



# **Capstone Safety Engineering Report #1**

## **ADS-B Radar-Like Services**

**VOLUME 1**

**Preliminary Hazard Analysis**

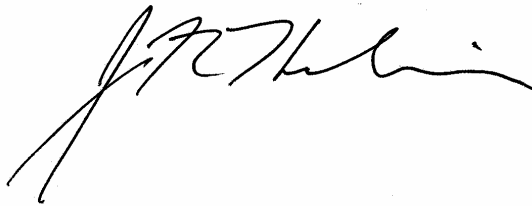
**02 December 2000**

The Capstone System Safety Working Group (CSSWG) prepared this report and conducted the analysis. The CSSWG also utilized expertise from other personnel involved in Capstone as needed. The Capstone Program Manager has primary responsibility for implementing system safety within Capstone. This analysis was performed in coordination with the FAA Office of System Safety (ASY) and follows standard safety practices.

CSSWG Members:

Michael Allocco, ASY-300  
August Asay, ACE-115N  
Lari Belisle, ZAN-530  
Kevin Brandon, NATCA  
James Call, AAL-1SC  
James Cieplak, MITRE/CAASD  
Leonard Kirk, University of Alaska Anchorage  
Michael Lenz, ASY-300  
Jim Patchett, ZAN-20  
Brad Wacker, Lt. Col. USAF

The CSSWG concurs that based on the Preliminary Hazard Analysis conducted on Capstone ADS-B radar-like services, the identified safety-related risks are controlled to an acceptable level provided that the mitigations are implemented.



John Hallinan  
Capstone Program Manager

## TABLE OF CONTENTS

### Volume 1 Capstone Safety Engineering Report #1: Preliminary Hazard Analysis

<b>1</b>	<b>SUMMARY.....</b>	<b>1</b>
<b>2</b>	<b>PURPOSE .....</b>	<b>3</b>
2.1	PURPOSE OF ANALYSIS .....	3
2.2	PURPOSE OF THE REPORT.....	3
<b>3</b>	<b>BACKGROUND.....</b>	<b>3</b>
3.1	CAPSTONE PROGRAM .....	3
3.1.1	Capstone System Safety Program Plan.....	4
<b>4</b>	<b>CAPSTONE ADS-B SYSTEM DESCRIPTION FOR RADAR-LIKE SERVICES.....</b>	<b>4</b>
4.1	OVERVIEW .....	4
4.2	CAPSTONE AVIONICS SYSTEM DESCRIPTION .....	5
4.2.1	GX60 GPS/VHF Communication System.....	6
4.2.2	MX20 Multi-Function Display .....	6
4.2.3	UAT Radio and Antenna .....	7
4.2.4	Serial Altitude Encoder.....	7
4.3	CAPSTONE ADS-B GROUND SYSTEM DESCRIPTION.....	7
4.3.1	Phase 1 ADS-B Architecture .....	8
4.3.2	System Performance Requirements .....	8
<b>5</b>	<b>ANALYSIS APPROACH AND METHODOLOGY .....</b>	<b>10</b>
5.1	CAPSTONE SYSTEM SAFETY ASSUMPTIONS .....	11
5.2	CAPSTONE SYSTEM SAFETY REQUIREMENTS.....	13
5.2.1	Hazard Tracking and Risk Resolution .....	13
5.2.2	Risk Assessment Measurement.....	13
5.2.3	Capstone System Safety Precedence .....	15
<b>6</b>	<b>HAZARD IDENTIFICATION AND ANALYSIS.....</b>	<b>16</b>
6.1	SCENARIO DISCUSSIONS .....	16
6.2	PRELIMINARY HAZARD ANALYSIS.....	18
6.2.1	MIL-STD-882 Approach .....	18
6.2.2	Risk Assessment .....	18
<b>7</b>	<b>PRELIMINARY CONTROLS/REQUIREMENTS RECOMMENDATIONS.....</b>	<b>21</b>
<b>8</b>	<b>REFERENCES AND BIBLIOGRAPHY.....</b>	<b>22</b>

### Volume 2 Capstone Safety Engineering Report #1: End-to-End System Preliminary Hazard Analysis Matrix of Scenarios

### Volume 3 Capstone Safety Engineering Report #1: List of Precautions, Controls and Mitigation

# Volume 1 Capstone Safety Engineering Report #1: ADS-B Radar-Like Services

## 1 Summary

A Preliminary Hazard Analysis (PHA) of Capstone ADS-B Radar-Like Services has been conducted by the members of the Capstone System Safety Working Group (CSSWG) to support the End-to-End Safety Review process requested by the Administrator of the Federal Aviation Administration (FAA). The PHA was conducted using methodologies based on MIL-STD-882D, Department of Defense Standard Practice for System Safety; the FAA Order 8040.4, Safety Risk Management; and the Draft FAA System Safety Handbook (April 2000). This PHA is a risk assessment considering severity of consequence and likelihood associated with a scenario (i.e., potential accident) and recommending precautions, controls, and mitigations.

The analysis evaluated approximately 200 scenarios (culled down to 81 in Volume 2) and produced 76 recommendations for controls to eliminate or reduce the risks associated with identified scenarios. The controls cover 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.

The following are general recommendations and findings from the CSSWG:

1. Precautions, controls, and mitigations generated by this analysis (Volume 3) should be implemented to ensure Capstone System Safety.
2. Controls should be reviewed approximately every 6 months and as the program changes to ensure their applicability and effectiveness as more information and operational experience is gained, and that the safety-related risks associated with the changes are evaluated.
3. Efforts should continue in the area of pilot training and familiarization given the pilot-in-command has final responsibility for the safety of the aircraft. All Capstone pilots' are to be appropriately trained and means to improve training and familiarization should be continued.
4. Each operator having a defined internal safety program can help mitigate risk related to Alaska flight operations and make Capstone efforts more effective. Mechanisms outside of regulating a safety program should be explored to ensure operator acceptance (e.g., insurance benefits).
5. The MX20 multifunction display is an integral part of the Capstone system and is therefore considered in this PHA. It was considered due to possible coordination issues between the pilot and controller during radar-like services, as well as being used as a control in such cases as ground system failures (e.g., enhanced pilot situational awareness).

