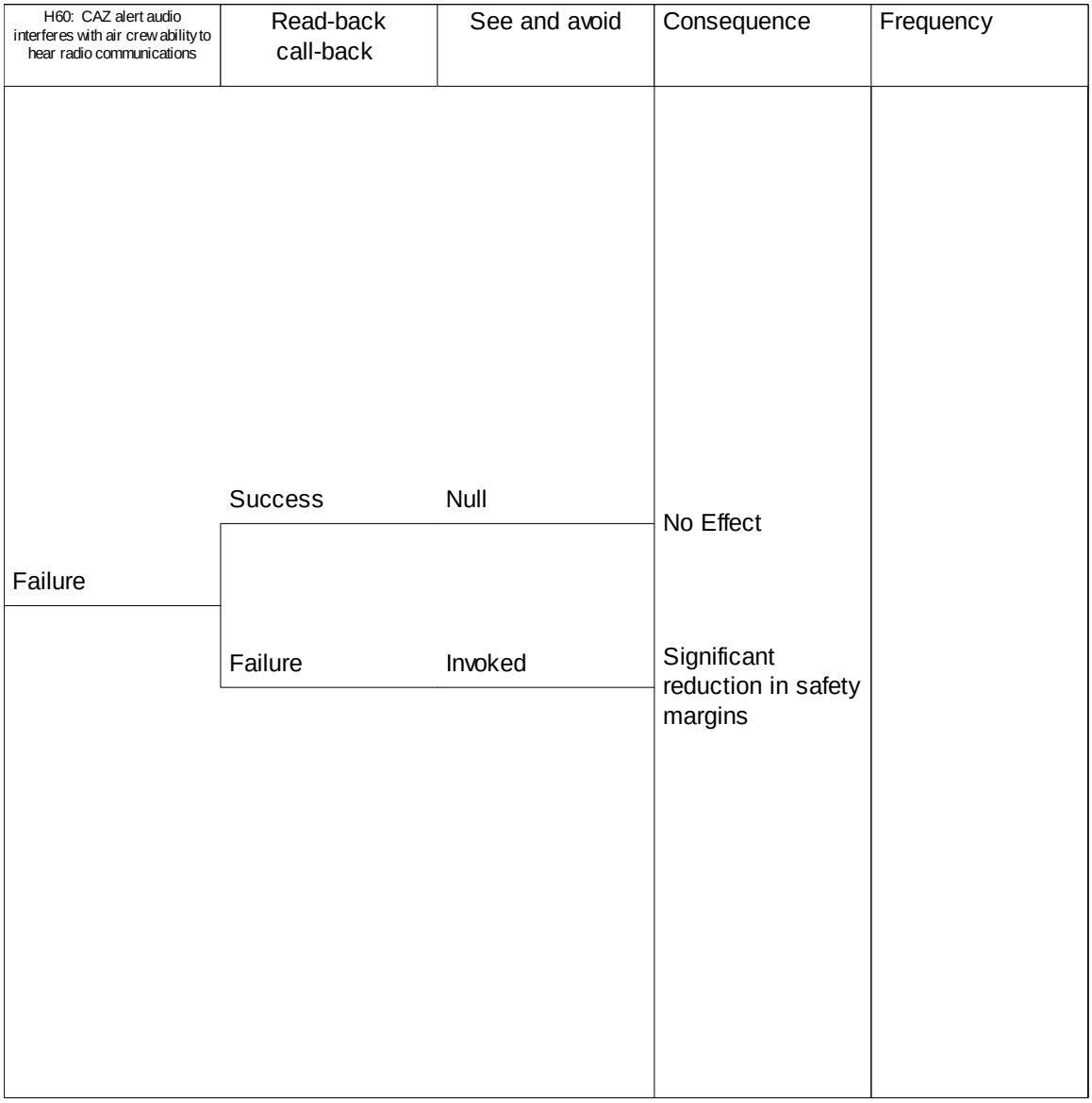


Figure 48: Fault Tree for H61

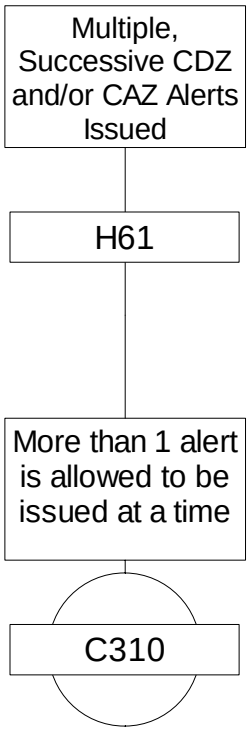


Figure 49: Event Tree for H61

Figure 50: Fault Tree for H61 – H65

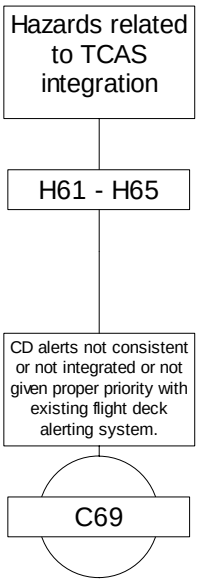


Figure 51: Event Tree for H61 – H65

Hazards related to TCAS integration		Consequence	Frequency
Failure	See and avoid procedures	Increase in workload	

B.2.5 Weather and NAS Status Situational Awareness

Note: Fault trees are not presented for the Weather and NAS Status Situational Awareness application, because causes for each hazard are combined by "OR" gates.