NASA/CR—2011-216325 SAA3–978–1

C-Band Airport Surface Communications System Engineering—Initial High-Level Safety Risk Assessment and Mitigation

Natalie Zelkin and Stephen Henriksen
ITT Corporation Advanced Engineering & Sciences Division, Herndon, Virginia

February 2011

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to *help@sti.nasa.gov*

- Fax your question to the NASA STI Help Desk at 443–757–5803

- Telephone the NASA STI Help Desk at 443–757–5802

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/CR—2011-216325 SAA3–978–1

C-Band Airport Surface Communications System Engineering—Initial High-Level Safety Risk Assessment and Mitigation

Natalie Zelkin and Stephen Henriksen
ITT Corporation Advanced Engineering & Sciences Division, Herndon, Virginia

Prepared under NNC05CA85C

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

February 2011

Level of Review: This material has been technically reviewed by expert reviewer(s).

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Available electronically at http://www.sti.nasa.gov

Preface

This National Aeronautics and Space Administration (NASA) Contractor Report summarizes and documents the work performed to develop concepts of use (ConUse), System Requirements and Architecture for the proposed L-band (960 to 1164 MHz) terrestrial en route communications system.

This work was completed under a NASA project-level agreement (PLA FY09_G1M.02-02v1) for "New ATM Requirements—Future Communications" in support of a Federal Aviation Administration (FAA)/European Organisation for the Safety of Air Navigation (EUROCONTROL) Cooperative Research Agreement (Action Plan 17 (AP–17)), commonly referred to as the Future Communications Study. The work was performed with the guidance of the FAA and NASA.

Executive Summary

A safety hazard analysis was completed providing a preliminary safety assessment for the proposed C-band communication system. The assessment was performed following the guidelines outlined in the Federal Aviation Administration (FAA) Safety Risk Management Guidance for System Acquisitions document (Ref. 1).

Safety analysis did not identify any hazards with an unacceptable risk, though a number of hazards with a medium risk were documented.

This effort represents an initial high-level safety hazard analysis. Section 3.6 details recommended triggers for risk reassessment. A detailed safety hazards analysis should be performed as a follow-on activity to assess particular components of the C-band communication system after the profile is finalized and system rollout timing is determined.

A security risk assessment has been performed by NASA as a parallel activity. Although safety analysis is concerned with a prevention of accidental errors and failures, the security threat analysis focuses on deliberate attacks. Both processes identify the events that affect operation of the system; from a safety perspective, the security threats may present safety risks.

Contents

List of Figures

List of Tables

1.0 Introduction

1.1 Background

During the past 4 years, NASA Glenn Research Center and ITT have conducted a three-phase technology assessment for the Federal Aviation Administration (FAA) under the joint FAA–European Organisation for the Safety of Air Navigation (EUROCONTROL) Cooperative Research Action Plan (AP–17), also known as the Future Communications Study (FCS). NASA/ITT provided a system engineering evaluation of candidate technologies for the future communications infrastructure (FCI) to be used in air traffic management (ATM). Specific recommendations for data communications technologies in very high frequency (VHF), C-, L-, and satellite bands, and a set of follow-on research and implementation actions have been endorsed by the FAA, EUROCONTROL, and the International Civil Aviation Organization (ICAO). In the United States, the recommendations from AP–17 are reflected in the Joint Planning and Development Office's (JPDO) "Next Generation Air Transportation System (NextGen) Integrated Work Plan" (Ref. X) and are represented in the "National Airspace System (NAS) Enterprise Architecture Communications and Avionics Roadmaps" (Ref X).

Action Plan 30 (AP–30), a follow-on cooperative research action plan to AP–17, is expected to start in fiscal year 2010 (FY10) to ensure coordinated development of FCI to help enable the advanced ATM concepts of operation (ConOps) envisioned for both NextGen in the United States and for EUROCONTROL's Single European Systems ATM Research (SESAR) program in Europe. Follow-on research and technology development recommended by NASA Glenn and endorsed by the FAA was included in the FAA's NextGen Implementation Plan 2009. The plan was officially released at http://www.faa.gov/about/initiatives/nextgen/ on January 30, 2009. The implementation plan includes a FY09 solution set work plan for C-band and L-band future communications research under the section, "New Air Traffic Management (ATM) Requirements."

On February 27, 2009, the FAA approved a project-level agreement (PLA) (PLA FY09_G1M.02-02v1) for "New ATM Requirements—Future Communications," to perform the FY09 portion of the FAA's solution-set work plan; this includes development of concepts of use (ConUse), requirements, and architecture for both a new C-band airport surface wireless communications system and a new L-band terrestrial en route communications system.

As required under the PLA, this report presents the initial high-level safety risk assessment for C-band communications systems. The assessment draws on the functional system analysis conducted in parallel and documented in the C-band airport surface communications system standards development deliverable.

The future airport surface communications network is based on the IEEE 802.16e standard and is envisioned to support future mobile and fixed data communication applications and services for both ground-to-air (G/A) and ground-to-ground (G/G) communication services on the airport surface. Examples include information exchanges to support collaborative decision making (CDM), surveillance broadcast system (SBS) applications, and System Wide Information Management (SWIM) data exchanges and its extension to aircraft (SWIM-Air), which includes aeronautical and metrological data link services. A mobile local area network (LAN) on the airport surface may also include fixed elements.

A number of nonaircraft mobile systems on the aircraft movement area (e.g., service and emergency vehicles use, and snow plow operations) could also use the C-band system to exchange information between and among aircraft, vehicles, and ground control operators.

Other future communications applications may include unmanned aircraft system (UAS) data communications.

Safety hazards identification, analysis, and assessment are performed assuming the services identified as potential applications for the C-band (5091 to 5150 MHz) system (Ref. 2). Recommendations for safety risk mitigation techniques follow the analysis.

Safety hazards analyses rely on FAA guidance documents, such as the NAS System Engineering Manual, the Safety Management System Manual (SMS), and the System Safety Handbook (SSH) for methodology and process.

1.2 Document Overview

This document is organized as follows:

- Section 1.0 includes background system development information as well as document organization and references.
- Section 2.0 describes the scope of the document.
- Section 3.0 describes methodology and presents the results of safety risk analysis.
- Appendix A provides an acronyms and abbreviations list.
- Appendix B presents hierarchical diagrams of functional requirements for the proposed C-band communications system.
- Appendix C contains C-band communications system safety hazards analysis worksheets showing the supporting work detail.
- Appendix D presents a summary of the operational safety assessment for the ATS services identified for C-band application adopted from the analysis presented in the COCR.
- Appendix E lists the existing NAS communications system safety controls.

2.0 Scope

2.1 Risk Management Objective

The goal of risk management is to ensure that new system development and integration meet or exceed FAA safety standards that support the FAA's core mission of ensuring the safety of the flying public. The objective of this document is to identify risks in the proposed C-band communication system from a safety viewpoint.

Figure 1 shows how risk management fits into the overall FAA NAS systems engineering process.

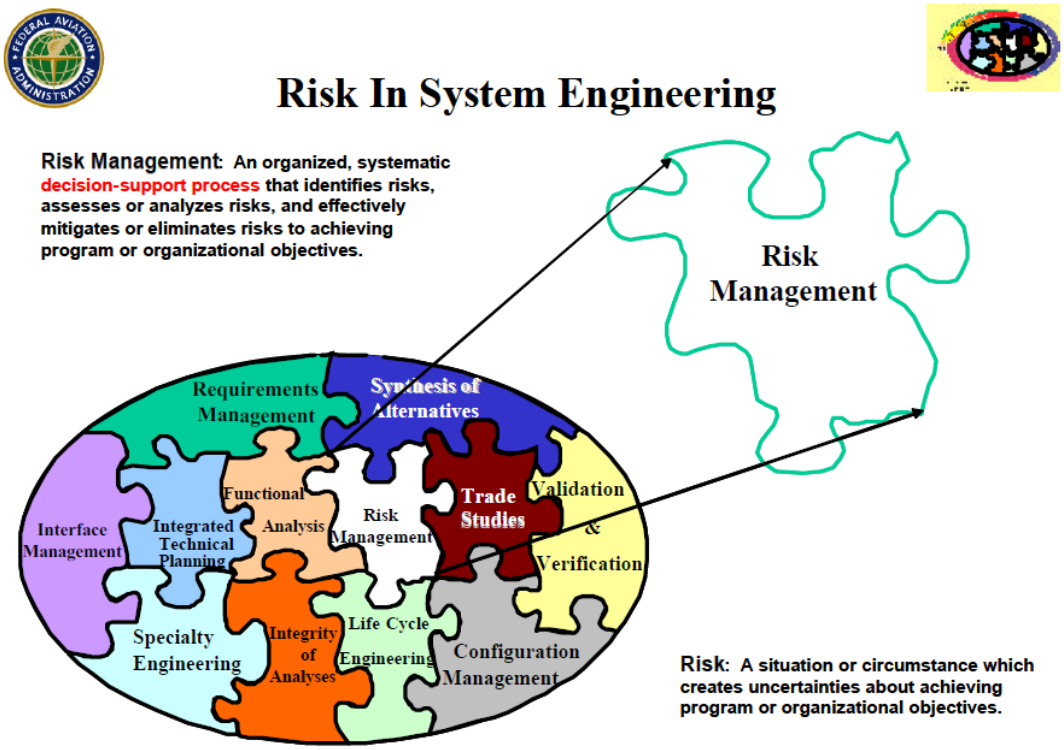

Figure 1.—Risk in system engineering (from Ref. 3).

