Report No. 0411-03

CAPSTONE PHASE II
RNAV Operations

Draft

Capstone Phase II RNAV Preliminary Hazard Analysis Status Report

April 11, 2003

Status Report: Capstone Phase II RNAV Preliminary Hazard Analysis

Draft

April 7, 2003

Prepared For: Federal Aviation Administration
Alaskan Region
Capstone Program Office
1250 Maryland Avenue, SW
Washington, DC 20024

Prepared By:

James Cieplak	Capstone Program Office/MITRE
Michael Allocco	FAA Office of System Safety, (ASY-300)
Robert Thornburgh	Adsystech, Inc.
	1250 Maryland Avenue, SW
	Washington, DC 20024

TABLE OF CONTENTS

Status Report: Capstone Phase II RNAV Operations in Southeast Alaska Preliminary Hazard Analysis

1.0 Summary

This Capstone Phase II RNAV Preliminary Hazard Analysis (PHA Phase II) Status Report was developed based upon an expansion of the Capstone Preliminary Hazard Analysis (PHA) Phase I Core Bethel completed 2 January, 2000. The PHA Phase I analysis, contained in Volume 1 Capstone Safety Engineering Report #1: ADS-B Radar-Like Services, produced controls and mitigations to eliminate or reduce the risks associated with identified hazards in the Core Bethel area. The controls and mitigations were turned into Candidate Safety Requirements/Recommendations statements for possible inclusion in an initial requirements document (IRD). The requirements covered the end-to-end operation of the system in the Core Bethel area and may therefore impact the manufacturers of the on-board avionics, the operators of the aircraft or vehicle, the services to be supplied by the NAS, the builders of the ground system, and the applications user community.

The PHA Phase II RNAV Operations in Southeast Alaska (PHA Phase II) expanded on the PHA Phase I Core Bethel and generated additional hazard descriptions. A hazard description shows the sequential events which must occur to culminate in an undesired outcome (harm). The harm (accident) is a combination of system state and causes in a sequence of events that result in a postulated harm.

The expanded PHA Phase II tabular-formatted Hazard Description Worksheets are contained in Volume II of the Capstone Phase II RNAV Operations in Southeast Alaska Design Analysis Report: Preliminary Hazard Analysis. The PHA Phase II is being conducted using the FAA System Safety Management Program, dated 1 January 2001 and the methodology defined in the FAA System Safety Handbook, dated 30 December, 2000. The Phase II hazard descriptions include new hazard descriptions based primarily on RNAV operations in the Juneau/Southeast Alaska environment with potential Capstone and legacy equipage combinations within the National Airspace System (NAS). The equipage combinations are derived from equipment assumed to be operational through the year 2015.

The output of the PHA Phase II will be used in: (1) further developing safety requirements to be added to the Safety Requirements Verification Table (SRVT), (2) preparing performance/design specifications, and (3) initiating the hazard tracking and risk resolution process for the Capstone Phase II system. The PHA Phase II currently produced a total of 151 Controls. Twenty-six (26) of the Controls were identified as Existing Requirements. The remaining one hundred twenty-five (125) Controls were identified as Recommended. Existing requirements are those that can be referenced in current program documentation, i.e., Military Specifications, FAA Orders and other governmental regulations, and consensus standards. Recommended Controls are those mitigation methods that are not referenced in current program documentation and are therefore, recommended. The Controls are written as high-level statements that are postulated to either eliminate or mitigate hazardous outcomes as identified in the analysis. By the conclusion of the PHA Phase II process it is anticipated additional hazard descriptions and safety requirements will be generated. It is important to note that the CAPIISSWG will evaluate the Controls and refine them into Recommended Safety Requirements.

The PHA Phase II initial findings from the ongoing analysis are summarized as follows:

- Recommendations relating to alternate, independent means of validating the ADS-B provided information, such as call sign, ID, position, velocity, and altitude. These are generally requirements on the NAS to continue to provide current surveillance and communications systems until sufficient confidence is established in the reliability and availability of ADS-B. This approach is consistent with current ADS-B plans for a transition period in which ADS-B will be operated in parallel with existing systems.
- Design and implementation requirements to identify and eliminate or mitigate hazardous misleading information generation and/or display from both the avionics and ground systems.
- Requirements that cite existing FAA or industry specifications or standards.
- Requirements to design system to meet applicable availability, maintainability, and reliability requirements from SR-1000 and SS-1000.
- Requirements to design system to prevent single-point failures or common-cause failures that can result in catastrophic or hazardous events.
- Recommendations for studies to determine human factors design requirements using pilots and controllers to determine the safest implementation of the system.
- Laboratory simulations, flight tests, and operational evaluations are included.
- Requirements for compatibility and integration of information from a wide range of input sources/types expected to be in use through the year 2015.
- Requirements for training associated with safety related to the new RNAV operations, avionics suites, tower displays, maintenance, or operation.
- Requirements to prevent interface malfunctions between existing and legacy systems and Capstone Phase II air and ground systems resulting in loss of capabilities.
- Requirements to prevent system/subsystem malfunctions from propagating to other systems/subsystems or communications/avionics equipment.
- Requirements to prevent communication delays or losses as a result of less than adequate mixed equipage procedural integration.
- Requirements to identify and eliminate or mitigate safety related hazards and integration associated with WAAS and GPS data information.
- Requirements to review existing contingency procedures and modify and/or develop new procedures as needed for the integration of Capstone Phase II technology.

A Design Analysis Report (DAR) will be produced at the end of the PHA process. The DAR will only list the hazard descriptions from each grouping of related hazards which represent the worst-credible harm. Hazard descriptions will not be shown which represent lesser harm for similar hazards and which do not generate any additional requirements.

In the DAR the high hazards will be ranked relative to all of the worst-credible hazards identified. All identified high, medium, and low hazards will be placed into a Hazard Tracking System (HTS). Only the high and medium hazards will be tracked to closure. The HTS will allow each hazard to be tracked throughout system lifecycle activities. As the system matures through design and build activities additional existing and recommended safety requirements may be identified which may impact a hazards ranking.

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

Although this analysis is being performed based on the current state of knowledge of the Capstone Phase II system, a full system design has not yet been generated: therefore, all hazards may not have been identified. In order to assure a successful System Safety Program, follow-on safety reviews must be conducted. Review and update of the hazard analysis, hazard description by hazard description, is required.

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

2.0 Purpose

2.1 Purpose of Analysis

This Capstone Phase II PHA is being conducted to identify hazard descriptions that are associated with Capstone providing ADS-B radar-like services in newly defined RNAV operations. These hazard descriptions are being defined with associated effects and risk defined by both severity and likelihood. These hazard descriptions are being identified in order to develop hazard controls (i.e., existing requirements and recommended safety requirements as identified in the DAR) that have been incorporated into high-level Capstone safety requirements. The End-to-End Safety Review involves an ongoing review of the PHA for concurrence and acceptance of residual risks, by the CIISSWG and Capstone program management.

A secondary objective of conducting this PHA is to comply with the policy requirements that are currently being included in the FAA's Order 8040.4 Safety Risk Assessment and to demonstrate "best practices" in safety engineering. The PHA is an initial activity associated with conventional system safety activities.

2.2 Purpose of this Report

This Capstone Phase II Status Report #1 documents the current findings of the ongoing Phase II PHA for Area Navigation Services utilizing ADS-B radar-like services. A safety baseline is being established and criteria defined in order to conduct this analysis and are presented in this report. The Phase II PHA was initiated in February 2002 to support the Capstone Program in defining the process to successfully conduct an End-to-End Safety Review.

3.0 Background

3.1 Capstone Phase II Program

The Capstone Program is sponsored by the FAA's Alaskan Region in cooperation with the FAA Safe Flight 21 Program. The Capstone Program accelerates nationwide efforts to improve aviation safety and efficiency through a multi-year introduction of current and emerging concepts and technologies. Initial validation plans include the installation of government-furnished Global Positioning System (GPS) driven avionics suites in up to 200 commercial aircraft serving the areas in and around Juneau, Alaska.