6. The accuracy, frequency, and reliability of Capstone ADS-B data has been verified by the Capstone ADS-B acceptability evaluation for ADS-B radar-like services. Consideration should be given in using ADS-B data for additional enhancements, such as ADS-B received altitude displayed with primary radar targets. The recommendation is to ensure the controller and the ground automation system can utilize best possible information.
7. The UAT Interim Design Specification requires that “navigation equipment independent of the avionics supporting Radar-Like Services must be retained.” This is a recognized control in this analysis. Additional consideration needs be undertaken if the same avionics are to be used for both navigation and surveillance.
8. Based on PHA discussions, the most system “stressing” scenarios are when an ADS-B target and radar-target are being separated on fringe coverage areas. This is due to the compounding of potential errors and failures in both the ADS-B and radar systems.
9. Current barometric altimeter separation standards and procedures will be applied with the ADS-B altitude, given it is derived the same way as a Mode C altitude report (i.e., altitude encoder). There are known errors with barometric altitude and several scenarios consider these errors. Future consideration should be made in using GPS geometric altitude as a crosscheck with the barometric altimeter data. Additional research and evaluation on implications may need to be accomplished, but this crosscheck could be an added control for altimeter errors.
10. Several scenarios consider separation of an ADS-B aircraft and a non-ADS-B aircraft in a non-radar environment. The primary control for this case is that if in a non-radar environment, current procedural separation rules are being applied, given one aircraft is not ADS-B equipped. There is no change to current operations. However, if new procedural separation rules are developed between ADS-B and non-ADS-B aircraft (e.g., ADS-B flight corridor), these scenarios need to be re-examined.
11. Controls based on current enroute separation standards as well as current controller, pilot, and maintenance procedures and training simplifies the introduction of Capstone ADS-B radar-like services. Standard controls that are already in place and proven combined with only an incremental change for ADS-B radar-like services could reduce the risk of implementation. This philosophy should continue to be applied to other Capstone enhancements.
12. The Air Traffic Service Operational Readiness Review and Independent Office of Test and Evaluation (IOT&E) activities are considered an additional control to the ones listed in Volume 3 and should be continued.
13. The CSSWG concurs that based on the Preliminary Hazard Analysis conducted on Capstone ADS-B radar-like services, the identified safety-related risks are controlled to an acceptable level provided that the mitigations are implemented.

The CSSWG believes a System Safety Program should continue with the following recommendations:

1. To ensure a successful completion of an End-to-End Safety Review the CSSWG must complete hazard tracking and risk resolution efforts. This includes closeout of the controls and mitigations upon concurrence of the CSSWG.
2. The engineering controls and mitigations are directly associated with the successful integration and operation of the Capstone system. Upon successful integration and operation of the system the associated controls will then be considered verified and validated.
3. The CSSWG activities are continuous, and monitoring efforts must continue throughout the Capstone life cycle.
4. Future changes to the Capstone baseline system or program must be evaluated from a system safety view. The Capstone baseline has been defined within this Safety Engineering Report.

## **2 Purpose**

### **2.1 Purpose of Analysis**

This PHA was conducted to identify potential accident scenarios that are associated with Capstone providing ADS-B radar-like services. These scenarios have been defined with associated effects and risk defined by both severity and likelihood. These scenarios have been identified in order to develop hazard controls (i.e., precautions, controls and mitigations) 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 CSSWG 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 the Report**

This Capstone Safety Engineering Report #1 documents the result of the PHA for ADS-B radar-like services. An initial baseline has been established and criteria defined in order to conduct this analysis. This report presents this information. The PHA was initiated in January 2000 to support the Capstone Program in defining the process to successfully conduct an End-to-End Safety Review.

## **3 Background**

### **3.1 Capstone Program**

The Capstone Program is sponsored by the FAA's Alaskan Region and is 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 150 commercial aircraft serving the Bethel/Yukon-Kuskokwim delta area in and around Bethel, Alaska. For the first year and beyond, compatible data link transceivers installed at strategically located ground sites are designed to facilitate Air Traffic Control and flight information services.

### **3.1.1 Capstone 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 is documented in Section 5 of the Capstone Test and Evaluation Master Plan for ADS-B Radar-Like Services.

## **4 Capstone ADS-B System Description for Radar-Like Services**

A Capstone objective, as specified in the FAA Administrator's letter to the Alaska Air Carriers Association (3 January 2000), is to meet an operational date of 1 January 2001, for the use of the Capstone ADS-B system for radar-like services in airspace in and around Bethel, Alaska. Throughout calendar year 2000, certification and operational testing has taken place for both the avionics and ground systems. This will include determination that the avionics' broadcast signal is adequate for ATC provided radar-like services and that the Capstone ADS-B system is at least equivalent to radar in terms of reliability and performance. Another task specified in the Administrator's letter is an End-to-End Safety Review. The following Capstone system (airborne and ground) description will provide the context for this safety review.

### **4.1 Overview**

While radar surveillance capability accounts for significant operational efficiency, safety, and improved services in the NAS, not all NAS airspace is under radar surveillance coverage. The effective coverage of ground-based radar systems is subject to line-of-sight and shadowing effects, and though radar coverage does exist down to near the surface in the vicinity of radar sites (such as in busier terminal areas), many outlying areas are without coverage. As a result, many flights operated at the lower altitudes or away from terminal areas will likely traverse non-radar airspace. The adverse impact this has on flight operations is best illustrated by considering the procedures and services that radar surveillance makes possible.

Where radar coverage does exist, for example, the air traffic controller can use a wide range of techniques to maintain IFR separation, such as aircraft vectoring and speed control. When coupled with the accuracy of radar-derived position data (as compared to pilot position reporting in a non-radar environment), these techniques allow much smaller separation minima to be applied, thereby increasing traffic throughput. In addition, radar surveillance capability makes it possible to offer a wide range of services to VFR and IFR aircraft, including flight following and traffic advisories, minimum safe altitude warning (MSAW), and navigational assistance, for example. Search-and-rescue activities can also be better focused if radar data are available for a flight presumed missing. All of these techniques and services require the accurate position information from radar to be operationally effective.

In spite of its importance in the provision of separation and other services, it is not cost-effective to site and install ground-based radar systems to achieve complete radar coverage of NAS