Although risk management is depicted as a separate system engineering task, as with most processes, it is closely intertwined with the other key elements. For example, as shown further in this report, functional requirements resulting from the functional analysis process become the basis for the safety hazard and security threat analyses. Furthermore, the safety engineering (a discipline within specialty engineering) and risk management processes are both applied to perform a safety assessment for the system (Ref. 3).

Within the opportunity-risk paradigm, the fundamental objective of the risk management process is to identify and analyze uncertainties of achieving program or organizational objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

This process is applied to ensure that a program or organization meets technical, schedule, and cost commitments, delivers a product or service that satisfies all stakeholders' lifecycle needs, and provides the expected benefit. Four lower-level objectives are established as part of the overall objective:

- Timely identification of risks (identifying a potential problem with sufficient lead time so that the team may implement appropriate alternate plans)
- Consistent assessment of the level of risk across a program (providing a structured decision making framework for prioritizing resource application)
- Communication of risk mitigation actions across the program or organization (ensuring that all elements of the program or organization are aligned in resolving risks)
- Review of risk mitigation action performance

Positive impacts on a plan or favorable consequences are not considered in this document in accordance with the FAA risk identification and analysis process guidance that treats them as opportunities (Ref. 3). Rather "in the context of the SMS, safety is defined as freedom from unacceptable risk" (Ref. 4).

2.2 Types of Identified Risks

Various types of risks may be identified during the course of system development. As illustrated by Figure 2, high-level risks can be categorized as technical, schedule, or business and cost-related risks.

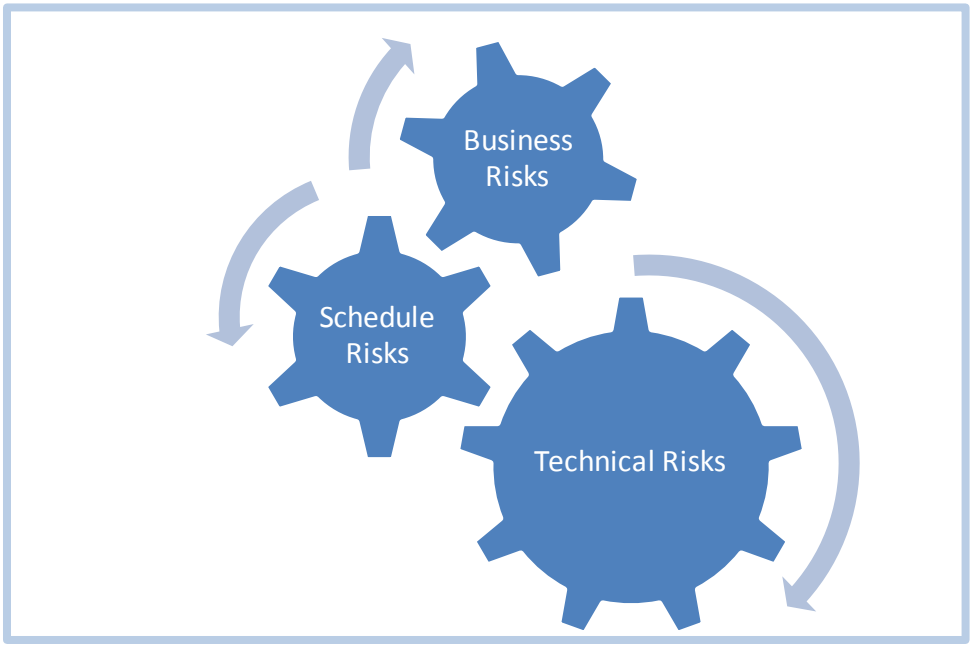

Figure 2.—Types of potential risks.

As explained in the NAS System Engineering Manual (SEM) (Ref. 3):

> Many sources must be considered for each risk area. For technical risk, likely sources include technology maturity, complexity, dependency, stakeholder uncertainty, requirements uncertainty, and testing/verification failure. Sources of schedule risks may include incomplete identification of tasks, time-based schedule (as opposed to event-based schedule), critical-path scheduling anomalies, competitive optimism, unrealistic requirements, and material availability shortfalls. Cost risks may stem from an uncertain number of production units, supplier optimism, additional complexity, change in economic conditions, competitive environment, supplier viability, and lack of applicable historical data.

Although the three types of risks are interrelated, this document will focus on technical risks only. Schedule and business risks are considered out of scope for this task and would significantly depend on system acquisition plan and schedule. Factors such as technology advancement and WiMAX profile development schedule, business plans, and further service selections could contribute to program risks and should be addressed elsewhere. It should also be noted that these nontechnical factors may affect technical risks. As such, this document presents an initial safety assessment only, and a safety analysis encompassing all three risk types should be revisited at a later stage.

Only safety risks are addressed for this assessment. Also out of scope for this analysis are the hazards attributable to a controller, pilot, or automation, Occupational Safety and Health Administration (OSHA) hazards, and all hazards not directly related to fixed-to-mobile and fixed-to-fixed communications, such as navigation systems and surveillance systems. Security risks are addressed in a separate document being prepared by NASA.

Finalizing the C-band data link profile will determine if any commercial off-the-shelf (COTS) products are used. The risk assessment should be revisited and hazards associated with the use of COTS should be evaluated at that time as appropriate. COTS-based risks identified in the SEM (Ref. 3) should be used as a starting point for that assessment.

2.3 System Safety Engineering

A type of specialty engineering (SE)—system safety engineering (SSE)—is applied to conduct the analysis described by this document.

It should be noted that another SE discipline, electromagnetic environmental effects (E3), is related to safety risk assessment but is better addressed with other interference issues. The risks of interference problems should be detailed and investigated, and should involve (Ref. 3)

> …system analysis for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and implement methods for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E3 consists of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC).
>
> The results [should then be] used to derive, validate, and verify requirements; evaluate system design progress and technical soundness; and manage risk.

SE analyses performed under this task are intended to aid in identifying and assessing potential operational problems early in the process and help shape system requirements. The results are fed into the risk management process for risk mitigation and control.

Safety and security risk identification, assessment, and mitigation for the C-band system are being addressed separately. A security risk assessment is performed by NASA as a parallel activity. The safety analysis is concerned with prevention of accidental errors and failures; the security threat analysis focuses on deliberate attacks. At the same time, both processes identify the events that affect operation of the system and are interrelated. Also, “From a safety perspective, the threats that concern security are another potential cause of safety hazards, while from a security perspective; the hazards that concern safety are another potential outcome of security threats” (Ref. 5). The relationship between the outcomes of the two analyses should be addressed when both are complete.

3.0 Safety Risks Management

3.1 Safety Analysis Requirement

The need for a safety analysis is driven by the FAA categorization of changes requiring safety analysis.

Table 1 depicts system changes recognized as those that need to be evaluated for safety risk (Ref. 4) and identifies the changes applicable to the proposed introduction of a C-band system.

TABLE 1.—CHANGES REQUIRING SAFETY ANALYSIS

Categories of change		Changes applicable to C-band system?
Airspace changes that impact safety	Reorganization of air traffic route structure	No
	Resectorization of an airspace	No
Changes to air traffic procedures and standards that impact safety	Reduced separation minima applied to airspace	No
	New operating procedures, including departure, arrival, and approach procedures	Yes
	Waivers to existing procedures, requirements, or standards	No
Changes to airport procedures and standards that impact safety	Reduced separation minima applied at an airport	No
	Physical changes to airport runways, taxiways, or the airport operations area	Yes
Changes to equipment that impact safety	Introduction of new equipment, systems (hardware and software) that impact safety, human-to-system interfaces, or facilities used in providing air traffic control (ATC) and navigation services	Yes
	Modifications to systems (hardware and software), maintenance activities associated with those systems, human-to-system interfaces, or facilities used in providing ATC and navigation services	

3.2 Process

The analyses described in this document adhere to the SSE methodology and involve "evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, and safety risk assessments and in hazard tracking and control (Ref. 3). It is anticipated that the approach adopted in this task will allow incorporation of suitable safety features in the system design with minimal cost and schedule impact.

Figure 3 shows the inputs to the safety risk management (SRM) process performed for this task, noting the documents used for guidance.