The principal objective of this Phase II initiative is to develop the RNAV infrastructure with satellite navigation as the only radio navigation equipment required onboard the aircraft to meet aviation radio navigation performance requirements. These requirements are for oceanic, remote area and domestic en route, terminal, non-precision approach, and precision approach phases of flight. In doing so, Capstone seeks to obtain the required accuracy improvement for precision approaches, as well as integrity, continuity, and availability of navigation for all phases of flight. Activities will initially center on and between Juneau, Haines, Hoonah and Gustavus airports. Activities supporting this objective include establishing or amending air routes to achieve lower minimum enroute altitudes using RNAV, filling communication gaps and providing more terminal weather observations. Automatic Dependent Surveillance-Broadcast (ADS-B) avionics will be provided for see-and-avoid and a limited ADS-B ground infrastructure will be installed to support flight following by the aircraft operators/operations centers and AFSS.

3.1.1 Capstone Phase II System Safety Program Plan

The Capstone System Safety Program Plan defines the system safety-related tasks and activities conducted within the Capstone Program. This plan document is titled Capstone Phase II System Safety Program Plan for RNAV Operations in Southeast Alaska. The Phase II SSPP was signed by the Alaska Region Administrator and is dated 19 February 2003.

4 Capstone Phase II RNAV Services

The principal objective of this initiative is to develop the RNAV infrastructure with satellite navigation as the only radio navigation equipment required onboard the aircraft to meet aviation radio navigation performance requirements. These requirements are for oceanic, remote area and domestic en route, terminal, non-precision approach, and precision approach phases of flight. In doing so, Capstone seeks to obtain the required accuracy improvement for precision approaches, as well as integrity, continuity, and availability of navigation for all phases of flight. Activities will initially center on and between Juneau, Haines, Hoonah and Gustavus airports.
Activities supporting this objective include establishing or amending air routes to achieve lower minimum enroute altitudes using RNAV, filling communication gaps and providing more terminal weather observations. Automatic Dependent Surveillance-Broadcast (ADS-B) avionics will be provided for see-and-avoid and a limited ADS-B ground infrastructure will be installed to support flight following by the aircraft operators/operations centers and AFSS.

4.1 Overview

This initiative makes use of GPS/WAAS as the sole means of navigation from departure, throughout en route to approach and arrival at the distant airport. This navigation will be supplemented by a terrain avoidance warning system (TAWS) as well as electronic airport maps for each airport surface. This application makes use of current Terminal Instrument Procedures Standards (TERPS) … (Note this is not intended to limit the use of satellite navigation for reduced TERPS standards.) An example of this application would be development of a departure-approach pair from Juneau to Hoonah. Aircraft would depart Juneau and follow low altitude routes while avoiding unnecessary climbs to clear terrain or to stay within the service volumes of traditional navigation aids. These procedures have the added advantage of allowing aircraft to fly below adverse weather and perhaps avoid weather obscurations as well. RNAV will allow the use of a new instrument approach at Hoonah.

The United States Standard for Terminal Instrument Procedures (TERPS) is the approved criteria for formulating instrument approach procedures. RNAV minimums are dependent on navigation equipment capability, as stated in the applicable Aircraft Flight Manual (AFM) or AFM Supplement and as outlined below:

- GLS (Global Navigation System (GNSS) Landing System): Must have WAAS (Wide Area Augmentation System) equipment approved for precise approach.
- LNAV/VNAV (lateral Navigation/Vertical Navigation): Must have WAAS equipment approved for precision approach.
- LNAV (Lateral Navigation): Must have IFR approach approved WAAS or GPS.

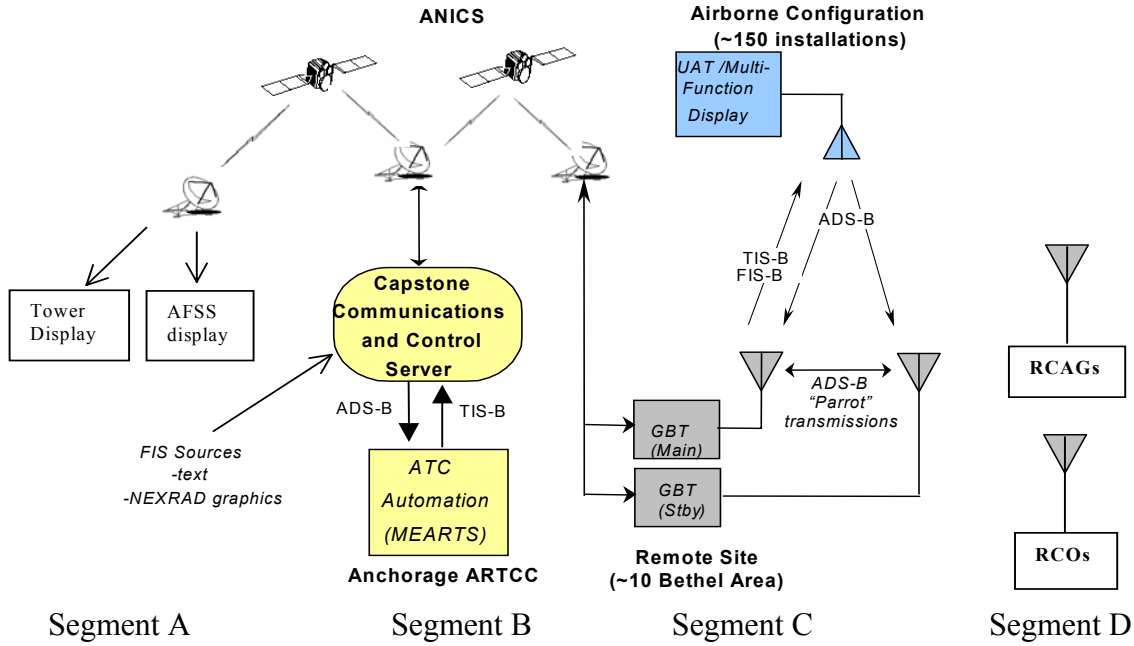


Figure 4.1. Phase II Capstone System Block Diagram

5.0 Approach and Methodology

The Phase II PHA is based on the guidance provided in the System Safety Management Program and FAA System Safety Handbook. Given knowledge of the ADS-B, WAAS, and GPS concepts of operations, and postulated RNAV operations, potential hazards (accidents) are being hypothesized. The team identifies the potential system accidents/incidents should failures, malfunctions, or human errors occur. The analysis is conducted using a tabular format as shown in Figure 5-1.

Scen # (1)	Hazard Description (2)	Causes (3)	Subsequent Causes (4)	Phase of Flight (5)	Possible Effect (6)	Risk (7)	Recommendations Safety Requirements (8)
	Fixation, confusion, and loss of situational awareness occur due to participating aircraft are not equipped for intended use. Situation results in near accident/miss.	Aircraft are not equipped for intended use due to: LTA Human Factors consideration LTA design LTA analysis LTA procedures Oversight Omission LTA training Pilot/Aircrew attempt to utilize excessive data/information Fixation, confusion and loss of situational awareness occurs Aircraft on collision course	Initial loss of situational awareness occurs Pilot/Aircrew able to regain situational awareness Pilot/Aircrew able to avoid accident	IFR navigation within route structure	Near Accident/ Miss	3C	15. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with new route structure requirements, procedures, protocols, regulations, rules, codes, and standards related to upgrades, changes, and integration, within Capstone Phase 2 and implement controls to preclude such risks. 16. Develop Aircrew/ATC procedures to accommodate contingency situations associated with new route structure development. 17. (E) Provide training on operational uses of the Capstone equipment to include terrain avoidance, weather avoidance, contingencies, and other flight planning functions. 21. Continue to implement/establish/refine requirements for procedures, protocols, regulations, rules, codes, and standards associated with aircraft certification to preclude external hazards/risks associated with Capstone Phase 2. 23. Conduct controller/pilot workload assessments to evaluate the potential for informational overload associated with Capstone Phase 2 equipment and implement controls to preclude such risks. 24. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with human factors in the integration of Capstone Phase 2 and implement controls to preclude such risks. 25. Design, develop, and implement engineering and administrative controls to preclude overload associated with Capstone Phase 2 equipment and implement controls to preclude such risks. 52. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to ensure that participating aircraft are equipped for the intended application.