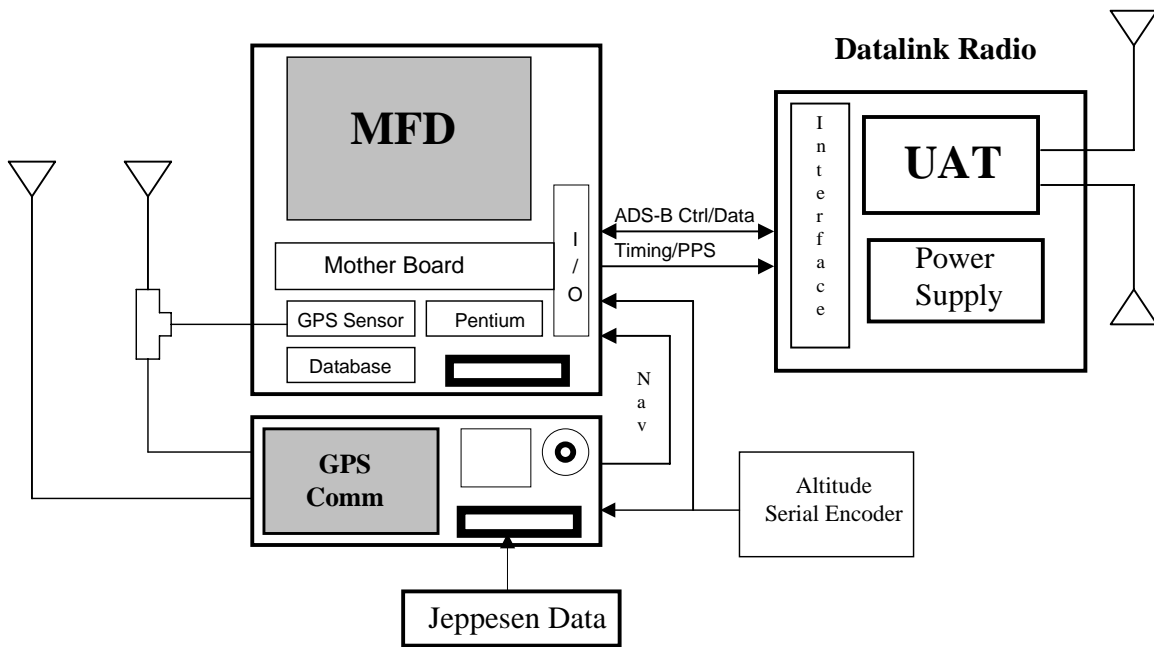
airspace. As a result, operations in non-radar airspace are conducted using less-efficient separation techniques, and some services are not possible. IFR operations at many airports that are below radar coverage, for example, are subject to what is known as “one-in-one-out” procedures. Under such procedures, only one IFR aircraft at a time is allowed to enter the non-radar airspace, and no other aircraft can enter until the preceding aircraft either reports clear of the runway (in the case of a landing), or becomes radar-identified upon entering radar coverage after takeoff. As a result, aircraft awaiting takeoff or approach clearances while a preceding aircraft is completing an operation can encounter significant delays.

The Capstone program provides avionics and ground systems with corresponding procedures and training for pilots, controllers, and maintenance personnel to implement the ADS-B radar-like services concept described above. Specific procedures and training will not be described in this document, but can be found in the Capstone Test and Evaluation Master Plan for ADS-B Radar-Like Services.

#### **4.2 Capstone Avionics System Description**

The Capstone program provides three UPS Aviation Technologies avionics products: the Apollo GX60 TSO-C129A certified GPS navigator/VHF communication radio (or GX50 TSO-C129A certified GPS navigator), the Apollo MX20 multi-function cockpit display (Capstone configured), and the Universal Access Transceiver (UAT) (Figure 1). Installation of these avionics is covered under FAA Supplemental Type Certificate (STC) No. SA02149AK in accordance with UPS Aviation Technologies “Capstone STC Master Drawing List” (P/N 560-1027-01). They are limited to supplemental VFR operations via the FAA approved “Airplane Flight Manual Supplement or Supplemental Airplane Flight Manual for Capstone System Installation” (UPSAT #560-1028-01). This system will be placarded “GPS and MFD limited to VFR use only”, and the aircraft/pilot must have other navigation capability appropriate to the route of flight. For radar-like services, the pilot use of the GPS and MFD will remain the same (i.e., enhanced situational awareness), however the UAT broadcasted ADS-B signal will be certified for use by controllers.





**Figure 1. Capstone Avionics System Block Diagram**

#### **4.2.1 GX60 GPS/VHF Communication System**

The GX60 is TSO-C129A Class A1 approved for IFR non-precision approach operation and also TSO-C37d, TSO-C38d and TSO-C128 approved 760-channel VHF communication transceiver. The Apollo GX60 will provide navigational data to the pilot via the internal moving map (note: the navigational information can also be displayed on the MX20). It also utilizes a navigational database that will be updated every 56 days. The Capstone installation limits the GX60 for VFR operation only. The GPS antenna is a low profile, low drag, active antenna previously certified with the GX60. The communication system will utilize the aircraft's existing audio and antenna interface. The GX60 Installation Manual, P/N 560-0959, provides detailed instructions on GPS installation and checkout. (Note the GX50, provided on a few Capstone aircraft, is equivalent to a GX60 without the communication transceiver and therefore is not described in this document.)

#### **4.2.2 MX20 Multi-Function Display**

The MX20 is a multi-function display capable of displaying ADS-B traffic, Flight Information Service, Moving Map, Terrain Awareness information, and VFR/IFR charting functions. The Capstone version of the MX20 display has an internal GPS receiver to provide timing and positioning for the UAT datalink. Further, the MX20 uses the internal GPS for ownship display. The GX60 will provide backup GPS position and flight plan information to the MX20. The MX20 Installation Manual, P/N 560-1025, provides detailed instructions on placement and installation.

### **4.2.3 UAT Radio and Antenna**

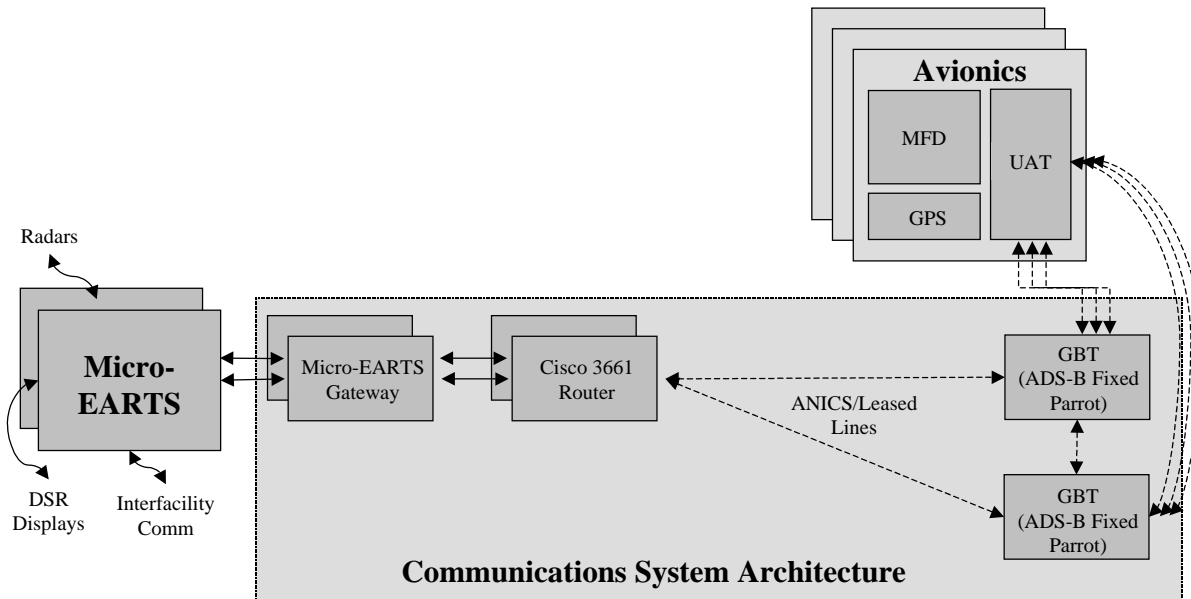
The UAT will transmit the ADS-B position reports as generated by the MX20 (via the internal GPS receiver). The transceiver will receive data from other aircraft as well as data transmitted by ground stations (i.e., Flight Information Service-Broadcast (FIS-B) and Traffic Information Service-Broadcast (TIS-B)) and transfer it to the MX20. The UAT antenna is a custom L-band antenna and is TSO-C66c certified. Dual antennas are installed to resolve shadows created from various mounting configurations. One antenna is top mounted, while the second antenna is bottom mounted. The Capstone System Installation Manual, P/N 560-1024-02, provides detailed instructions for the UAT radio installation.