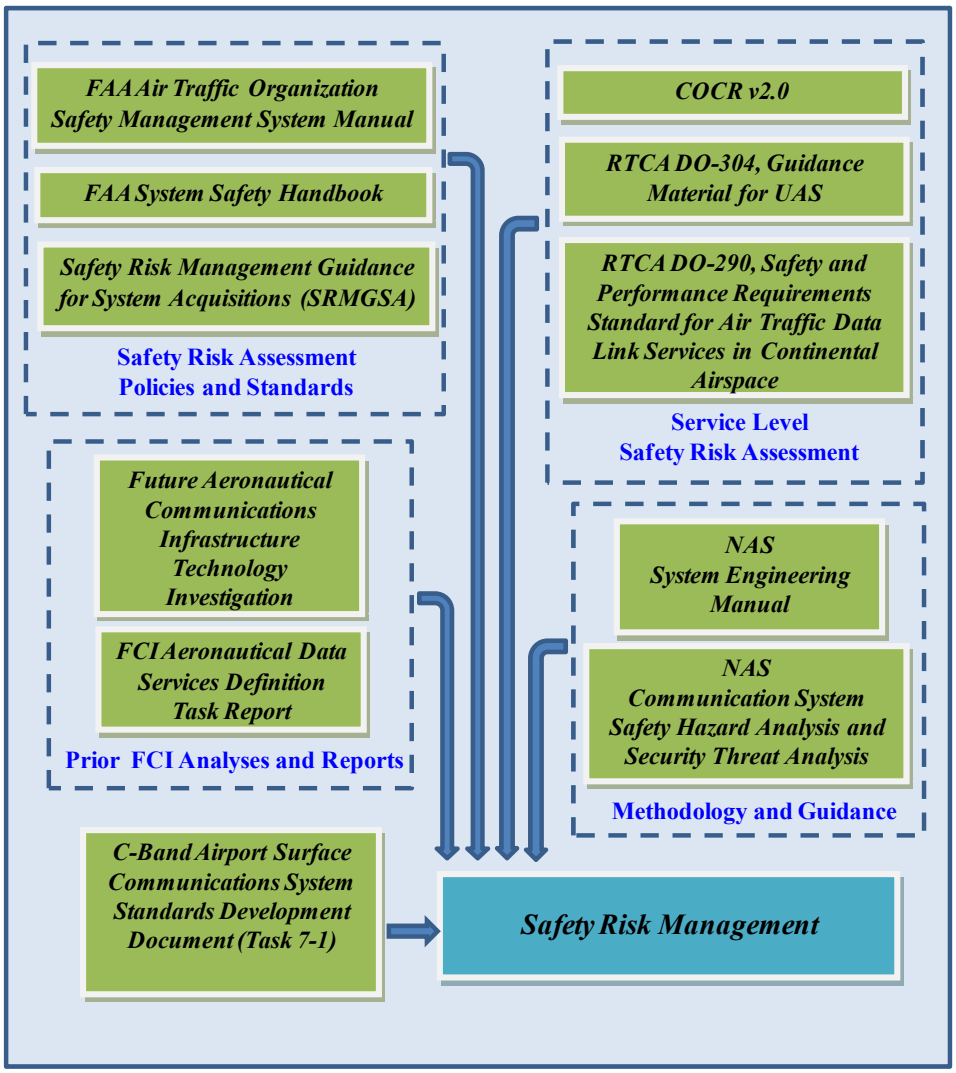

Figure 3.—Safety risks management, inputs to the process. (Acronyms defined in Appendix A.)

As depicted on Figure 4, the systematic SRM process applied for this task proceeded through five general phases (Ref. 4).

Figure 4.—Safety risk management process.

Using the NAS SEM for guidance, the decision flow chart detailing how the process was implemented is shown in Figure 5. The following sections of this report describe the results of the activities conducted to implement this process.

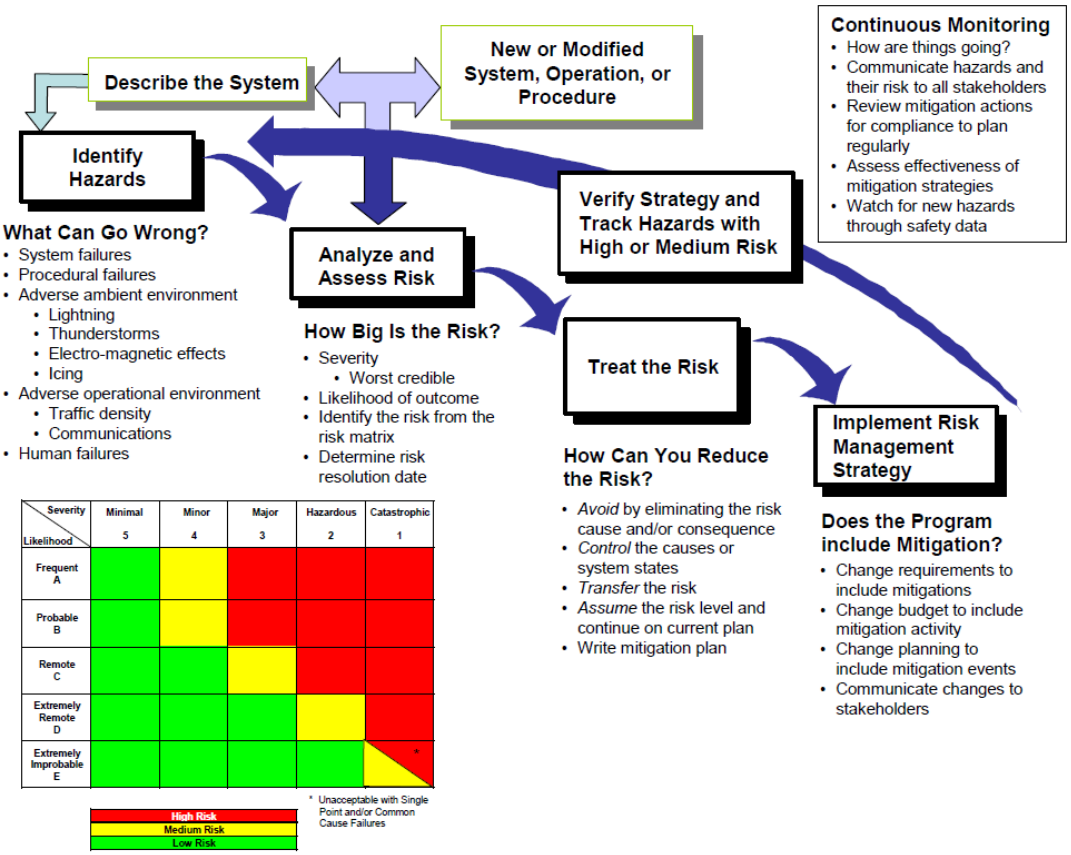

Figure 5.—Safety risk management decision flow chart (Ref. 4).

3.3 System Description

Accurate system description is the first step in a safety hazards analysis. As noted in the C-band airport surface communications system standards development document (Ref. 6) that details ConUse for the proposed system, an AeroMACS,[1] the system covered by this document, will provide air-to-ground (A/G) and ground-to-ground (G/G) communications services on the airport surface.

Figure 6 depicts an end-to-end communications system supporting air traffic services (ATS). On the ground, these systems typically consist of radio ground station subsystems, including radios, antennas, cabling, power systems, environmental systems, towers, and monitoring and control (M&C) functionality, to provide A/G communications services; networking subsystems to provide G/G communications service connectivity to endsystems and endusers; and usually some centralized M&C functionality to monitor and control system operations and performance.

[1]AeroMACS is a proposed term for the C-band airport surface communication technology based on the IEEE 802.16e standard.

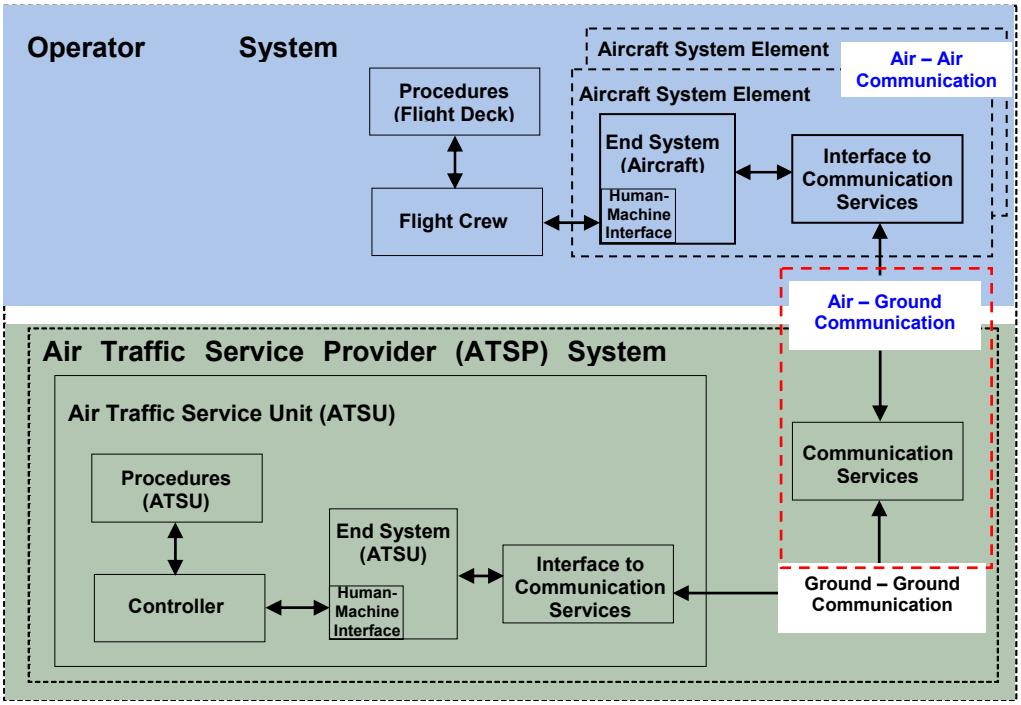

Figure 6.—Communications systems covered by this document (slightly altered Figure 1-1 from Ref. 7).