Figure 5-1 – Tabular Format for the Phase IIPHA

The first column is the hazard-specific number. A description of the hazard is in the 2rd column. The initial Causes are in Column 3 and subsequent causes in Column 4. The phase of flight is located in column 5 with the possible effect in column 6. The Risk Acceptance Code/Risk Rating is in Column 7. Safety Requirements are identified in Column 8. In addition, all hazard sequences are assumed to occur under adverse conditions (the system state) that are described in the assumptions section below.

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

The analysis team is attempting to be as inclusive as possible in the identification of a potential system accident based on system hazard descriptions. Factors considered are:

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

Assumptions:

- As identified in Safeflight 21

The System State part of the hazard model used in this PHA analysis is based on "worst credible" conditions. Worst credible conditions, for the sake of this analysis are defined as:

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

Limitations:

- This is not an all inclusive hazard analysis in that there are other hazard descriptions to be addressed that equate to the total lifecycle of the Capstone Phase II system as it will be integrated within the NAS.

5.1 Hazard Description Model

The SSMP provides guidance on the use of a hazard description to describe accidents that may cause harm, and therefore represent a hazardous situation. The Hazard Model is based on the premise that a harm (unwanted event or accident) is usually not the result of a single cause. There may be an initiating event, followed by various combinations of causes that lead to the possible effect or harm. The possible effects are defined as worst-credible potential harm.

The 5M model is used to develop the Capstone Phase II PHA. It is predicated on the concept that the total system comprises the Mission (i.e., what is the system trying to accomplish, as defined in the operational concept), the Machine (i.e., the system hardware and software), the Man (potential for human error in following rules and executing procedures), Media (the operational state of the system, as well as the physical environment such as fog, rain, wind, ice, snow, and other related weather phenomena), and Management (i.e., Rules, regulations, procedures such as FAA Order for Air Traffic Control 7110.65. For Capstone Phase II RNAV operations, the analysis considers the total end-to-end system, including hardware (systems and subsystems) and software failures, as well as the controller and the actions of the flight crew. As

the analysis considered legacy systems malfunctions that might give misleading or conflicting information, reliability and availability requirements are, in limited instances, imposed as safety requirements on them.

A Design Analysis Report (DAR) will be produced at the end of the PHA process. The DAR will only list the hazard descriptions from each grouping of related hazards which represent the worst-credible harm. Hazard descriptions will not be shown which represent lesser harm for similar hazards and which do not generate any additional requirements.

In the DAR the high hazards will be ranked relative to all of the worst-credible hazards identified. All identified high, medium, and low hazards will be placed into a Hazard Tracking System (HTS). Only the high and medium hazards will be tracked to closure. The HTS will allow each hazard to be tracked throughout system lifecycle activities. As the system matures through design and build activities additional existing and recommended safety requirements may be identified which may impact a hazards ranking.

5.2 Risk Determination

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

The Capstone Phase II RNAV PHA uses the criteria contained in the SSMP for both severity and likelihood of occurrence. These are shown in Figures 5-2 and 5-3.

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

Table 5-2 - Severity of Consequence Criteria

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

Table 5-3 - Likelihood of Occurrence Criteria

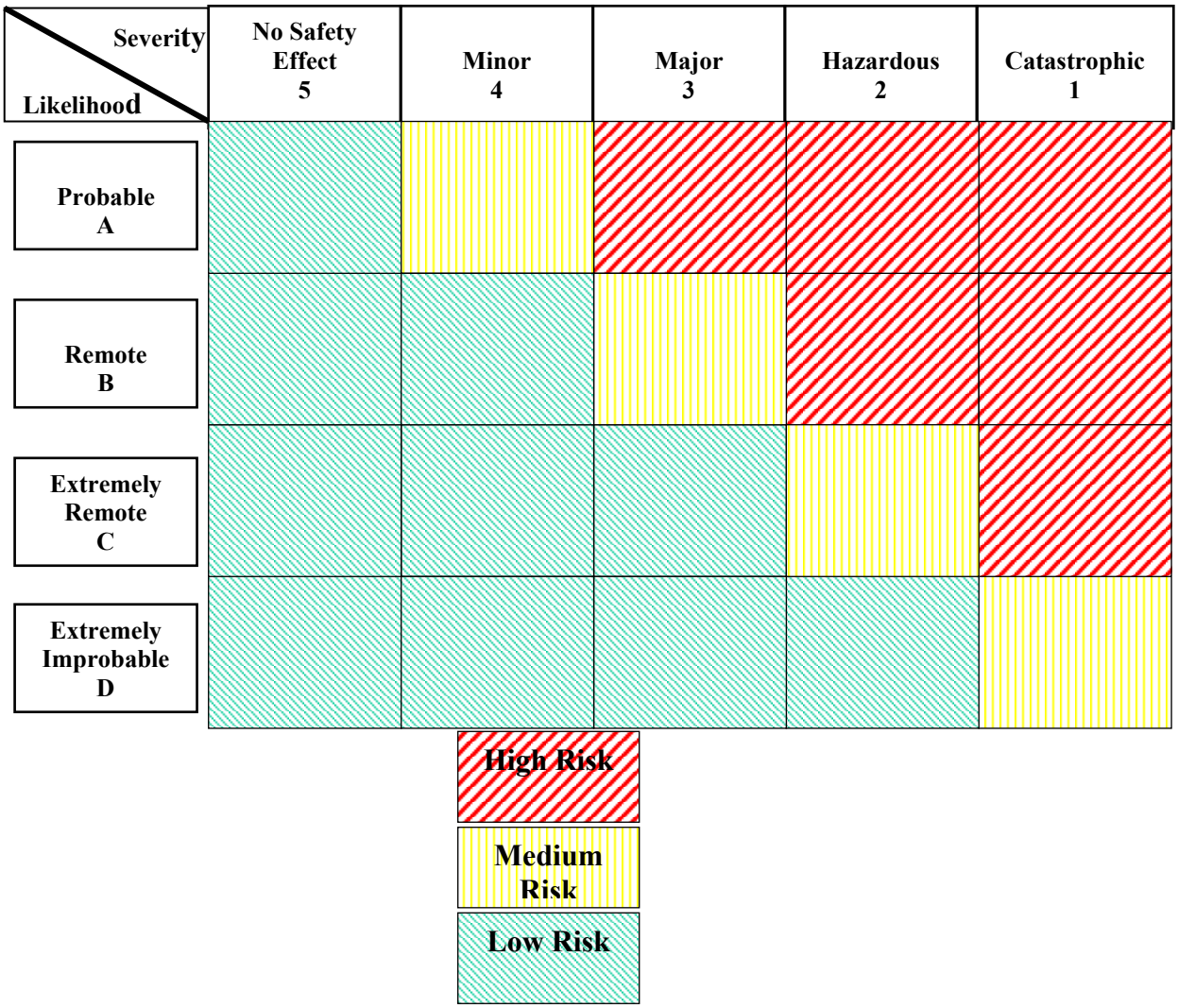


Table 5-4 – Risk Assessment Code (Risk)

Table 5-4 shows the criteria for risk acceptability. A high risk may be considered acceptable by the FAA, but in most cases all efforts must be made to mitigate or control the risk to a lower category. Medium and low risk acceptability is also defined in the figure.