### **4.2.4 Serial Altitude Encoder**

The serial altitude encoder will provide an RS232 altitude input to the GX60 and MX20. Trans Cal manufactures this serial encoder. This unit is certified to TSO-C88a and will have resolution of 10 feet to an altitude of 30,000 feet. The encoder selected will also have an extended environmental range to  $-55^{\circ}$  Celsius. This encoder also provides gray code output for use with transponders (100-foot resolution).

## **4.3 Capstone ADS-B Ground System Description**

The Capstone ADS-B Ground system includes a Lockheed Martin Micro-En Route Automated Radar Tracking System (Micro-EARTS) to process and display ADS-B information, and communication system architecture for transfer of information between remote sites and Anchorage Air Route Traffic Control Center (ARTCC). The communication architecture includes remotely located ADS-B Ground Broadcast Transceivers (GBTs), ADS-B fixed parrots, Alaskan NAS Interfacility Communications System (ANICS) and/or leased communication lines, and routers to the Micro-EARTS gateway (Figure 2). The Micro-EARTS will be certified through a NAS Change Proposal process (Capstone Case File NCP-AL512-MEARTS-013), that involves software changes to the currently certified Micro-EARTS baseline to incorporate processing of ADS-B data. The Capstone communications architecture must support surveillance (i.e., critical level) services in accordance with NAS performance requirements. Design goals for these requirements are specified in “NAS System Requirements Specification” (NAS-SR-1000). The Capstone ground system communication architecture will be tested via an FAA AOS-500/AAL-500/400 agreed upon process.



**Figure 2. Capstone ADS-B System Block Diagram**

For 1 January 2001, the Phase 1 ADS-B architecture only supports ADS-B messages to the Micro-EARTS as shown in Figure 2. A Capstone Communication Control Server (CCCS) when certified and installed between the Micro-EARTS gateway and routers will allow for an end-state architecture that also enables TIS-B and FIS-B. The Capstone end-state ground system architecture supports multiple services with emphasis on products (e.g., ADS-B, FIS-B, TIS-B) that meet the goals of the aviation community and the NAS. The ground system architecture will provide ADS-B information to the Micro-EARTS, and information such as text/graphical weather (i.e., FIS-B) and radar-tracked targets (i.e., TIS-B) will be broadcast to the aircraft. Traditionally these two functions are preformed by separate communications media and are classified critical (C) for surveillance and Essential (E) for weather/flight information. Given this architecture is designed to do both, the physical and logical architecture must support the highest criticality.

#### **4.3.1 Phase 1 ADS-B Architecture**

For Phase 1 certification the Micro-EARTS gateway will communicate directly with the Cisco 3661 router. This will provide the Micro-EARTS with the received ADS-B messages and allow the Micro-EARTS to attain ADS-B certification without waiting on the CCCS. Figure 2 gives a block diagram of this architecture.

A separate test system that incorporates the CCCS will communicate with a separate Cisco 3661 router and GBT for development of the client server applications. In this way, the CCCS and the CCCS software will continue certification with AOS-500 and AUA-640 for combined ADS-B and FIS-B/TIS-B services.

#### **4.3.2 System Performance Requirements**

The end-state Capstone ground communications is shared by the surveillance and weather/flight information communications services listed above. A system architecture, which meets the most

critical, will support the least. Of the services listed above the most critical is surveillance. Within the NAS-SR-1000 the surveillance system requirements and communications system requirements are defined separately. The connection between them is clear in NAS-SR-1000 paragraph 3.8.1 where the definitions of the service levels clearly relate surveillance to critical service. NAS-SR-1000 goes on to define design goals for the various levels of service in terms of availability and restoration. It also defines design goals for single point of failure and system reliability. In addition to the communications service requirements the communications system must also meet the needs of the surveillance system.

#### **4.3.2.1 Communications Service Level**

The NAS System Requirements have defined the communications service requirements in paragraph 3.8.1 of NAS-SR-1000 as follows.

- **Critical** Functions or services which, if lost, would prevent the NAS from exercising safe separation and control over aircraft.
- **Essential** Functions or services which, if lost, would reduce the capability of the NAS to exercise safe separation and control over aircraft.
- **Routine** Functions or services which, if lost, would not significantly degrade the capability of the NAS to exercise safe separation and control over aircraft.

The Capstone ground system is considered critical.

#### **4.3.2.2 Communications Availability**

As specified in NAS-SR-1000, the availability **goal** for a function or service to the user/specialist is expressed as the ratio of the total time the service is provided to the user/specialist to the maximum available operating time. Service availability shall not be less than that provided by existing capabilities. The availability goal for critical services is 0.99999. Capstone analysis estimates 0.99995 for the Capstone communication architecture, which is provided today by ANICS. Availability data will continue to be collected during operations.

#### **4.3.2.3 Single Point Failure**

No single failure of equipment, system, installation or facility shall cause loss of service to the user/specialist. The Capstone architecture redundancy is design to meet this requirement.

#### **4.3.2.4 Restoration**

The **goal** for a single loss of service to a user/specialist shall not exceed the duration of 6 seconds for critical services. Capstone meets this objective by having a dual GBT and communication line configuration, both continuously active, thus if one fails the other is an immediate backup.

#### **4.3.2.5 System Reliability**

The frequency of occurrence goal for any loss of service shall not exceed one per week. Capstone will monitor system reliability data through the normal airway facilities and maintenance control center (MCC) process.

#### **4.3.2.6 Surveillance Time Delay**

The NAS-SR-1000 paragraph 3.2.3.G.5 states the following:

The NAS terminal area surveillance response time, antenna boresight to display, which includes radar surveillance and data, shall be within 2.2 seconds. The NAS en route area surveillance response time, antenna boresight to display, which includes radar surveillance and data, shall be within 3.0 seconds.

The total time listed above is a complete budget for all detection, communication, processing and displaying functions. The UAT and on board GPS can take as much as 0.9 second of the total budget. A satellite communications system will require no less than 0.3 seconds for travel time, error correction algorithms and CCCS routing. The desired budget for these two parts of the process is 1 second or less. Estimates of the total time delay from aircraft to CCCS are 1.304 sec (System Architecture Description for Capstone Communications).