A number of nonaircraft mobile systems for use on the aircraft movement area (e.g., service and emergency vehicles or snow plow operations) could also use the C-band system to exchange information between and among aircraft, vehicles, and ground control operators.

Finally, and perhaps as an early implementation, a new C-band airport surface mobile LAN is expected to be used for fixed point-to-point applications on the airport surface.

It should be noted that although Figure 6 effectively illustrates different types of communications provided by the proposed C-band system (G/G and A/G), it depicts air traffic service provider (ATSP) systems only.[2]

The C-band communication system safety hazard analysis is based on a C-band system functional analysis. This analysis is detailed in the C-band airport surface communications system standards development document (Ref. 6). Appendix B of this report contains hierarchical diagrams of the functional requirements for the proposed C-band system. The functional breakdown and methodology are adopted from the NAS Communication System Safety Hazard Analysis and Security Threat Analysis (Ref. 5) and modified as appropriate to reflect the scope and requirements for the proposed C-band system.

At a high level, the following communication system functions were identified:

- Use the communication system to send and/or receive messages
  - transceive fixed-to-mobile message
  - transceive mobile-to-fixed message
  - transceive fixed-to-fixed message
- Provide the C-band communication system, including
  - monitor the C-band communication system
  - maintain the C-band communication system
  - configure the C-band communication system

[2]ATSP presents a subset of a broader Air Navigation Service Providers (ANSP) category that in addition to ATSP may encompass Aeronautical Information Services (AIS) providers, communication, navigation, and surveillance CNS providers, meteorological office services (METS) providers, and include Airport/Aerodrome Flight Information Service (AFIS) providers.

Though the proposed C-band could enable ATS, aeronautical (airline) operational control (AOC), and aeronautical administrative communication (AAC), ATS are likely to have the strictest safety and security requirements. As such, this document considers ATS to be the worst case scenario from the safety viewpoint.

3.4 Safety Risk Identification

Figure 7 shows the risk management risk identification process recommended by the FAA.

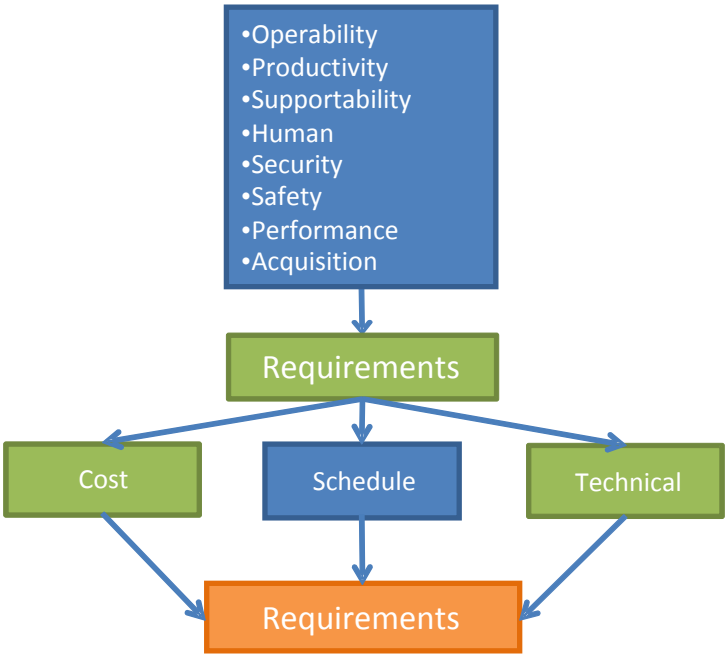

Figure 7.—Federal Aviation Administration risk management risk identification flow chart (Ref. 6).

Although multiple factors contribute to the overall program and system risks, the scope of this document is limited to safety issues. Security risks are addressed in a separate document.

To identify potential safety hazards for the proposed C-band system, the hazards present in the current NAS Communications System were reviewed first. The safety hazards identified in the NAS Safety Hazard Analysis (Ref. 5) were found to be applicable to the proposed C-band system, and Table 2 shoes the safety hazard categories. Table 2 is decomposed into lower level hazards.

TABLE 2.—SAFETY HAZARDS CATEGORIES

Safety hazards categories	Safety hazards
Hazards due to lack of availability of the C-band communication system	C-band communication capability totally unavailable: C-band air traffic services (ATS) failure
	C-band communication capability partially unavailable: C-band ATS failure
	C-band system communication capability unavailable: Sender to recipient of C-band ATS unavailable
Hazards due to failures of the C-band communication system	C-band communication fails (e.g., aborts) with a given recipient for a single message.
	C-band communication fails (e.g., aborts) with multiple recipients for a single message per aircraft.
Hazards due to misdelivery of a message by the C-band communication system	The recipient accepts a message affecting separation from an C-band ATS that is not its control authority.
	The recipient accepts a message NOT affecting separation from a C-band ATS that is its control authority.
	A message affecting separation gets to unintended recipient.
	A message NOT affecting separation gets to unintended recipient
Hazards due to late delivery of a message by the C-band communication system	Message affecting separation received too late (or expired)
	Message NOT affecting separation received too late (or expired)
Hazards due to corruption of message by the C-band communication system	A message affecting separation corrupted
	A message NOT affecting separation corrupted
Hazards due to messages arriving out-of-sequence due to the C-band communication system	A message affecting separation sent/received out of sequence
	A message NOT affecting separation sent/received out of sequence

These 15 hazard categories were then applied to each of the high-level C-band communication system functions shown in Figure 8.

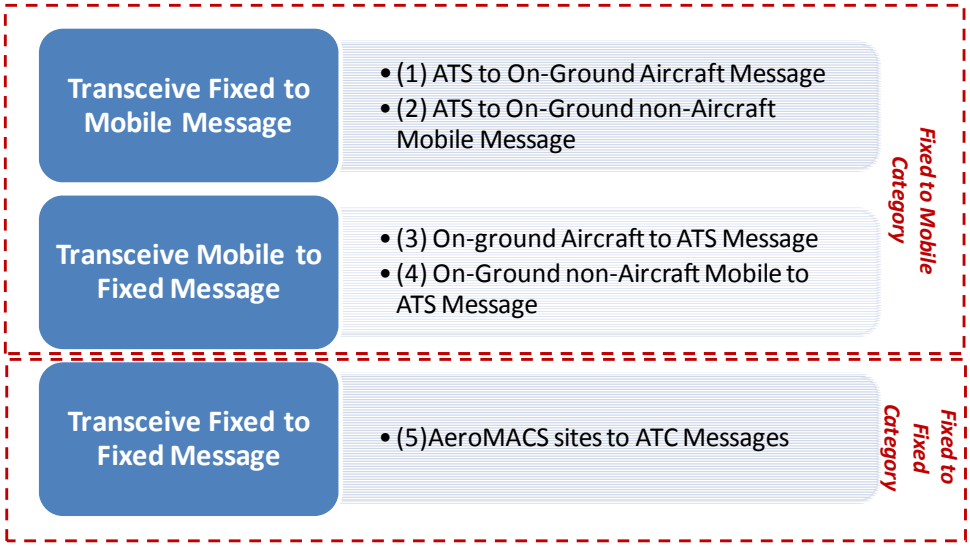

Figure 8.—Functional hazard categories. (Acronyms are defined in Appendix A.)

Following the methodology suggested in Reference 5, fixed-to-mobile and mobile-to-fixed messages transmission functions were combined into one category for safety hazards analysis. Fixed-to-fixed transmissions hazards are shown in the second hazard category.

Based on this functional categorization of 15 hazard categories applied to each of the two functional categories, 30 C-band communication system safety hazards were identified. Details of the identified hazards and the safety causes of each hazard are presented in Appendix C.

3.5 Safety Risks Analysis and Assesment

Once again, it is useful to borrow from the NAS SEM (Ref. 3) to define the term risk.

> "A risk has three aspects: (1) the event is in the future, (2) the likelihood/probability that an event will occur (a degree of uncertainty), and (3) a negative or unfavorable consequence/impact if it occurs"

Safety risk analysis is the third step in the SRM process. For each of the identified C-band communication system safety hazards (summarized in Table 2 and detailed in Appendix C) the following process was followed (Ref. 5):

> [T]he severity of consequence (i.e., what is the worst thing that can credibly happen) was determined. This was done by determining a system state for each hazard that could lead to the worst credible effect occurring and then tracing a scenario(s) that could result should the hazard occur.