The risk is then determined from the Risk Assessment Matrix shown in Table 5-4. Severity is shown in the top row and likelihood in the left column. For a given hazard description, the severity is first determined using the methodology above. In some cases the hazard descriptions postulated a collision of two aircraft or controlled flight into terrain, making them catastrophic by definition. The likelihood of occurrence was determined based on a qualitative judgment with input from experts familiar with the system and its operation. The intersection of Severity and Likelihood determines the level of risk acceptability on the matrix. For example, a "1 C" is of Catastrophic Severity (1), but Extremely Remote (C) Likelihood; therefore, the risk is high.

5.3 Hazard Descriptions

For the purpose of this Status Report hazard descriptions were further refined into sub-hazard descriptions, with identifying hazard description codes. The sub-hazard descriptions were generated as a means to further breakdown, categorize, and understand the Capstone Phase II RNAV operations system. The 17 hazard description codes in the PHA are based on the assumed system and subsystem equipment and external interfaces. The hazard descriptions are defined below.

Type Code	Description	Hazard Description Number
H	Hazardous Misleading Information	This column will be completed in the DAR once all the hazard descriptions are identified and validated.
EM	Emergency	
UNP	Unable to proceed	
IND	Inadequate data	
M	Misuse	
LSA	Loss of situational awareness	
INPD	Inappropriate presentation of data Data deviation Alteration of data	
O	Overload of data/information	
MK	Masking of data/information/communication	
T	Training	
P	Procedure	
L	Loss of safety-related data/information Loss of communications Loss of system	
D	Design	
HE	Human Error	
A	Alert/warning	
I	Integration	
MA	Maintenance Availability	

Table 5.5 Hazard Description Table

In most cases, hazard descriptions are grouped into hazard description "sets," A set consists of a theme, which is a combination of system state and causes to a sequence of events that result in a postulated harm. The causes are varied in combinations and permutations of system failures and inappropriate human action or response. Each variation in a hazard description set may affect either severity or likelihood, or both and were developed to identify new or different requirements. If variations in a hazard description set do not produce new requirements, or another worst-credible hazard the additional hazard descriptions will not be reflected in the DAR.

Hazard descriptions are short concise statements that define the basic hazard description (the circumstances and outcome expected from the full tabular hazard description data). The severity is the worst-credible severity harm expected should the hazard description occur. Risk is based upon Table 5.4, Operational Safety Assessment Hazard Classification Matrix the FAA System Safety Management Plan. The left-hand number refers to the "Effect on" column; the right-hand number refers to the Hazard Classification. Possible Effect indicates the worst-credible harm expected. Flight Phase defines when in the life cycle the event could occur, i.e. Takeoff, Landing, Approach, Terminal, Surface, EnRoute, Oceanic, etc.

It is expected that hazards will be eliminated or controlled to an acceptable level should appropriate implementation of the Status Report Controls (existing and/or recommended safety requirements) occur. Since this is the case, initial high-level Safety Requirements have been defined from these Status Report Controls.

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

5.4 System Safety Order of Precedence

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

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

Table 5-6 Safety Order of Precedence

6.0 Preliminary Hazard Analysis

6.1 Preliminary Hazard Analysis General Findings

The Preliminary Hazard Analysis has currently identified 41 high hazards, one hundred and fourteen medium hazards, and seventy-six low hazards. More hazards are being developed and will be contained in the DAR. High and medium hazards are defined by the catastrophic loss of life, and/or loss of aircraft. These losses are postulated on undesired outcomes, such as a collision between two airplanes, Controlled Flight into Terrain (CFIT) or crash landing. Because the hazard description sets or variations on a theme are postulated with one of each set's outcomes predetermined as a worst-credible there are many hazard descriptions identified as potential "high" risks. The high risks are also partially due to the fact the full Capstone Phase II system architecture is not developed. The hazard controls (existing and/or recommended safety requirements) will be further refined as the system is further defined and most, if not all, high hazards are expected to be lowered.

7.0 Preliminary Requirements Recommendations

While the Capstone Phase II PHA is still currently under development a number of early safety requirements have been identified. These safety requirements are expected to expand as the PHA is completed.

7.1 Candidate Safety Requirements

Table 7.1 below is set up in a tabular format divided into four (4) columns. The first column (1) (Control/Requirement Number) shows the sequential numeric listing of all current Recommended Candidate Requirements. The sequential numeric listings start with the number one (1) and proceeds through number one hundred fifty-one (151). Column two (2) contains the Requirements. The last columns, three (3) and four (4) allow identification of the Candidate Safety Requirements/Recommendations statements as either "Existing" or "Recommended." An Existing Requirement is one that can be traced to current FAA, other governmental, or consensus requirements documentation.

Note: Numerous requirements contain language which is broad in context, such as "to preclude", etc. The requirements language will be more clearly defined following the May meeting of the CIISSWG. The validation process will include a rewrite of the controls/requirements into verifiable requirements language where possible.

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

Req. #	Controls	Existing	Recommended
1	1. Design, develop, and implement engineering and administrative controls to preclude hazardous misleading information (HMI) from occurring due to automated ground system malfunction.		X
2	2. Design, develop, and implement engineering and administrative controls to preclude hazardous misleading information (HMI) from occurring due to avionics system malfunction.		X
3	3. Design system to meet reliability and availability requirements of NAS-SR-1000.	X	
4	4. Apply system reliability and availability requirements to preclude hazardous failures, system anomalies, and malfunctions.	X	
5	5. Design system such that no single software anomaly, common software malfunctions or design feature shall result in a catastrophic or hazardous event, (severity 1 or 2).	X	
6	6. Design Software in accordance with Advisory Circular 20-115B (DO-178B).	X	
7	7. Design, develop, and implement engineering and administrative controls to provide and assure detection of hazardous failures, malfunctions and anomalies.		X
8	8. Evaluate electromagnetic environments at site-specific areas and design system to preclude electromagnetic environmental effects.		X
9	9. Design system to be hardened against electromagnetic interference to the applicable standards in FAA G 2100-F, MIL-STD-461D, MIL-STD-436D and FCC Regulations.	X	
10	10.Provide pilot and controller training and procedures for Capstone Phase 2, to preclude human error and increase situational awareness.		X
11	11. ATC to use 7110.65 procedures for validating aircraft ID, position and altitude.	X	
12	12. Design, develop, and implement engineering and administrative controls for Capstone Phase 2, to preclude traffic, CFIT, and conflict hazards.		X
13	13. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with existing WAAS requirements, procedures, protocols, regulations, rules, codes, and standards related to upgrades, changes, and integration, within Capstone Phase 2 and implement controls to preclude such risks.	X	
14	14. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with existing GPS requirements, procedures, protocols, regulations, rules, codes, and standards related to upgrades, changes, and integration, within Capstone Phase 2 and implement controls to preclude such risks.	X	
15	15. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with new route structure requirements, procedures, protocols, regulations, rules, codes, and standards related to upgrades, changes, and integration, within Capstone Phase 2 and implement controls to preclude such risks.		X
16	16. Develop Aircrew/ATC procedures to accommodate contingency situations associated with new route structure development.		X
17	17. (E 35b.) Provide training on operational uses of the Capstone equipment to include terrain avoidance, weather avoidance, contingencies, and other flight planning functions.		X