## **5 Analysis Approach and Methodology**

A Preliminary Hazard Analysis has been conducted using the methodology contained in MIL-STD-882D for End-to-End Safety Review. The CSSWG looked at potential accident scenarios from a Capstone-wide, top-down system point of view. During the first five months (Jan-May 2000) of the analysis process several telecons were conducted between the Alaska and “lower 48” portions of the CSSWG for familiarization on Alaska and Capstone operations and the system safety analysis process. During this period the “lower 48” team developed the initial PHA matrix. In May, members of the “lower 48” team conducted a status and initial review of the analysis on site in Alaska with the rest of the CSSWG. For the next 2 months (Jun-Jul 2000) the Alaska members of the CSSWG conducted a detail review of the PHA. Any changes introduced by Alaska were then reviewed by the “lower 48” team. Satisfied with the initial results and that the review process allowed the scenarios and controls to be discussed by the people/organizations implementing them, the next few months (Aug-Oct 2000) were used for further development and testing, while applying the controls. In November 2000, the CSSWG reviewed each control and listed a status of verification in the controls list (Volume 3).

In general, the approach was to hypothesize potential accidents given knowledge of the Capstone concept and Alaska flight operations. The CSSWG identified the potential accidents should failures, malfunctions, or human errors occur. The scenarios in Volume 2 include the scenario descriptions, risk, possible effects, and controls.

The CSSWG attempted to be as inclusive as possible in the identification of a potential system accident based on an “end-to-end” system scenario. Factors considered were:

- What are potential events within the Alaskan flight environment?
- What are the particular tasks of aircrew, controllers, and maintenance personnel for ADS-B radar-like services?
- What are the risks associated with such things as particular designs, latent design hazards, installation, maintenance of the system, logistics, reliability, availability, specific computer-human considerations?

## 5.1 Capstone System Safety Assumptions

The assumptions associated with the Capstone System Safety Program and PHA are discussed below.

- The higher risk scenarios are the result of a worst case analysis. The worst case harm has been estimated. Higher risk scenarios that are associated with high likelihood are considered most important.
- Without appropriate contingency, loss control, recovery, or damage control lower severity risks could develop into more severe risk.
- Scenarios represent potential accidents. Accident dynamics will vary from single events to many contributors. In the consideration of likelihood, if many contributors have to occur for the scenario to happen it is assumed that the likelihood of the scenario will decrease.
- The risk levels have been estimated for comparative risk ranking purposes only, in order to allocate risk control resources. The risk levels do not represent actual estimates of accident probability.
- Safety can imply freedom from all forms of harm, however this is not possible. In order to characterize safety, safety-related risks are hypothesized -- they are the scenarios defined within the PHA. Recommendations for precautions, hazard controls, and mitigation are identified in order to eliminate or control risk.
- Hazards are the potential for harm and many hazards can contribute to one accident. This analysis has been conducted at a high level in a scenario summary form. It considers that there may be many combinations of contributory hazards associated with the scenarios. It is not possible to provide all possible combinations of contributors. In order to eliminate or control these risks, high level recommendations, hazard controls, and precautions are provided.
- The Capstone system safety activities have been conducted on consensus bases in order to utilize the knowledge, expertise, and experience of the members of the CSSWG and other personnel involved in Capstone as needed.
- Any changes to the Capstone System Safety Program, analysis, or Safety Engineering Reports will be made upon concurrence of the CSSWG.
- It is expected that risk will increase should the recommendations, hazard controls, and precautions not be followed, or implemented.
- The Capstone system safety activities have been conducted in accordance with the practices defined within Mil-Std 882 D, Department of Defense Standard Practice for

System Safety; FAA Order 8040.4, Safety Risk Management; and the Draft FAA System Safety Handbook (April 2000).

- In order to accomplish the recommendations, hazard controls, and precautions, hazard tracking and risk resolution activity must be completed. The recommendations, hazard controls, and precautions must be formally implemented in the design or program. This effort must continue throughout the Capstone Program life cycle.
- The analysis is not all-inclusive in that there are unknown risks within any operation.
- In order to assure a successful Capstone System Safety Program, safety reviews must continue. A scenario by scenario review has been conducted.
- Future changes to the Capstone baseline system or program must be evaluated from a system safety view. The Capstone baseline has been defined within this Safety Engineering Report.
- The analysis is based upon the best engineering judgement and subjective logic has been applied to make conservative estimations of scenarios, risks, and mitigation.
- It is appropriate to apply an understanding of a “system accident” considering that accidents are the result of many contributors, both unsafe acts and/or conditions. The approach taken was not confined to a single failure and outcome, but considered the operation of Capstone that has been defined in the system description.
- The PHA matrix (Volume 2) has been designed to convey appropriate information related to a potential scenario, its worst case severity, and recommendations for precautions, controls, and mitigations. Scenarios were further refined into sub-scenario codes with hazard descriptions indicated. The scenario codes are defined below.
- Scenario Descriptions are short concise statements that define the basic scenario. The possible effect column indicates the worst-case harm expected. The Risk column indicates the worst-case severity and likelihood given the recommendations are implemented. R# column indicates the risk index code from Table 3. The Recommendations for Precautions, Controls and Mitigation column defines the risk controls to eliminate or reduce the associated risk.
- It is expected that the associated risks will be eliminated or controlled should appropriate implementation of the precautions, controls and mitigation’s occur. These precautions, controls and mitigations can be considered high-level system safety requirements.
- All current Federal Aviation Regulations, FAA Orders, safety practices, flight and ATC factors that are required in the current system apply to flying with Capstone equipment.

## 5.2 Capstone System Safety Requirements

The general engineering and administrative requirements for Capstone System Safety are described within the Capstone System Safety Program Plan. As the design and the preliminary hazard analysis matures specific system safety standards and requirements are to be developed by the program in concert with the CSSWG. The PHA indicates the controls for the identified risks. These controls are to be formally verified and validated. Every accepted mitigation, precaution, hazard control or risk control is to be formally incorporated into the design and/or administrative procedures. This effort involves hazard tracking and risk resolution.

### 5.2.1 Hazard Tracking and Risk Resolution

Hazard Tracking and Risk Resolution is a procedure to document and track risks, contributory hazards, and their associated controls by providing an audit trail of risk resolution that will be documented in the safety engineering report (Volume 3). The controls are to be formally verified and the specific risks and/or contributory hazards are to be closed during safety reviews.

### 5.2.2 Risk Assessment Measurement

The Capstone measurement for risk assessment is defined below (Tables 1, 2, 3). Risk is associated with a specific accident (event); it is an expression of the credible worst case severity and likelihood related to the scenario under study. Capstone program management, with input from the CSSWG, is to define acceptable risk levels. The CSSWG will define the current levels of risk without Capstone implementation, the transitional risks during implementation, and the residual risks after Capstone implementation and acceptance.

The definitions shown in the tables below are appropriate to support system hazard analysis activities, in that events can occur at any time considering possible exposure within the system life cycle. Consider events occurring on the ground, during maintenance, within a facility, within an individual aircraft, or between a number of aircraft. The PHA is conducted at a system level. The system considers interfaces and interactions of humans, hardware, software, firmware, and/or the environment.