The system state leading to the worst credible effect (WCE) is the same for all hazards because of the C-band communication system, including

- Heavy traffic conditions
- Instrument meteorological conditions (IMCs)
- Adverse weather conditions

Causes of identified hazards include

- Hardware failure
- Software failure
- Insufficient capacity
- Radiofrequency (RF) interference

3.5.1 Hazard Severity Definition and Safety Likelihood Categories

Table 3 outlines hazard effects and the standardized classification scheme used to describe the severity of safety hazards as presented in the COCR Version 2.0 document (Ref. 8). It, in turn, is based on the FAA's Safety Management System Manual (Ref. 4) severity and likelihood definitions and EUROCONTROL's Safety Regulatory Requirement (ESARR 4) Set 1 Severity Indicators.

TABLE 3.—DESCRIPTION OF HAZARD SEVERITY (REF. 8)

Effect on	Hazard class				
	5, No safety effect (NO)	4, Minor (MN)	3, Major (MJ)	2, Hazardous (HZ)	1, Catastrophic (CS)
General		Does not significantly reduce system safety. Required actions are within operator's capabilities. Includes the ATC and flying public items.	Reduces the capability of the system or operators to cope with adverse operating conditions to the extent that:	Reduces the capability of the system or operators to cope with adverse operating conditions to the extent that:	Total loss of system control such that:
Air traffic control (ATC)	Slight increase in ATC workload	Slight reduction in ATC capability or significant increase in ATC workload.	Reduction in separation as defined by low- to moderate-severity operational error or a significant reduction in ATC capability.	Reduction in separation as defined by a high-severity operation error, or a total loss of ATC.	Collisions with other aircraft, obstacles, or terrain
Flying public	No effect on flight crew No safety effect Inconvenience	Slight increase in workload Slight reduction in safety margin or functional capabilities Minor illness or damage Some physical discomfort	Significant increase in flight crew workload Significant reduction in safety margin or functional capabilities Major illness, injury, or damage Physical distress	Large reduction in safety margin or functional capability Serious or fatal injury to a small number Physical distress or excessive workload	Outcome would result in: Hull loss Multiple fatalities

Following the methodology described in the NAS Communication System Hazard Analysis and Security Threat Analysis (Ref. 5) as well as in the COCR Version 2.0 (Ref. 8), this safety analysis was limited to hazards caused by C-band communication system failures; hazards due to the controller, and the flight crew outside of the communication link portion of a system and/or service were considered out of scope.

Definitions of safety likelihood categories qualifying and quantifying the degree of tolerance for each category are shown in Table 4. The likelihood of occurrence of the WCE for each of the identified hazards is presented in the hazard analysis worksheets in Appendix C.

TABLE 4.—SAFETY LIKELIHOOD CATEGORIES[a]

Category		Qualitative[b,c]	Quantitative[d]
A	Frequent	Expected to occur frequently for an item	Probability of occurrence per operation/operational hour is equal to or greater than 1×10^{-3}
B	Probable	Expected to occur several times in the life of an item	Probability of occurrence per operation/operational hour is less than 1×10^{-3}, but equal to or greater than 1×10^{-5}
C	Remote	Expected to occur sometime in the lifecycle of an item	Probability of occurrence per operation/ operational hour is less than 1×10^{-5} but equal to or greater than 1×10^{-7}
D	Extremely remote	Unlikely but possible to occur in an item's lifecycle	Probability of occurrence per operation/operational hour is less than 1×10^{-7} but equal to or greater than 1×10^{-9}
E	Extremely improbable	So unlikely, it can be assumed that it will not occur in an item's lifecycle	Probability of occurrence per operation/operational hour is less than 1×10^{-9}

[a]Adopted from Reference 1. Only part of the table found relevant to this analysis is presented.
[b]Qualitative definition for individual item/system as defined in SRMGSA is used. The definition excludes ATC service/NAS level system (assumes NAS-wide occurrence is an order of magnitude greater than an individual item/system), flight procedures, and operational definitions.
[c]These qualitative definitions differ from the definitions used in the existing NAS System Safety Risk Analysis.
[d]Assumes operation 24 hr/day each day of the year or approximately 8000 hr/yr for a single item/system.

Hazard severity and safety likelihood definitions used in this document are the same and/or similar to those used in the NAS Communication System Hazard Analysis and Security Threat Analysis (Ref. 5) for the existing system as well as the COCR Version 2.0 (Ref. 8) as applied to individual services (described later in this report). They, in turn, are based on the recommendations provided in the Safety Risk Management Guidance for System Acquisitions document (Ref. 1).[3]

3.5.2 C-Band System Safety Risks Matrix

Finally, risk was determined for each C-band communication system hazard using its severity and likelihood values. A summary of the risk associated with each of the 30 hazards identified for the C-band communication system is shown in Table 5 and detailed in the hazard worksheets in Appendix C. Figure 9 and Figure 10 present the findings in the "stop-light" matrix format.

Safety risk likelihood and severity were determined by mapping the results of the operational safety assessments for the ATS documented in COCR to the C-band system safety hazards. A summary of the safety assessment for the subset of services applicable to the C-band system is presented in Appendix D. It should be noted that for the assessment, when more than one category of services is potentially affected by a safety hazard, the most severe hazard assessment is applied.

The COCR identifies two phases of implementation of operational service capabilities. The first phase is based on existing or emerging data communications services and is scheduled to be completed around 2020. Initial steps under this phase are currently being implemented, for example, as part of the FAA Data Communications Program. During the second phase, data communications is expected to become the primary means of A/G communication supporting increased automation in the aircraft and on the ground.

Although the C-band system could to be introduced prior to the start of the second phase of the future communications infrastructure implementation, Phase II system requirements and constraints are more conservative. As such, only the Phase II COCR data is adopted for the table below.

Data communications is a primary objective for the proposed system; digital voice may be considered in the future set of capabilities.

TABLE 5.—C-BAND COMMUNICATIONS SYSTEM SAFETY RISK SUMMARY

Safety hazards	Safety risk likelihood and severity[a]	
	Exist. NAS	C-band FCS[b,c]
1. Communication capability totally unavailable: ATS failure[d]	3D	3D
2. Communication capability partially unavailable: ATS failure	3D	3C[e]
3. System communication capability unavailable—Sender to recipient of ATS unavailable	4D	4C
4. Communication fails (e.g., aborts) with a given recipient for a single message	4C	4B[f]
5. Communication fails (e.g., aborts) with multiple recipients for a single message per aircraft	4C	3C[g]
6. The recipient accepts a message affecting separation from an ATS system that is not its control authority	2D	2D
7. The recipient accepts a message NOT affecting separation from an ATS system that is its control authority	5	5D
8. A message affecting separation gets to unintended recipient	2D	2D
9. A message NOT affecting separation gets to unintended recipient	5	5D
10. Message affecting separation received too late (or expired)	2D	2D
11. Message NOT affecting separation received too late (or expired)	5	5D

[3]It should be noted that the letters used to categorize likelihood definitions and the numbers suggested for the severity of consequences definitions in NAS SEM are used opposite to the ones used herein (i.e., "A" represents a nonlikely event while "E" is for Nearly Certain; "1" stands for Low Risk" hazards, and 5 is for High). This discrepancy does not affect the methodology or the essence of risk analysis.

TABLE 5.—C-BAND COMMUNICATIONS SYSTEM SAFETY RISK SUMMARY

Safety hazards	Safety risk likelihood and severity[a]	
	Exist. NAS	C-band FCS[b,c]
12. A message affecting separation corrupted	2D	3D[h]
13. A message NOT affecting separation corrupted	5	5D
14. A message affecting separation sent/received out of sequence	4D	3D[h]
15. A message NOT affecting separation sent/received out of sequence	5	5D

[a]Severity assessment presented in this document is based on a worst case scenario.
[b]Communications with vehicles other than aircraft is considered to present lower safety risks, therefore ATS to aircraft communication safety risks are presented as a worst-case scenario.
[c]Fixed messages will be represented by relay messages, for example, those carrying meteorological and surveillance information. Messages may also include other data being relayed for the Air/Ground data communication services. Thus, for the worst credible effect (WCE), severity and likelihood ratings would be the same for fixed-fixed categories as they are for the fixed-to-mobile transmissions.
[d]Where hazard was split in two cases, the most significant risk is shown.
[e]The system being partially unavailable is considered to be more likely than it being totally unavailable. The severity for the partial and total unavailability is assumed the same as a worst case scenario.
[f]Classified as "probable" (B) and "minor severity" (4) because of the capability of retransmissions.
[g]Considered less likely but potentially more severe than failure of communication with a given recipient.
[h]Assumed to be not as severe as when a message affecting separation received too late or expired because system would recognize corruption and request retransmission, assuming that re-transmission comes within latency requirements. If re-transmission is too late, then hazard no. 10 would apply.