18	18. Ensure terrain/airfield chart accuracy, associated with Capstone Phase 2, i.e. fixed object location, data base and terrain integrity, runway locations, construction, helipads, changes, etc		X
19	19. (E) Establish minimum proficiency requirements for Capstone Phase 2 equipment, flight procedures, and refresher training; based upon inputs from lessons-learned and pilot survey information.		X
20	20. (E 57.) Ensure the Capstone participation agreement specifically defines both appropriate and inappropriate uses of the Capstone Phase 2 system and equipment.		X
21	21. Continue to implement/establish/refine requirements for procedures, protocols, regulations, rules, codes, and standards associated with aircraft certification to preclude external hazards/risks associated with Capstone Phase2.		X
22	22. Continue to implement/establish/refine requirements for procedures, protocols, regulations, rules, codes, and standards associated with ground system certification to preclude external hazards/risks associated with Capstone Phase 2.		X
23	23. Conduct controller/pilot workload assessments to evaluate the potential for informational overload associated with Capstone Phase 2 equipment and implement controls to preclude such risks.		X
24	24. Conduct analysis, studies, simulations and/or flight tests to identify system safety related risks associated with human factors in the integration of Capstone Phase 2 and implement controls to preclude such risks.		X
25	25. Design, develop, and implement engineering and administrative controls to preclude overload associated with Capstone Phase 2 equipment and implement controls to preclude such risks.		X
26	26. Design, develop, and implement engineering and administrative controls to preclude the inappropriate presentation of data/information within cockpit causing fixation, confusion, and loss of situational awareness.		X
27	27. Design, develop, and implement engineering and administrative controls to preclude the masking of safety-critical data/information within cockpit from causing fixation, confusion, and loss of situational awareness.		X
28	28. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude the inadvertent loss of safety-related data/information presented within cockpit.		X
29	29. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude the inadvertent altering of safety-related data/information presented within cockpit.		X
30	30. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude deviations to safety-related data/information displayed between the controller and pilot.		X
31	31. Design, develop, and implement engineering and administrative controls associated with new holding areas to provide collision clearances.		X
32	32. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude loss of, or interruption of communication associated with Capstone Phase 2.		X
33	33. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude loss of		X

	surveillance of single or multiple aircraft.		
34	34. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to provide safety-related communications/emergency communication/notice between pilots, controllers, and technicians related to hazardous failures, malfunctions, errors, or anomalies.		X
35	35. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to provide redundant safety-critical applications associated with Capstone Phase 2.		X
36	36. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude the inadvertent shut down of safety-critical applications.		X
37	37. Design, develop, and implement engineering and administrative controls associated with ground systems to preclude the loss of all ATC displays.		X
38	38. Design, develop, and implement engineering and administrative controls associated with ground systems to preclude external and environmental hazards.		X
39	39. Conduct analysis and studies to identify system safety related risks associated with external and environmental hazards in the integration of Capstone Phase 2 and implement controls to preclude such risks.		X
40	40. Design, develop, and implement engineering and administrative controls associated with ground systems to preclude physical hazards.		X
41	41. Conduct analysis and studies to identify system safety related risks associated with physical hazards in the integration of Capstone Phase 2 and implement controls to preclude such risks.		X
42	42. Researved		
43	43. Design, develop, and implement engineering and administrative controls associated with airborne systems to preclude external, environmental, and physical hazards.		X
44	44. Design, develop, and implement engineering and administrative controls associated with airborne and ground systems to preclude latent hazards associated with inappropriate assembly, installation, and / or maintenance action.		X
45	45. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to preclude errors in installation, assembly, maintenance; design, calculation, analysis, protocols, procedures, training, communication, SW development, interpretation, integration, and reading of, or use of, instruments.		X
46	46. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to preclude delay, interruption, malfunction of safety-related data/information due to latency.		X
47	47. Design Capstone Phase 2 communication links to meet latency requirements of NAS-SR-1000.	X	
48	48. Design Capstone Phase 2 system, including application processing to meet latency requirements of NAS-SR-1000.	X	
49	49. Test to detect latency times in excess of those in NAS-SR-1000.	X	
50	50. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to integrate with ADS-B/NAS provide redundancy, maximize system alert capability, and preclude alert delay, alert malfunction, masking, and LTA alert communication, associated with catastrophic or hazardous events, (severity 1 or 2 risks).		X

51	51. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to preclude the risks of inappropriate mixed-equipage use.		X
52	52. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to ensure that participating aircraft are equipped for the intended application.		X
53	53. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to preclude weather-related HMI.		X
54	54. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to include weather data/information to enable navigation.		X
55	55. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to include integration of FIS and preclude associated HMI, loss of information, or inadequate information.		X
56	56. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to include integration of AWOS and preclude associated HMI, loss of information, or inadequate information.		X
57	57. Design, develop, and implement engineering and administrative controls associated with FIS and AWOS and preclude associated HMI, loss of information, or inadequate information.		X
58	58. Design, develop, and implement engineering and administrative controls associated with NOTAMS affecting Capstone Phase 2 related services and provide requirement for use prior to accessing flight routes.		X
59	59. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude the inadvertent loss of safety-related data/information presented within controllers display.		X
60	60. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude the inadvertent altering or intentional loss of of safety-related data/information presented within controllers display.		X
61	61. Design, develop, and implement engineering and administrative controls associated with ground and airborne systems to preclude/mitigate security-related risks, i.e. spoofing, jamming, intentional alteration of data, loss of safety-related data/info.		X
62	62. Designate alternative airports/landing areas in support of contingency planning associated with new route structure development.		X
63	63. Design, develop, and implement engineering and administrative controls associated with navigation and surveillance to assure the accuracy of information and data, and provide real-time independent accuracy checks/tests to identify, report, and correct deviations.		X
64	64. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 aircraft to include missed approach requirements and preclude related risks.		X
65	65. Conduct analysis, studies, simulations and/or flight tests to evaluate "poor-mans INS' for contingency use in dead-reckoning; Design, develop, and implement engineering and administrative controls to implement capability if appropriate.	X	
66	66. Design, develop, and implement engineering and administrative		X

	controls associated with Capstone Phase 2 to provide redundancy in support of (TBD) reliability, availability, and maintainability requirements.		
67	67. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to provide maintenance accessibility in support of (TBD) reliability, availability, maintainability, requirements.		X
68	68. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics adaptable parameters to preclude human error/ procedure deviation associated with data configuration and inappropriate alteration of safety-related data/information.		X
69	69. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics adaptable parameters to preclude the inappropriate interchanging of avionics spares.		X
70	70. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics parameters associated with the "dead stick glide" function to preclude error in use, inappropriate use, mis-use, or mis-information.		X
71	71. Conduct analysis, studies, simulations and/or flight tests to evaluate "dead stick glide" function for contingency use in an emergency; Design, develop, and implement engineering and administrative controls to implement capability if appropriate.		X
72	72. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics parameters associated with the "skyway" function to preclude error in use, inappropriate use, mis-use, or mis-information.		X
73	73. Conduct analysis, studies, simulations and/or flight tests to evaluate "skyway" function for contingency use in an emergency; Design, develop, and implement engineering and administrative controls to implement capability if appropriate.		X
74	74. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics parameters associated with the "skyway" and "direct-to" function to preclude error in use, inappropriate use, mis-use, or mis-information.		X
75	75. Conduct analysis, studies, simulations and/or flight tests to evaluate "skyway" and "direct-to" function for nominal and contingency use in an emergency; Design, develop, and implement engineering and administrative controls to implement capability if appropriate.		X
76	76. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics parameters associated with configuring "BUG" functions (altitude, heading, airspeed, VNAV) to preclude the setting of parameters/functions that may cause the aircraft to be flown outside it's performance envelope, or be exposed to collision/CFIT hazard.		X
77	77. Conduct analysis, studies, simulations and/or flight tests to evaluate 78"BUG" functions (altitude, heading, airspeed, VNAV) for nominal and contingency use in an emergency; Design, develop, and implement engineering and administrative controls to implement capability if appropriate.		X
78	78. Design, develop, and implement engineering and administrative		X

	controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data presented in manuals, supporting literature, and training materials, procedures, protocols, to preclude the presentation of false, inaccurate, inappropriate and/or hazardous misleading information.		
79	79. Conduct analysis, studies, simulations and/or flight tests to evaluate safety-related information/data presented in manuals, supporting literature, and training materials, procedures, protocols, to preclude the presentation of false, inaccurate, inappropriate and/or hazardous misleading information.		X
80	80. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude the presentation of conflicting information.		X
81	81. Conduct analysis, studies, simulations and/or flight tests to evaluate functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude the presentation of conflicting information.		X
82	82. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude simultaneous loss of primary and navigation displays as a result of common cause event/failure.		X
83	83. Conduct analysis, studies, simulations and/or flight tests to evaluate functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude simultaneous loss of primary and navigation displays as a result of common cause event/failure.		X
84	84. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude displaying erroneous /inaccurate navigation database information.		X
85	85. Conduct analysis, studies, simulations and/or flight tests to evaluate functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays to preclude displaying erroneous /inaccurate navigation database information.		X
86	86. Provide requirements, procedures, protocols, regulations, rules, codes, and standards related to upgrades, changes, and integration of Capstone Phase 2 to incorporate and implement notification/training of non-Capstone aircraft/flying public non-participants, for public RNAV procedures (AIM, NOTAM, general guidance); to preclude traffic/collision hazards.		X
87	87. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 ATC/ground adaptable parameters to preclude human error/ procedure deviation associated with data configuration and inappropriate alteration of safety-related data/information.		X
88	88. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to include human factors		X

	considerations to preclude misinterpret weather observation/forecast information provided/presented in the cockpit.		
89	89. (E 43.) Conduct associated system safety efforts such as hazard analysis, risk assessment, hazard tracking and risk resolution activities throughout Capstone life cycle.		X
90	90. (E 25) Pilot situational awareness.	X	
91	91. (E 42.) Evaluate the avionics package for design enhancements to prevent erroneous pilot action.		X
92	92. (E 60.) Conduct human factors evaluation and conform to appropriate standards (e.g., Human Factors design guide FAA CT-96/1).		X
93	93. (E 35a.) Pilot training/procedures in place for Capstone – approved Part 135 training curriculum, 2 day ground school, line flight check. Preflight set-up/procedures to make as simple use as possible – normal instrument scan. Includes e.g., proper CRM for cross check of erroneous info (e.g., setting baro, target and navigation info). This may include cross-check with other information in cockpit as well as coordinating with ATC (e.g., ATC gives altimeter setting).		X
94	94. (E 5.) Controller situational awareness.	X	
95	95. (E 41.) Assure that controller training and procedures are in place for Capstone, to minimize human error and increase situational awareness.		X
96	96. (E 42a.) Evaluate the ground system package for design enhancements to prevent erroneous controller action.		X
97	97. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays, controller's/technicians displays, and instruments to enable and enhance visual identification of safety-related data/information; considering possible lighting and placement conditions.		X
98	98. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 functions, capabilities, and annunciations associated with safety-related information/data displayed on primary and navigation displays, controller's/technicians displays, and instruments to enable and enhance cautions, warning, detection indications.		X
99	99. Conduct analysis, studies, simulations and/or flight tests to evaluate functions, capabilities, annunciations, indications, symbols, icons, depictions, and illustrations associated with cautions, warning, detection indications and to preclude hazards associated with LTA communication.		X
100	100. (E 17.) Avionics certification, installation, and approval process in place for Capstone, in conformance with DO-178B for avionics.	X	
101	101 (E 18b). Avionics include integrity monitor to alert of avionics failure.	X	
	18a. Integrity, availability, reliability should meet the requirements specified in the UAT Interim Design Specification.	X	
102	102. (E 24.) Avionics include data flag annunciation to pilot, automatically indicating various avionics system failures (MX20 User Guide, GX60 Users Guide).	X	
103	103 (E 39a.) Avionics are placarded with warnings to prevent inappropriate use.	X	
104	104 (E39b.) Conduct a review of installed Capstone equipment to verify appropriate placarding.		X
105	105 (E 59.) Verification and validation of critical software during testing		

	for avionics and ground system.		
106	106 (E 63.) Continue tracking and evaluation of software anomalies for avionics and ground system.		
107	107. Design, develop, and implement engineering and administrative controls associated with airborne and ground system displays to preclude inadvertent loss of targets, exclusion of targets, clutter of targets, misidentification of targets, and to depict real-world indications and enhance situational awareness.		
108	108. Conduct analysis, studies, simulations and/or flight tests to evaluate the airborne/ground displaying of targets to depict real-world indications and enhance situational awareness.		
109	109. (E 8.) ADS-B radar-like separation standard (e.g., 5 nmi, MEAs) is defined to allow intervention time for ATC and pilot to respond safely in case of system failure or other contingencies.	X	
110	110 (E 15.) Standard 7110.65 controller procedures for validating aircraft altitude will be applied when using ADS-B as a surveillance source, the same as when using radar as a surveillance source.	X	
111	111 (E 64.) Establish database update revision cycle requirements for Capstone, including changes between revision cycles, and annunciation to pilot if outdated.		X
112	112 (E 71.) Review and validate terrain databases to eliminate conflicting, inaccurate, and inappropriate data that could result in hazardous misleading information.		X
113	113. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 avionics parameters associated with configuring "BUG" functions (altitude, heading, airspeed, VNAV) to preclude the setting of parameters/functions that may cause the aircraft to be flown into hazardous situations.		X
114	114. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude inappropriate placement of Capstone Phase 2 equipment which creates hazards: fixation, confusion, and loss of situational awareness, excessive workload, inaccessibility of controls/equipment, material handling stress, illumination, noise, blocking of instruments/access, maintainability, excessive heads down, and ergonomic stress.		X
115	115. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude Pilot/aircrew fixation, confusion, and loss of situational awareness occur due to excessive safety-related data/information presented associated with Capstone Phase 2.		X
116	116. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude excessive glare on Capstone Phase 2 cockpit instruments/ Displays results in fixation, confusion, and loss of situational awareness, misreading, miscommunication, and misinterpretation of safety-related data/information.		X
116a	116. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to include placarded warnings associated with Capstone Phase 2 are adequate to prevent inappropriate use.		X
117	117. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude electromagnetic environmental effects to Capstone Phase 2 system/equipment/components which results in damage to system,		X

	malfunction, fault, failure, and/or loss of range, and/or loss of position accuracy, ghosting, noise, electrical/static discharge.		
118	118. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude loss of, or malfunction of, Capstone Phase 2 system due to electro-static discharge damage to ground or airborne equipment.		X
119	119. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude local loss of/degradation of Capstone Phase 2 system due to extreme weather conditions/exposure.		X
120	120. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system in accordance with FAA G 2100-F specifically to precludes hazards associated with environmental/physical factors, i.e., shock, vibration, temperature, electrical fault, foreign object damage.		X
121	121. Conduct analysis, studies, simulations and/or flight tests to evaluate weather-related anomalies that adversely effect signal in space availability and continuation of service associated with GPS, WAAS, and voice communications; design system to preclude hazards: loss of signal, intermittent signal, saturation, unavailability, noise, electromagnetic environmental effects.		X
122	122. (E 77.) Evaluate and design the Capstone system to minimize the potential for bandwidth saturation.		X
123	123. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system to preclude frequency saturation of receivers, allocate appropriate bandwidth to accommodate current and projected traffic growth and select transmission frequencies with enough bandwidth to accommodate the allocation.		X
124	124. (E 6.) ADS-B track loss is detected and indicated to controller. If available primary or secondary radar targets will be indicated, or lost track will automatically coast.		X
125	125. (E 7a.) Standard 7110.65 controller procedures for validating aircraft ID, position, and altitude when using radar as a surveillance source will be applied when using ADS-B as a surveillance source. Including procedures for loss of target. Controller will apply another means of separation.	X	
126	126. (E 9.) Air-to-air ADS-B surveillance could allow a cockpit situational awareness back up for ground system failures.		X
127	127. (E 29.) Air-to-air ADS-B surveillance can provide an additional means of detection of aircraft ADS-B avionics failure.		X
128	128. (E 1.) Ground system certification, installation, and approval process in place for Capstone to meet critical-level services in accordance with NAS-SR-1000.	X	
129	129. (E 1a.) Ground system certification, installation, and approval process in place for equipment external to Capstone to meet critical-level services in accordance with NAS-SR-1000.	X	
130	130. (E 3.) Real-time monitoring of ground system through use of GBT status message and ADS-B fixed parrot.	X	
131	131. (E 4a.) Controller and maintenance procedures (proactive and reactive) and training are in place for ground system equipment failures/malfunctions.		X
132	132. Conduct analysis, studies, simulations and/or flight tests to evaluate the redundancy associated with avionics and ground system safety-critical		X