**Table 1. Event Severity Definitions**

<b>Description</b>	<b>Category</b>	<b>Definition</b>
<i>Catastrophic</i>	I	Fatality, and/or system loss, and/or severe environmental damage, and/or collision with aircraft, and/or structure, and/or ground
<i>Critical</i>	II	Severe injury, severe occupational illness, major system, and/or environmental damage, and/or near midair collision, and / or service termination.
<i>Marginal</i>	III	Minor injury, minor occupational illness, and/or minor system damage, and/or environmental damage, and/or loss of separation of aircraft, and/or loss of communication single aircraft, and/or service interruption.
<i>Negligible</i>	IV	Less than minor injury, occupational illness, and/or less than minor system damage, and/or environmental damage



**Table 2. Event Likelihood**

<b>DESCRIPTION</b>	<b>LEVEL</b>	<b>CAPSTONE GROUND EQUIPMENT</b>	<b>CAPSTONE AIRCRAFT FLEET</b>
<i>Frequent</i>	<b>A</b>	Likely to occur frequently	Continuously experienced
<i>Reasonably Probable</i>	<b>B</b>	Will occur several times in the life of item	Will occur frequently
<i>Remote</i>	<b>C</b>	Likely to occur sometime in life of exposure	Will occur several times
<i>Extremely Remote</i>	<b>D</b>	Unlikely, but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
<i>Extremely Improbable</i>	<b>E</b>	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

**Notes:**

1. Event Likelihood is an estimation of the probability of a specific potential event under study, based upon best judgment.
2. Consider that potential events will have many contributors, i.e., human errors, software malfunctions, deviations, failures. The system reliability/availability approximation may only be a part of this overall estimation of the scenario likelihood. System risks can occur even with perfect system reliability and availability.
3. Consider worst case severity and likelihood, when evaluating system safety related risks.
4. A contributory hazard is the potential for harm, i.e., unsafe acts and/or unsafe conditions. Contributory hazards may be associated with the potential events under study.
5. The Risks associated with any changes within the system must be reevaluated.

**Table 3. Risk Assessment Code (R#)**

SEVERITY LEVEL	LIKELIHOOD OF OCCURRENCE				
	A Frequent	B Reasonably Probable	C Remote	D Extremely Remote	E Extremely Improbable
<b>I CATASTROPHIC</b> Collision, Fatality, System Loss, Severe Damage	IA	IB	IC	ID	IE
<b>II CRITICAL</b> NMAC, Severe Injury, Severe Illness, Major System Damage, Service Termination	IIA	IIB	IIC	IID	IIE
	IIIA	IIIB	IIIC	IIID	IIIE
<b>III MARGINAL</b> Loss of Separation, Minor Injury, Minor Illness, Minor System Damage, Loss of Comm (single aircraft), Service Interruption	IIIA	IIIB	IIIC	IIID	IIIE
<b>IV NEGLIGIBLE</b> Less Than Minor Injury or Illness, Less Than Minor System Damage	IVA	IVB	IVC	IVD	IVE
	IVA	IVB	IVC	IVD	IVE
<b><u>Risk Assessment Code</u></b>	<b><u>Criteria</u></b>				
<b>R1</b>	Risk must be eliminated or controlled to an acceptable level. Residual risk is extremely high, and additional mitigation will be required.				
<b>R2</b>	Risk is still considered very high because of the nature of Alaska operations. Risk must be controlled to an acceptable level.				
<b>R3</b>	Risk is considered moderate.				
<b>R4</b>	Risk is considered low.				
<b>R5</b>	Risk is considered very low.				

**5.2.3 Capstone System Safety Precedence**

The order of precedence for satisfying system safety requirements and resolving identified risks is defined in Table 4.

**Table 4. System Safety Precedence**

<b>Description</b>	<b>Priority</b>	<b>Definition</b>
<i>Design for minimum risk</i>	1	From the first design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.
<i>Incorporate safety devices</i>	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.
<i>Provide warning devices</i>	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.
<i>Develop procedures and training</i>	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.

## **6 Hazard Identification and Analysis**

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

### **6.1 Scenario Discussions**

Approximately 200 scenarios were developed, reviewed, and then culled down to 81 within this analysis and are listed in Volume 2. Through the review process, some scenarios and controls were added, removed, and/or combined; this accounts for the scenario and control numbering not being sequential and some missed numbers. Scenarios were also subdivided into scenario types for analysis purposes and discussion. Table 5 lists the scenario types along with definitions and scenario counts. Scenario Descriptions are short concise statements that define the basic scenario. The Possible Effect column indicates the worst-case harm expected. The Risk column indicates the worst-case severity and likelihood given the recommendations are implemented. The R# column indicates the risk index code from Table 3. The Recommendations for Precautions, Controls and Mitigation column defines the controls to eliminate or reduce the associated risk.

**Table 5. Scenario Subdivision**

<b>Scenario Type</b>	<b>Definition</b>	<b>Scenario Count</b>
<b>10</b>	<b><i>Human Factors</i></b>	9
11	Confusion	2
12	Inappropriate Use	6
13	Installation Error	5
14	Lack of Currency/Proficiency	2
15	Loss of Situational Awareness	5
16	Missed Communications	1
17	Erroneous Action	1
<b>20</b>	<b><i>Environmental</i></b>	6
<b>30</b>	<b><i>Ground System</i></b>	9
31	Calibration	5
32	Lost Communication	2
33	Malfunction	8
<b>40</b>	<b><i>Capstone Avionics Failure (Aircraft)</i></b>	14
41	GPS	3
<b>50</b>	<b><i>Weather</i></b>	+
51	Lack of Coverage	+
52	Limited Forecasts	+
53	Limited Reporting Stations	+
<b>60</b>	<b><i>Hazardous/Misleading/Erroneous Information</i></b>	*
61	Terrain/Obstacles	*
62	Traffic	*
63	System Malfunction	*
<b>70</b>	<b><i>Security</i></b>	*
71	Jamming	1
72	Spoofing	2
<b>80</b>	<b><i>Blind Spots/Masking</i></b>	*
<b>90</b>	<b><i>Future use</i></b>	+
* Covered under other Scenario Types + Reserved for future use (e.g., FIS-B, TIS-B)		

The matrix of scenarios in Volume 2 was considered for the end-to-end PHA. They follow a MIL-STD-882C/D methodology. The scenarios assume all current FARs, safety practices, flight and ATC factors that are required in the current system apply to flying with Capstone equipment. During the initial analysis process the CSSWG differentiated between IMC and VMC scenarios, but given severity level does not change, all scenarios should consider worse case being IMC operations. Note that the likelihood is generally less for VMC operations given the additional control “Pilot responsible for see-and-avoid in VMC” (Control 25b).