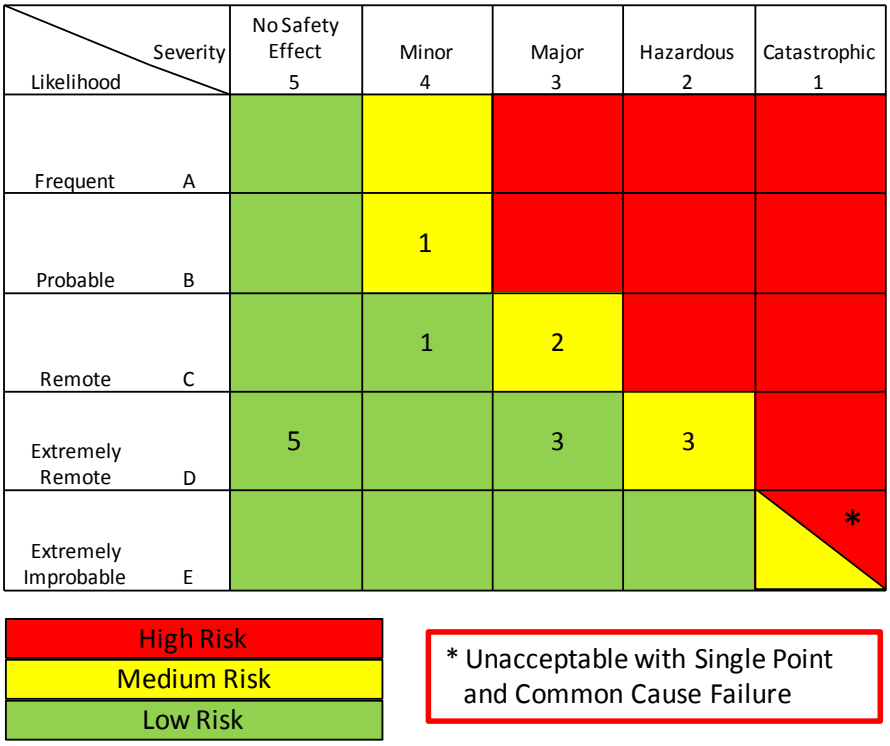

Figure 9.—C-band system safety risk matrix air-traffic-services-to-aircraft communication.

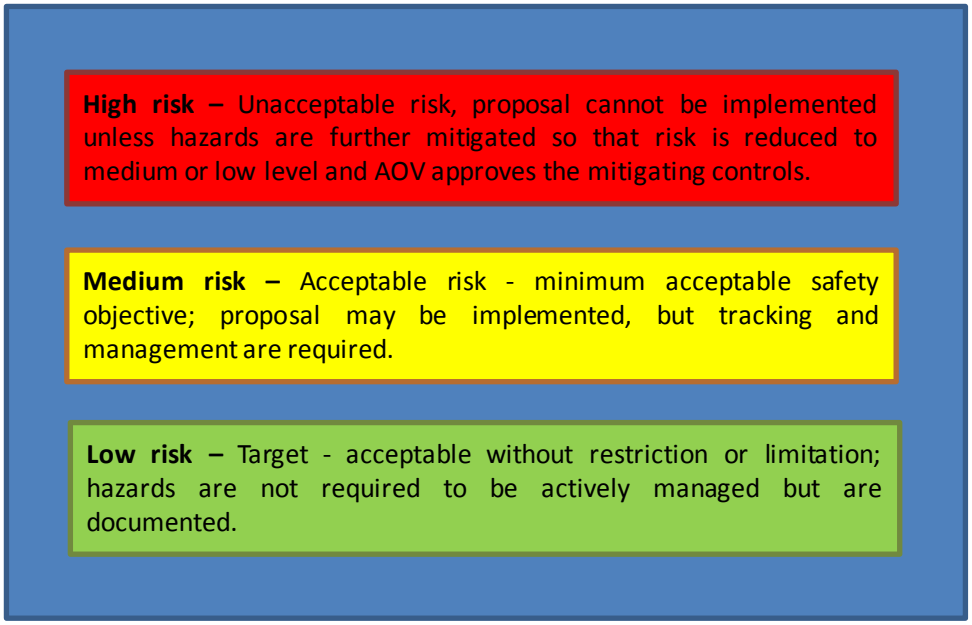

Figure 10.—Risk acceptance criteria (Ref. 1).

The completed risk assessment shows that none of the hazards associated with the proposed C-band communication system were determined to be high risk.

3.5.3 Safety Risks for Unmanned Aircraft System operations

Services related to UAS operations are also considered to be candidates for the C-band system applications. Data transmission is expected to be used as a primary mode of communication with voice communications limited to special advisories and emergencies or for aircraft not equipped for datalink exchanges (Ref. 9). Studies considering the implications of operating UASs in nonsegregated airspace are underway, and RTCA SC–203 is currently creating the standards for the community. The COCR has not assessed the requirements to support command and control links (i.e., telecommand and telemetry) for the UAS.

As UAS requirements mature, the command and control link traffic load could be estimated. As noted in COCR (Ref. 8)

> All other communications services with UASs are considered to be the same as those with manned aircraft, i.e., UAS operation is transparent for the ATM system. In the future, in some parts of the world, the number of these vehicles may represent a large portion of an Air Traffic Service Unit's (ATSU's) traffic load. When providing ATS to a UAS, this may involve the relay of communication and execution instructions to and from a remote pilot; however, operational performance requirements between an ATSU and an UAS remain the same as those between an ATSU and any manned aircraft.

At this time,

> The only UAS CC applications for which 5091 to 5150 MHz might be a viable candidate band are those requiring short-range, high-bandwidth communication at short ranges—e.g., pilot control of a low-autonomy UA during takeoff and landing. During those crucial phases of flight, a short-range system using this band might be useful as a backup for a "primary" CC link operating in a less encumbered band such as 960 to 1024 MHz.[4]

[4]Proposed changes to Annex 16 of 5B/296-E (Ref. 10).

Reference 10 further explains that

> At ranges less than 3 km, the power levels necessary for the 5091–5150 MHz link would probably be consistent with the need to protect incumbent satellite services and with UA power constraints. It is likely that relatively few UA would be taking off or landing at any given time within the NAS, thus minimizing the interference threat to satellite uplinks. The guard times necessary at such short ranges would be small enough that the UAS CC links might be able to employ the 802.16e standard, whose growing acceptance for vehicular applications may eventually drive down the unit costs of lightweight 802.16e devices that would be suitable for UA use. However, it is not yet clear that 802.16e links will perform well at UA takeoff and landing speeds. Some degradation of 802.16e's higher-order modulations might result, adversely affecting link capacities. Measurement and/or analysis would be needed to quantify this effect.

A UAS safety analysis will greatly depend on user applications that may vary from commercial to Government, military to civil, etc. As defined by the ITU (Ref. 10) and illustrated in Figure 11, commercial applications would provide services that would be sold by contractors in the course of carrying out normal business operations, while Governmental applications ensure public safety by addressing different emergencies and involve issues of public interest and include scientific matters.

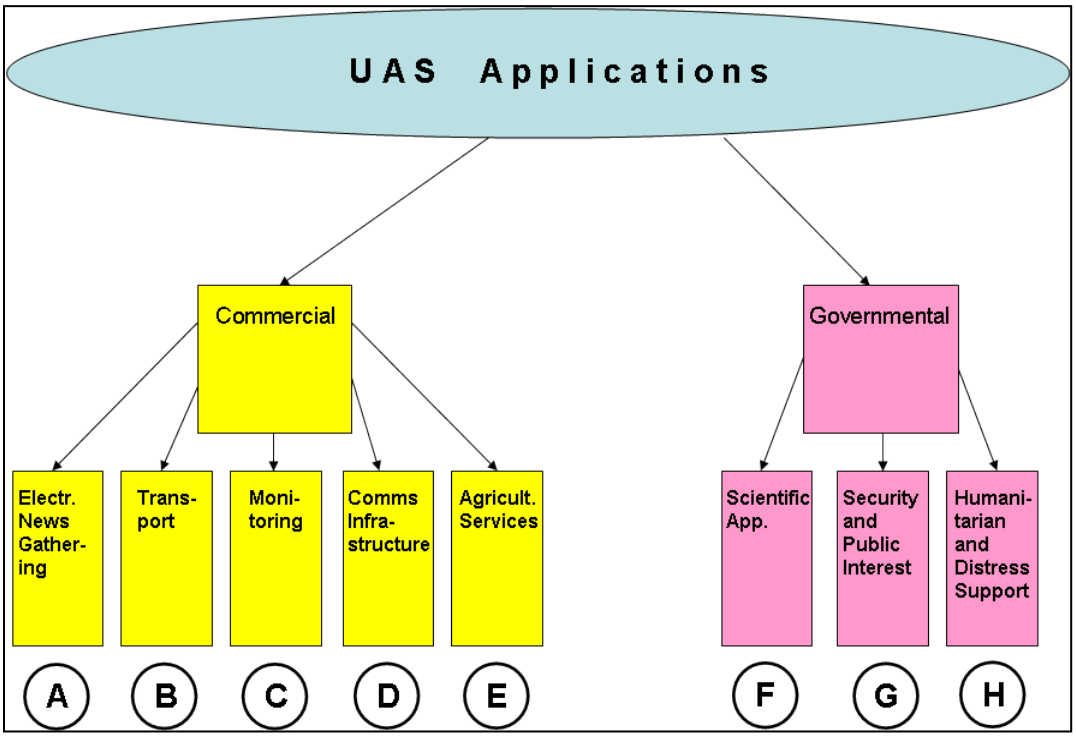

Figure 11.—UAS applications (from proposed changes to Annex 16 of 5B/296-E (Ref. 9)).

Example operational scenarios for each type of application are presented in Table 6, demonstrating a wide range of possible applications.