	data/information and design avionics to meet (TBD) redundancy, reliability, and availability.		
133	133. Conduct analysis, studies, simulations and/or flight tests to evaluate interface hazards associated with Capstone Phase 2 and design system to preclude such hazards.		X
134	134. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 system architecture to ensure failure isolation of COTS and NDI hardware, firmware, and software.		X
135	135. Conduct analysis, studies, simulations and/or flight tests to evaluate the use of COTS and NDI; Design, utilize, and provide COTS and NDI hardware, firmware, and software discriminators TBD.		X
136	136. Contractor safety studies, analyses, assessments, reviews, and system safety documentation shall be reviewed by the CSSWG for consistency, accuracy, quality, soundness, applicability, and inconsistencies evaluated and investigated to assure that design are developed, and implemented via engineering and administrative controls associated with Capstone Phase 2 system.		X
137	137. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 SW architecture to ensure failure/malfunction isolation, and risk mitigation of firmware, and software.		X
138	138. Conduct analysis, studies, simulations and/or flight tests to evaluate the use of SW; Design, utilize, and provide SW-related hardware, firmware, and software controls/ discriminators TBD.		X
139	139. Conduct analysis, studies, simulations and/or flight tests to evaluate airports associated with Capstone Phase 2 to provide suitable/intended use and provide marking, illumination, surface design, weather/communication/movement sensors/ accessibility of equipment, vehicles and provide procedures in accordance with (TBD) FAA requirements.		X
140	140. Conduct analysis, studies, simulations, contingency drills, and/or flight tests to evaluate search and rescue activities using Capstone Phase 2 system; provide controls to preclude the hampering, hindering, or delaying of operations.		X
141	141. Provide FSS personnel training and procedures for Capstone Phase 2, to preclude human error and increase situational awareness.		X
142	142. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 FSS situational display to preclude HMI and the inappropriate presentation of safety-related data/information.		X
143	143. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 displays to preclude the presentation of inconsistent safety-related data/information from being communicated via automation and voice to the cockpit.		X
144	144. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 RCAG and RCO design, application, placement, and availability to preclude loss of communication.		X
145	145. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 preclude such hazards, i.e. latency, delay, inaccurate/inadequate weather data/information.		X
146	146. Conduct analysis, studies, simulations and/or flight tests to evaluate weather-related hazards associated with Capstone Phase 2 and design system to preclude such hazards, i.e. latency, delay, inaccurate/inadequate		X

	weather data/information.		
147	147. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 and the use of, and integration of, multilateration to preclude such hazards, i.e. loss of targets, ghosting, loss track, false target indication, loss of function.		X
148	148. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 and the use of, and integration of, TIS-B to preclude such hazards, i.e. loss of information, HMI, loss of function.		X
149	149. Provide AFS personnel training and procedures for Capstone Phase 2.		X
150	150. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 AFS oversight responsibilities.		X
151	151. Design, develop, and implement engineering and administrative controls associated with Capstone Phase 2 to include the accurate input, coding, decoding, and maintenance of chart data throughout the life cycle.		X
152	152. (E17) Avionics certification, installation, and approval process in place for Capstone, in conformance with standard aircraft certification procedures (e.g., TSO-129C, DO-178B (software) and AC-23.1309-1C (hardware).	X	
	Phase I Controls Carried-Over		
	1. Ground system certification, installation, and approval process in place for Capstone to meet critical-level services in accordance with NAS-SR-1000.		
	1a. Ground system certification, installation, and approval process in place for equipment external to Capstone to meet critical-level services in accordance with NAS-SR-1000.		
	1b. Certification, installation, and approval process in place for equipment external to Capstone to meet critical-level services in accordance with NAS-SR-1000.		
	2. If in non-radar environment, current procedural separation rules are being applied, given the large is not ADS-B equipped. No change to current operations.		
	3. Real-time monitoring of ground system through use of GBT status message and ADS-B fixed parrot.		
	4a. Controller and maintenance procedures (proactive and reactive) and training are in place for ground system equipment failures/malfunctions/limitations.		
	4b. Ensure applicable avionics maintenance procedures and training are in place, to assure avionics maintenance is conducted appropriately.		
	4c Ensure GBT coverage is adequate for providing ATC radar-like services		
	6. ADS-B track loss is detected and indicated to controller. If available primary or secondary radar targets will be indicated, or lost track will automatically coast.		
	9. MFD could enhance pilot situational awareness in the event of a ground system and/or avionics failure.		
	10. ADS-B erroneous position is detected via MEARTS track processing and indicated to controller. If available primary or secondary radar targets will be indicated, or lost track will automatically coast.		
	11. Design to minimize risk due to transmission delay		
	26. Real-time monitoring of ground system through use of ADS-B fixed parrot. Real-time tracker processing of ADS-B tracks is conducted, to determine if tracks are valid (e.g., 3 good hits).		

	36. Conduct a review of Capstone ground system manuals to ensure that appropriate cautions and warnings are provided.		
	53. Minimum proficiency requirements have been established for Capstone equipment, flight procedures, and refresher training; based upon inputs from lessons-learned and pilot survey information.		
	55. Provide security controls to minimize the potential for jamming risk.		
	56. Provide security controls to minimize the potential for spoofing risk.		
	74. Assure that the ground system conforms to the specifications for electronic equipment (e.g., general requirements in FAA-G-2100g).		
	77. Evaluate and design the Capstone system to minimize the potential for bandwidth saturation.		
	78. Evaluate and design the Capstone system to minimize the potential for erroneous or inappropriate ICAO address posting on ADS-B tracks.		

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

8.0 Preliminary Hazard Analysis Findings

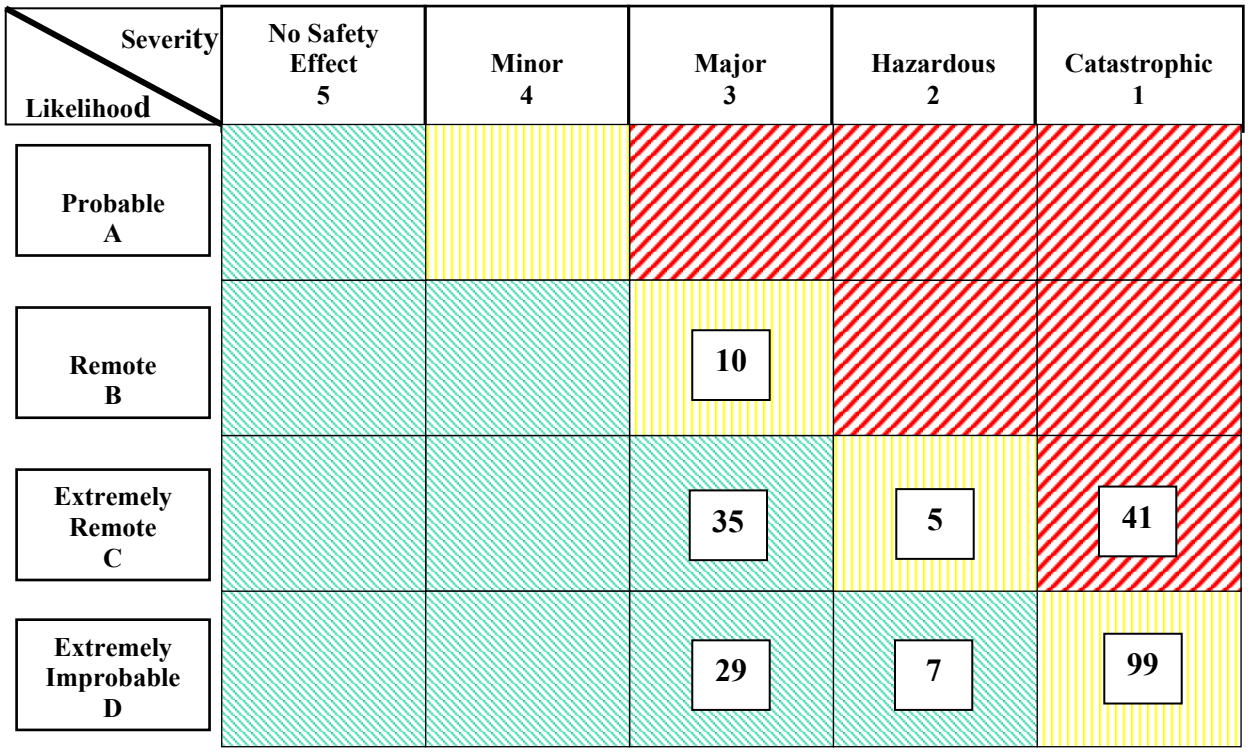
The Preliminary Hazard Analysis findings are provided as they currently exist. Additional findings, in the form of hazard descriptions and safety requirements may be developed as the PHA matures to completion. The early findings do indicate the need for the development of a Capstone Phase II System Specification document.