## 6.2 Preliminary Hazard Analysis

### 6.2.1 MIL-STD-882 Approach

Volume 2 contains the end-to-end system PHA matrix of scenarios based on a top-down end-to-end system approach as defined in MIL-STD-882. It contains a Scenario Description, Risk, Possible Effect, and Recommendations for Precautions, Controls and Mitigations, and a Comments column. Each recommended precaution, control or mitigation is given a unique control number. In many cases, the same control applies to several sub-scenarios. Volume 3 provides the list of Precautions, Controls and Mitigation and the current status. Review and closeout of these controls is ongoing.

### 6.2.2 Risk Assessment

Table 6 lists each scenario number categorized by risk assessment code (see Table 3). There were no R1 or R5 scenarios found in this analysis. R1s are very high risk and were eliminated by controls the standard air traffic control system and Capstone have in place. R5s are very low risk and the CSSWG did not spend much time reviewing this area. The most important scenarios for Capstone and the CSSWG to focus on are the R2 scenarios. These are considered very high risk because of the nature of Alaska operations and must be controlled to an acceptable level.

**Table 6. Risk Assessment Code per Scenario**

<b>Risk Assessment Code</b>	<b>Scenario Number</b>
<b>R1</b>	
<b>R2</b>	28, 29, 31, 32, 61a, 79, 91, 119
<b>R3</b>	1, 3, 7, 8, 11, 18, 35, 37, 42a, 42b, 44b, 55, 77a, 80a, 114, 129
<b>R4</b>	2, 4, 5, 6, 9, 10, 12, 13, 15, 16, 17, 19, 20, 21, 22, 24, 25, 26, 27, 30, 33, 34, 39, 44a, 47, 49, 51, 52, 53, 54, 60, 64, 65, 66, 67, 69, 70, 71a, 71b, 76, 77b, 78, 80b, 87, 88, 89, 93, 95, 97, 99, 108, 109, 116, 122, 126a, 126b, 128
<b>R5</b>	

Table 7 lists all the R2 scenarios with scenario description and possible effect as found in Volume 2. All Capstone R2 scenarios have a risk severity and likelihood of 1D (extremely remote catastrophic). The CSSWG concluded that the basic hazards in these scenarios (e.g., pilot loses situational awareness, inappropriate pilot operations, pilots not following procedures, and human error) exist in current Alaskan flight operations and that their current risk severity and likelihood is a 1C (remote catastrophic). With the introduction of Capstone avionics, procedures, and training the likelihood of these kinds of hazards is reduced (C-remote to a D-extremely remote). Therefore the R2 scenarios with indicated controls (Table 8) are controlled to an acceptable level, but efforts need to continue to further reduce their likelihood. For example, each operator having a defined internal safety program would help mitigate risk related to Alaska flight operations and make Capstone efforts more effective.

**Table 7. R2 Scenario Description and Possible Effect**

<b>Scenario #</b>	<b>Scenario Description</b>	<b>Possible Effect</b>
<b>28</b>	Pilot loses situational awareness due to excessive heads down time reading MFD.	Collision risk Loss of aircraft control
<b>29</b>	Pilot loses situational awareness due to less than adequate proficiency and/or currency.	Collision risk Loss of aircraft control
<b>31</b>	Inappropriate use of ADS-B. Pilots attempt aircraft to aircraft separation via MFD. Aircraft not under ATC separation.	Mid-air collision
<b>32</b>	Inappropriate use of ADS-B. Pilots attempt aircraft to aircraft separation via MFD. Possible increased collision risk between ADS-B and non-ADS-B aircraft. Only ADS-B targets displayed on MFD.	Mid-air collision
<b>61a</b>	Collision between ADS-B IFR aircraft with terrain/fixed object due to human error.	Collision risk
<b>79</b>	ADS-B Capstone pilots not following procedures.	Collision risk with terrain, other aircraft, ground equipment.
<b>91</b>	Inappropriate use of terrain function for surface or primary navigation results in collision	Collision risk
<b>119</b>	Pilot loses situational awareness due to excessive heads down time reading GX60.	Collision risk Loss of aircraft control

Table 8 lists the controls versus R2 scenarios in order of most used controls. The need for continued efforts in the area of pilot training and familiarization given the pilot-in-command has final responsibility for the safety of the aircraft is apparent in Table 8. This is also consistent with the order of precedence for satisfying system safety requirements (Table 4), which has “develop procedures and training” as the final mitigation. All Capstone pilots’ are to be appropriately trained and means to improve training and familiarization should be continued. Review of controller and maintenance training and procedures should also be continued. It should be noted that the R2 high-risk scenarios are not specific to ADS-B radar-like services. As mentioned earlier, these hazards are present in Alaskan flight operations and Capstone is helping to mitigate them. However, since they can occur during radar-like services, they are covered in this analysis.

The bulk of the scenarios specific to ADS-B radar-like services have worse case severity of near midair collision or loss of separation. These less severe outcomes are largely due to controls based on current enroute separation standards as well as current controller, pilot, and maintenance procedures and training. Standard controls that are already in place and proven combined with only an incremental change for ADS-B radar-like services reduces the risk of implementation.

**Table 8. Controls versus R2 Scenario**

Control # and Abbreviated Description	R2 Scenario Number							
	28	29	31	32	61a	79	91	119
25b Pilot ability to see-and-avoid in VMC	*	*	*	*	*	*	*	*
35a Pilot training/procedures	*	*	*	*	*	*	*	*
60 Human factors evaluation	*	*	*	*	*	*	*	*
5 Controller situational awareness	*	*		*	*	*	*	*
25a Pilot situational awareness			*	*	*	*	*	
7b Standard 7110.65 controller procedures				*	*	*	*	
8 ADS-B radar-like separation standard				*	*	*	*	
39a Avionics placarded			*	*		*	*	
39b Avionics placards checked			*	*		*	*	
57 Ensure pilot training defines appropriate and inappropriate use			*	*		*	*	
53 Pilot minimum proficiency requirements	*	*						*
16 Aircraft maintenance training/procedures					*		*	
17 Avionics certification/installation/approval	*							*
35b Pilot training					*		*	
41 Controller training/procedures					*		*	
42 Avionics design enhancements	*							*
64 Avionics database revision					*		*	
71 Review/validate terrain databases					*		*	
9 MFD enhanced pilot situational awareness					*			

## 7 Preliminary Controls/Requirements Recommendations

The following are general recommendations and findings from the CSSWG:

1. Precautions, controls, and mitigations generated by this analysis (Volume 3) should be implemented to ensure Capstone System Safety.
2. Controls should be reviewed approximately every 6 months and as the program changes to ensure their applicability and effectiveness as more information and operational experience is gained.
3. Efforts should continue in the area of pilot training and familiarization given the pilot-in-command has final responsibility for the safety of the aircraft. All Capstone pilots' are to be appropriately trained and means to improve training and familiarization should be continued.
4. Each operator having a defined internal safety program can help mitigate risk related to Alaska flight operations and make Capstone efforts more effective. Mechanisms outside of regulating a safety program should be explored to ensure operator acceptance (e.g., insurance benefits).
5. The MX20 multifunction display is an integral part of the Capstone system and is therefore considered in this PHA. It was considered due to possible coordination issues between the pilot and controller during radar-like services, as well as being used as a control in such cases as ground system failures (e.g., enhanced pilot situational awareness).
6. The accuracy, frequency, and reliability of Capstone ADS-B data has been verified by the Capstone ADS-B acceptability evaluation for ADS-B radar-like services. Consideration should be given in using ADS-B data for additional enhancements, such as ADS-B received altitude displayed with primary radar targets. The recommendation is to ensure the controller and the ground automation system can utilize best possible information.
7. The UAT Interim Design Specification requires that "navigation equipment independent of the avionics supporting Radar-Like Services must be retained." This is a recognized control in this analysis. Additional consideration needs be undertaken if the same avionics are to be used for both navigation and surveillance.
8. Based on PHA discussions, the most system "stressing" scenarios are when an ADS-B target and radar-target are being separated on fringe coverage areas. This is due to the compounding of potential errors and failures in both the ADS-B and radar systems.
9. Current barometric altimeter separation standards and procedures will be applied with the ADS-B altitude, given it is derived the same way as a Mode C altitude report (i.e., altitude encoder). There are known errors with barometric altitude and several scenarios



consider these errors. Future consideration should be made in using GPS geometric altitude as a crosscheck with the barometric altimeter data. Additional research and evaluation on implications may need to be accomplished, but this crosscheck could be an added control for altimeter errors.

10. Several scenarios consider separation of an ADS-B aircraft and a non-ADS-B aircraft in a non-radar environment. The primary control for this case is that if in a non-radar environment, current procedural separation rules are being applied, given one aircraft is not ADS-B equipped. There is no change to current operations. However, if new procedural separation rules are developed between ADS-B and non-ADS-B aircraft (e.g., ADS-B flight corridor), these scenarios need to be re-examined.
11. Controls based on current enroute separation standards as well as current controller, pilot, and maintenance procedures and training simplifies the introduction of Capstone ADS-B radar-like services. Standard controls that are already in place and proven combined with only an incremental change for ADS-B radar-like services reduces the risk of implementation. This philosophy should continue to be applied to other Capstone enhancements.
12. The Air Traffic Service Operational Readiness Review and Independent Office of Test and Evaluation (IOT&E) activities are considered an additional control to the ones listed in Volume 3 and should be continued.
13. The CSSWG concurs that based on the Preliminary Hazard Analysis conducted on Capstone ADS-B radar-like services, the identified safety-related risks are controlled to an acceptable level provided that the mitigations are implemented.

## **8 References and Bibliography**

The CSSWG or members of the CSSWG have reviewed each of the following documents. Listing of the following documents does not imply concurrence of contents from a system safety view.

### Ops Req Docs

- ADS-B MASPS DO-242 (RTCA)
- Capstone Program Plan v2.0 (<http://www.alaska.faa.gov/capstone/docs/docs.htm>)
- NTSB 1995 Alaska Safety Study (NTSB)
- RTCA Free Flight Select Committee Joint Gov/Industry Roadmap for Free Flight Operational Enhancements (RTCA)
- FAA Administrator's letter in support of 1 Jan radar-like services
- Various meeting minutes and e-mail distribution list (Jim Cieplak MITRE/CAASD)
- Alaska Sectionals and Approach plates

### Ops Procedures, Training, and Ops Approval

- DRAFT ATP Notice (Chris Metts ATP-110)
- DRAFT Pilot Ops Bulletin (Gary Childers AAL-1SC)

- ATP-1->AFS-400 request memo (19 Jul 2000), Separation Standards for the Use of ADS-B by ANC ARTCC (Jeff Griffith ATP-1)
- AFS-400->ATP- reply memo (20 Jul 2000), Separation Standards for the Use of ADS-B by ANC ARTCC (Bob Wright AFS-400)
- Note for AF procedures, training, approval – see maintenance manuals under certification procedures

#### Ops Concepts and TEMP

- Capstone Test and Evaluation Master Plan for ADS-B Radar-like Services (also contains concept of use from SF21) (<http://www.alaska.faa.gov/capstone/docs/docs.htm>)
- MEARTS Functional Description Narrative for ADS-B and WJHTC Acceptance Test Plan (Jack Neuberger AUA-600)
- 12 June Acceptance testing ADS-B accuracy memo (Neuberger AUA-600)
- NATCA local "evaluation" MOU w/ ADS-B Acceptability Evaluation Test Plan (Jack Neuberger AUA-600) and Capstone ADS-B Action Request System (Robin Badger ZAN)
- UAA Baseline report (Leonard Kirk Univ of Alaska <http://www.alaska.faa.gov/capstone/docs/docs.htm>)
- Initial Results Data Collection Effectiveness Pilot Comments and Interviewer Notes (Leonard Kirk Univ of Alaska)
- MEARTS Capstone April WJHTC Acceptance Test Report
- AUA-600 ADS-B Acceptability Report/testplan for Dec WJHTC testing

#### Certification Procedures

- Avionics STC and AFM
- Capstone UAT Interim Design Specification, Draft, May 18, 2000
- Ground-Based Transceiver Installation Manual, September 2000
- Capstone System Installation Instructions, Doc No. 560-1024-02
- Apollo GX60 Installation Instructions, Doc No. 560-0959-03
- Apollo MX20 Installation Instructions, Doc No. 560-1025-02
- Apollo GPS Antenna Installation Instructions, Doc No. 560-0949-01
- UAT Datalink Antenna Installation Instructions, Doc. No. 560-0215-01
- Altitude Encoder Installation Instructions, Doc No. 930005
- Capstone Installation Kit, Doc. No. 424-1004-000
- MX20 User's Guide Doc. No. 560-1026-00
- Apollo GX GPS User's Guide, Doc. No. 560-0961-02
- MX20 Multi-Function Display System Safety Assessment, Doc. No. PD1415
- Capstone "Radar-Like Services" Certification Plan, Doc. No. PD6000
- MEARTS Maintenance Manual (Jack Neuberger AUA-600)
- GBT Maintenance Manual (Hugh Barber, AAL-400)
- GBT Interim Requirements NOTICE AL N6360.1) (Hugh Barber AAL-400)
- Interim ADS Procedures – Certification, Restoration, and Logging (memo 18 Aug 2000) certification memos (Hugh Barber/Alan Falkenstein AAL-400)
- Spectrum analysis and agreement (Chris Moody MITRE/CAASD, Mike Biggs FAA Spectrum Office)

#### System Architecture Documents

- Capstone System Architecture Description (<http://www.alaska.faa.gov/at/510/>)
- Capstone Communication System Interface Control Document (<http://www.alaska.faa.gov/at/510/>)
- NAS –SR-1000, *System Requirements Specification*, November 1991

#### System Safety-Related Documents

- FAA Order 8040.4 *Safety Risk Assessment*, June 26, 1998
- MIL-STD-882 C and D, *System Safety: Standard Practice*
- FAA CT96/1 *Human Factors Design Guide*
- FAA *System Safety Handbook*