TABLE 6.—UNMANNED AIRCRAFT SYSTEM OPERATIONAL SCENARIOS[a,b]

Mission type	Scenario description
A	Movie making, sports games, and popular events like concerts
B	Cargo planes with reduced manning (one-man cockpit)
C	Inspections for industries (e.g., oil fields, oil platforms, oil pipelines, power line, or rail line)
D	Provision of airborne relays for cell phones in the future
E	Commercial agricultural services like crop dusting
F	Earth science and geographic missions (e.g., mapping and surveying or aerial photography) Biological and environmental missions (e.g., animal monitoring, crop spraying, volcano monitoring, biomass surveys, livestock monitoring, or tree fertilization)
G	Coastline inspection, preventive border surveillance, drug control, anti-terrorism operations, strike events, search-and-rescue of people in distress. Public-interest missions like remote weather monitoring, avalanche prediction and control, hurricane monitoring, forest fires prevention surveillance, insurance claims during disasters, and traffic surveillance
H	Famine relief, medical support, aid delivery, search-and-rescue activities

[a]Proposed changes to Ref. 10.
[b]Additional scenarios and detail can be found in Ref. 9.

As stated at the International Conference & Exhibition on Unmanned Aircraft Systems that took place in Paris, France in June 2009, the RTCA Special Committee 203 (SC–203) and EUROCAE Working Group 73 (WG–73) have agreed to collaborate on a pilot project for initial UAS safety assessments.

3.5.4 Airborne System Wide Information management (SWIM) Suitable Services Safety Assessment

System Wide Information Management (SWIM), an FAA technology program designed to facilitate sharing of ATM system information (airport operational status, weather information, flight data, status of special use airspace, NAS restrictions), might be implemented via G/G, A/G, and A/A communications infrastructure components. Each of these components would enable efficient data exchange between authorized users in the respective domain. An AeroMACS could provide means for the G/G and A/G data transfer.

An implementation of the proposed C-band system would facilitate meeting the primary objective of the SWIM program, that is, to improve the FAA's ability to manage the efficient flow of information through the NAS. When used to enable SWIM capabilities, a C-band system could be designed to assure that its use provides the following desired SWIM features:

- Reduced costs for NAS users to acquire NAS data and exchange information
- Increased shared situational awareness among the NAS user community
- FAA-compliant secure data exchange among the NAS user community

Figure 12 shows how airborne SWIM (with the communication links potentially provided over the C-band for A/G communications on airport surface, e.g., loading flight plans) fits in the overall FAA A/G communications plan and illustrates interactions of SWIM elements with the other NextGen programs, such as ADS–B and Data Comm.

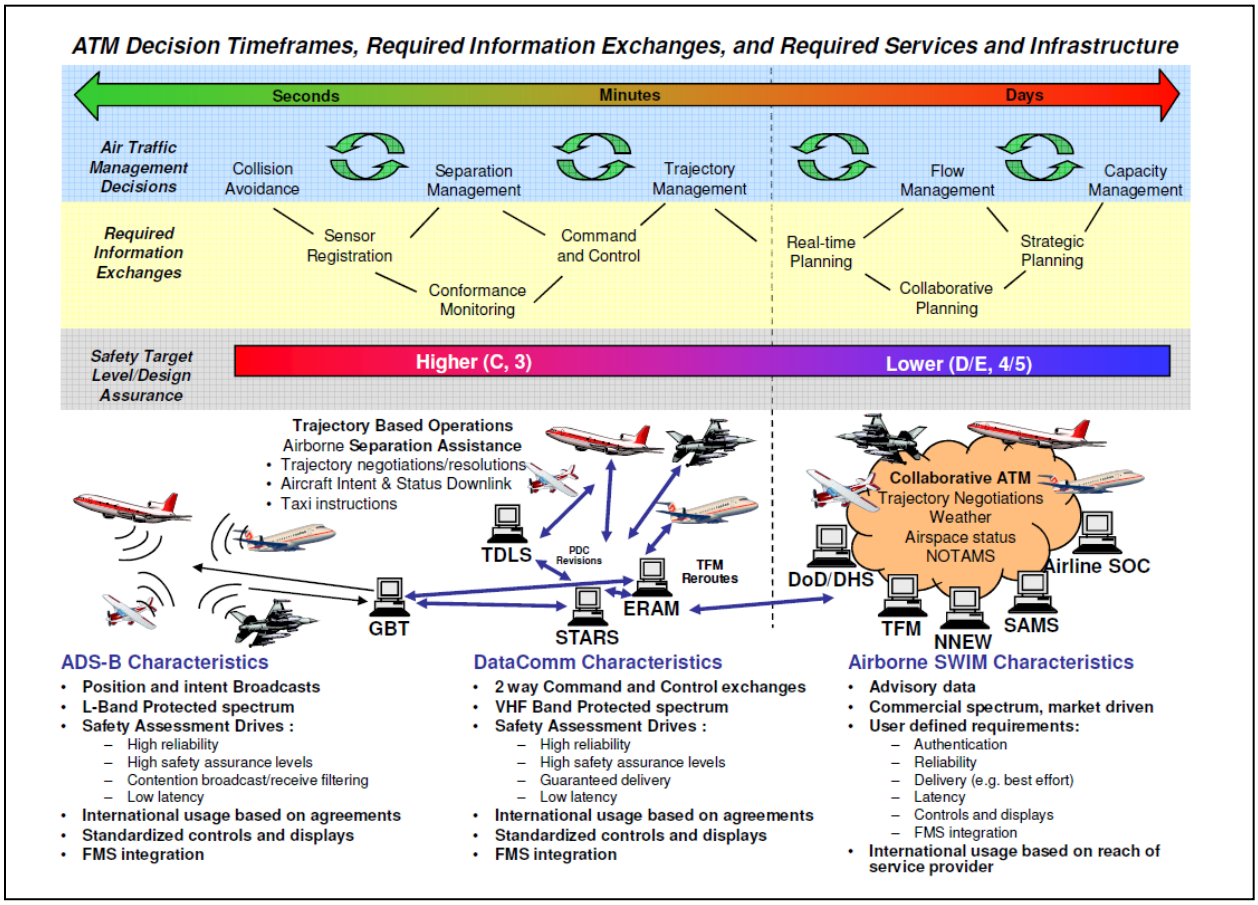

Figure 12.—Airborne SWIM and other NextGen programs (Ref. 11).

C-band communications links will have a lower safety targets when used to provide SWIM-related services compared with the other data communications services. For example, Figure 12 shows a required level of C3 (medium risk) for Data Comm and D/E 4/5 9 (low risk) for SWIM.

3.6 C-Band Communication System Safety Risks Treatment

The final step in the safety analysis is to treat the risk. Risk treatment includes mitigation, monitoring and tracking. Risk monitoring and tracking are sometimes referred to as risk maintenance.

3.6.1 Risk Mitigation

Figure 13 illustrates the risk management strategies that were considered (Ref. 3).

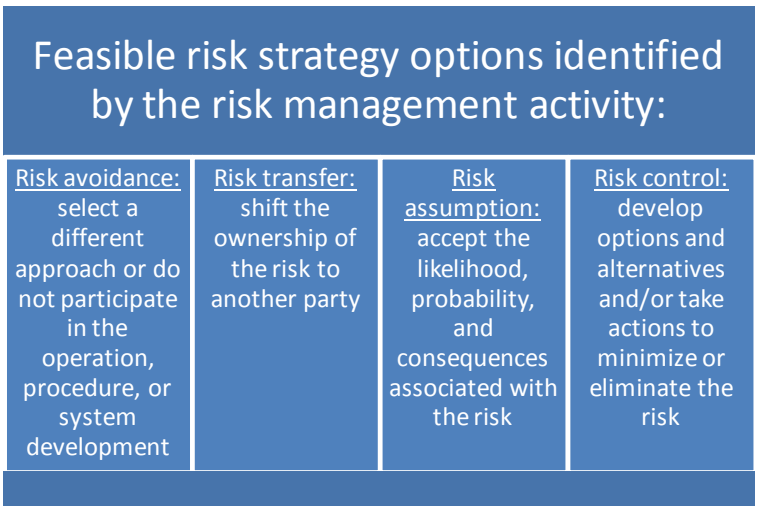

Figure 13.—Risk strategy options.

Risk avoidance is typically an operational strategy that involves a go or no-go decision. This analysis focuses on technical risks only. While operational controls could be applied to mitigate technical risks, for example a decision not to have a particular service provided over the C-band, such a measure is likely to apply to high risk hazards only. Since none of the hazards were found to be high risk, the risk avoidance strategy is not recommended for mitigation of the identified C-band safety risks.

Similar to the above, risk transfer does not appear applicable to the presented communications system analysis. The risk transfer strategy shifts the ownership of risk to another party. Again, such operational change could be used to mitigate a technical risk, for example, transfer of aircraft separation responsibility in applying visual separation from the air traffic controller to the pilot, it would likely to apply to high hazard risks only. Since none of the hazards were found to be high risk, the risk transfer strategy is not recommended for mitigation of the C-band safety risks.