8.1 Risk Assessment Ratings

At this time Forty-one (41) **High Risk** hazard descriptions were identified. One hundred fourteen (114) fell in the **Medium Risk** region of the matrix, and seventy-one (71) hazard descriptions were in the **Low Risk** region. The PHA in the Preliminary Hazard Analysis Tables is sorted in the order of decreasing risk, i.e., 1C/High, 1D, 2C, 3B/Medium, 2D, 3C, 4B, 3D, and 4C/Low.

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

Figure 8-1 - Assessment of Risk Associated with PHA Hazard descriptions



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

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

9.0 System Safety Activities

9.1 Proposed Activities

The following is an initial list of system safety efforts for Phase II:

The Capstone System Safety Program has been expanded to include Phase II.

- The program includes the formation of a Capstone Phase II System Safety Working Group to administer the program and conduct analysis.
- A System Safety Program Plan should be developed for Capstone Phase II activities.

1 A System Safety Program Plan has been developed for the Capstone Phase II RNAV program. It has been reviewed by the CIISSWG and signed by the Program Office. It will next go through the NAS SSWG for approval.

- A System Hazard Analysis will be conducted to identify safety-related risks associated with Phase II.
- Hazard Tracking and Risk Resolution activities are planned to closeout all identified risks.
- All controls/requirements must be validated

Specific system safety contractual requirements should be included in subcontracts (e.g., avionics, ground systems).

- Subcontractor System Safety Program
- Subsystem Hazard Analysis
- Participation in the Capstone System Safety Working Group
- Generation of System Safety Status Reports

Lessons learned and safety activities from Phase I should be applied to Phase II. This includes such things as additional detail on operational data collection requirements in the Phase II Capstone Program Aircraft Owner Agreement, facilitating pilot/user safety meetings, encouraging internal safety programs/attitudes among the operators, and exploring means to ensure consistent training.

9.2 Completed Activities

- The Phase II Capstone Program Aircraft Owner Agreement has been completed and distributed.
- Facilitating pilot/user safety meetings are being conducted.
- The Capstone Phase II System Safety Program Plan was completed 19 February 2003. The document was signed by John Hallinan, the Capstone Program Manager. It is currently waiting approval by the NAS System Safety Working Group (SSWG) which is scheduled to meet 18 March 2003.
- The Capstone Phase II Preliminary Hazard Analysis (PHA) is currently under development. The draft report identified high level hazards and controls/requirements.
- All hazards have been evaluated by the Capstone Phase II SSWG and been determined to be appropriate/valid for the system.

The status of controls/requirements will be determined during meetings scheduled in Anchorage and Juneau for the week of 19 May 2003. Safety requirements not verified and closed at the end of these meetings will be worked and verified and closed during subsequent meetings.

The results of the May meeting will be incorporated into the PHA. The findings in the PHA will then be entered into the Hazard Tracking System for the purpose of verification of closure of all open controls/requirements. The data entered into the HTS will produce Safety Action Records which will be periodically review by the NAS SSWG.

9.3 Continuing Activities

A part of the requirements for the end-to-end safety analyses is a Functional Analysis. A Functional Analysis is under development and is scheduled for completion by the end of June 2003.

- A Design Analysis Report (DAR) is scheduled to be completed by the end of June 2003. The DAR will contain the findings, conclusions, and recommendations generated by both the PHA and Functional Analysis.
- A System Hazard Analysis will be conducted as the Capstone Phase II system architecture and hardware mature.

9.4 Analysis Conclusions

The analysis, at this time, evaluated approximately 226 hazards and produced 151 recommendations for controls to eliminate or reduce the risks associated with identified hazards. The controls covered the end-to-end operation of the system and may therefore impact the manufacturers of the on-board avionics, the operators of the aircraft or vehicle, the services to be supplied by the NAS, the builders of the ground system, and the user community.

9.5 Concerns

The table below groups all of the "High" risk hazards currently identified in the PHA. The risk associated with these hazards are considered "High" because the system design or maturity does not yet demonstrate appropriate solutions for risk controls. As the system matures adequacy of engineering, procedural, and training controls can be evaluated. Where controls can be shown to either reduce or eliminate the hazard severity, or reduce the likelihood of occurrence, the control rankings will be reduced to mediums or lows.

HMI Hazardous Misleading Information	Loss of Situational Awareness & Human Factors	Alerts Warnings	Primary navigation subsystem * Avionics	Safety Data & Display Data	Weather Related	Loss of Comm.	Lost Surveillance	Less that Adequate Training	Less that Adequate Procedures
Undetected HMI occurs due to avionics malfunction.	Fixation confusion	Airborne alert/warning is inadvertently shut off/down and do not provide notice when needed.	Inadvertently shut down at critical time.	Inadvertent altering of safety-related data /information	Rapid deterioration of weather	EnRoute IFR aircraft loses communications with ATC during emergency.	EnRoute IFR aircraft surveillance is lost due to malfunction.	Fixation, confusion, and loss of situational awareness occur due to LTA training	Missed approach procedure is LTA situation results in CFIT
	LTA human factors consideration	Airborne Alert/ warning are not adequately communicated	Pilot/ Aircrew configures BUG functions (altitude, heading, airspeed, VNAV) outside of aircraft	Deviations occur between the controller and pilots	VFR aircraft inadvertently enters poor weather conditions and progresses into EnRoute IFR aircraft flight path.			VFR aircraft inadvertently enters extreme weather and attempts to use Phase 2 avionics/ subsystem for emergency navigation.	Fixation, confusion, and loss of situational awareness occur due to LTA procedures

			performance parameters.						
		Ground Alert/warning is not adequately communicated.	Loss of powered flight condition exists, and dead stick glide function is in use and is LTA		Aircraft is EnRoute at minimums for VFR and weather deteriorates rapidly				Capstone Phase 2 contingenc y planning and access associated with the use of alternate airports is LTA
		LTA integration of cockpit alerts							

In addition to the above hazard groupings, the Capstone Phase II System Safety Working Group believes it is prudent to develop a Capstone Phase II system specification.

10.0 Security

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

11.0 References

(1) FAA, *Research Evaluation Plan for ADS-B, Phase 1: Identification of Research Needs*, September 30, 1999

(2). *NAS Modernization System Safety Management Plan, FAA Acquisition Management System,* January 1 2001

(3). FAA-APO-99-1 FAA Long Range Aerospace Forecasts Fiscal Years 2015,2020 & 2025, June 1999.

(4). MIL-STD-882C System Safety Program Requirements, 19 Jan 1993

(5) FAA System Safety Management Program, May 1, 2000

(6) FAA System Safety Handbook, January 2001

(7) ADS-B High-Level Concept of Operations, status Summary, 12 January 2001.

12.0 Bibliography

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

Appendix A Acronyms and Definitions

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