Risk assumption and risk control have been determined to be the strategies most applicable to the mitigation of the identified technical risks. Following FAA recommendations (Ref. 3), risk assumption should be limited to lower level risks, as it implies assuming a risk, a likelihood of occurrence and its consequence (i.e., a safety risk must be reduced to medium or low) before it can be accepted into the NAS.

As noted in Reference 5, multiple existing Controls are present in the NAS system that

> either prevent or reduce the probability of the hazard occurring at all, or should the hazard occur, prevent or reduce the likelihood of the worst credible severity effect from occurring. Existing controls can be requirements, equipage, procedures, and/or environmental conditions. Many of the existing controls are not specific to the NAS Communication System itself (e.g., the requirement to protect the airspace of both the current and amended clearance is a control of the NAS system as a whole). Existing controls were implemented specifically with safety in mind.

The existing controls identified by the NAS safety analysis are included in Appendix E. Most of the existing controls are expected to remain in place at the time of C-band system implementation. Many of the controls can also be viewed as requirements (generally identified by “the system shall…”).

Table 12 is annotated with the existing controls that would not be relevant to the proposed system.

Additional controls specific to an AeroMACS system will be added as part of system design and implementation. The current trend points toward meeting QoS/reliability requirements with the number of communications threads needed to satisfy these requirements. Depending on final services selection (i.e., essential vs. critical), if requirements cannot be met otherwise, the second link or backup system will be considered. If a system is implemented in segments, as, for example a Data Comm program, a

backup system may be added at a later stage if and when critical services requiring higher reliability are added.

An example of system redundancy would include dual-blanket-coverage system design providing signal coverage from two base stations for any point within a service area. Each of the base stations would then be able to pick up full traffic load should another station is unavailable. Fast hand-off capabilities inherent to a WiMAX-type system offer another layer of redundancy allowing a subscriber station to hand-off to a different base station if its first choice server is unavailable.

3.6.2 Safety Risks Maintenance

Risks are dynamic; their profile would change depending on events, decisions, and actions on the project. Therefore, risk monitoring and tracking are integral parts of any risk management process. It is especially important for a new state-of-the-art system such as the proposed C-band communications system.

As noted earlier, this report presents an initial safety risk assessment. Safety hazards, their consequences, and probability of occurrence need to be reevaluated as the C-band system development progresses. Triggers for risks reassessment should include

ConUse changes or significant modifications.—The safety risks assessment detailed in this document was based on the identified concepts of use. User requirements changes, modifications to system scope, services addition, and so on, will all affect the safety risks.

The mobile aircraft applications are the main focus of the proposed C-band system. However, because of the complexity and a potentially long time (10 years +) involved in certifying and installing any new equipment on aircraft, the near to midterm application for the C-band system may be fixed airport surface communication and mobile applications not linked to aircraft. Service selection and implementation timing may affect safety analysis and trigger reassessment.

Modification or deletion of any of the existing controls.—Existing NAS controls were assumed to be in place at the time of C-band system implementation. Should they be deleted or modified, safety risks should be reassessed.

Technology development.—As technology is not finalized at the time of this study, the 802.16e profile for an airport surface is still being developed and testing is being performed. Safety risks identification was limited to high-level, technology-independent risks. Additional risks may be identified as technology development and standardization progresses. The risks may involve but not be limited to interference to/from incumbent systems, capacity limitations, COTS use, etc.

Schedule milestones.—Various risks exist in respect to the C-band system development and implementation schedule in the United States and Europe. This document is limited to technical risks identification. Because of schedule changes and coordination requirements between the United States and European partners, schedule issues are intertwined with the technology development risks noted above. Schedule milestones should be used as triggers for safety risks reassessment. The milestones would include completing test bed installation, system testing and results review, preparation of design documents, and finalizing the technology standards.

Additionally, the maturity and implementation schedule of other components of FCS will affect C-band system development. As a more definitive timeline and technology details become available, potential interfaces between the proposed C-band system and L-band and VDL-2 Data Comm systems will be developed. Safety risks analyses will need to be reviewed, updated, and amended as appropriate. Risk tracking will become most relevant at the start of system implementation.

Appendix A.—Acronyms and Abbreviations

The following list identifies acronyms and abbreviations used throughout this document.

A/A	air to air
AAC	Aeronautical Administrative Communication
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance - Broadcast
AIM	Aeronautical Information Management
AOC	Aeronautical (Airline) Operational Control
AOV	Air Traffic Safety Oversight
AP–17	Action Plan 17
ATM	air traffic management
ATS	Air Traffic Services
ATSP	Air Traffic Service Provider
ATSU	Air Traffic Service Unit
CC	control and communications
CNS	communication, navigation, surveillance
COCR	Communications Operating Concepts and Requirements
ConOps	Concepts of Operations
ConUse	Concepts of Use
DHS	Department of Homeland Security
DoD	Department of Defense
D-ORIS	Data Link Operational Route Information Service
D-OTIS	Data Link Operational Terminal Information Service
D-RVR	Data Link Runway Visual Range
D-SIG	Data Link Surface Information and Guidance
D-SIGMET	Data Link Significant Meteorological Information
D-TAXI	Data Link Taxi Clearance
ERAM	En route Automation Modernization
FAA	Federal Aviation Administration
FCI	Future Communications Infrastructure
FCS	Future Communications Study
FIS	flight information services
FLIPCY	flight plan consistency
FMS	flight management system
GBT	ground base transceiver
GRC	Glenn Research Center
ICAO	International Civil Aviation Organization
ITU	International Telecommunication Union
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NNEW	NextGen Network Enabled Weather
NOCC	National Operations Control Center
NOTAM	Notice to Airmen
PLA	project-level agreement

PPD	pilot preferences downlink
QoS	quality of service
RAC	risk analysis code
RF	radiofrequency
RTCA	RTCA, Inc. (founded as Radio Technical Commission for Aeronautics)
RVR	runway visual range
SAMS	Special Use Airspace Management System
SBS	surveillance and broadcast services
SE	system engineering
SEM	System Engineering Manual
SESAR	Single European Sky ATM Research
SHA	safety hazard analysis
SOC	systems operations control
SSE	system safety engineering
STARS	Standard Terminal Automation Replacement System
SWIM	System Wide Information Management
TFM	traffic flow management
UA	unmanned aircraft
UAS	unmanned aircraft system
VHF	very high frequency
WAKE	wake vortex
WCE	worst credible effect

Appendix B.—Hierarchical Diagrams of Functional Requirements

Appendix B contains the functional analysis of the C-band communication system presented as a series of hierarchical diagrams. The functional analysis was used to structure both the safety and security analyses. The "C" preceding all of the numerical functional levels is used to represent C-band.

The analysis and diagrams are adopted from the National Airspace System (NAS) Communications System Safety Hazard Analysis and Security Threat Analysis document (Ref. 5).

Solid blocks in the diagrams represent system functions that are part of the C-band system scope assumptions; white background blocks show NAS functions that are currently not part of the C-band functionality.

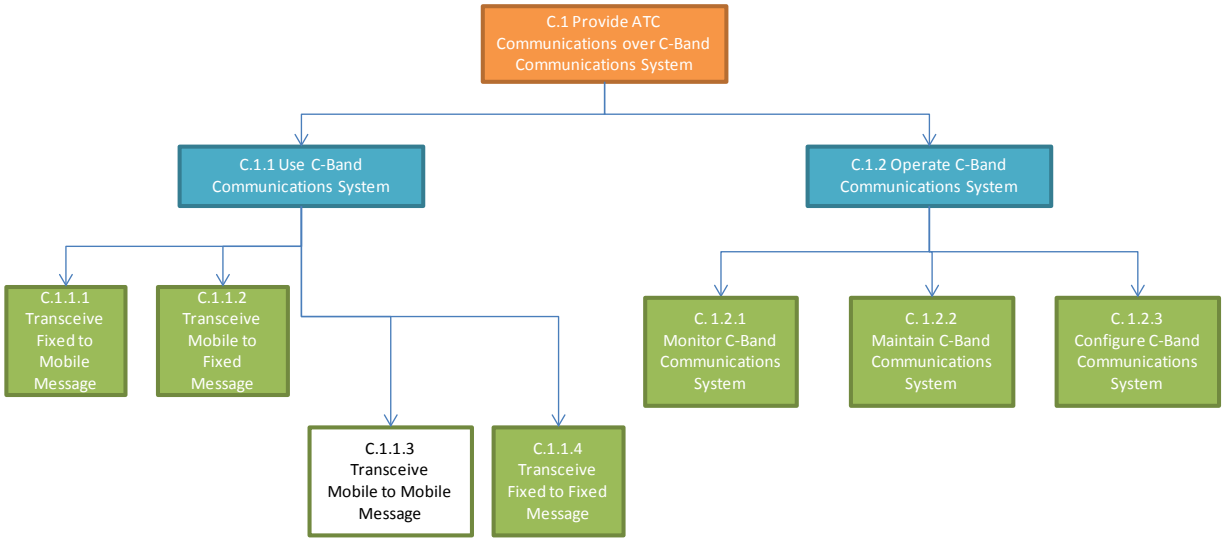

Figure 14.—C-band communications system high level.

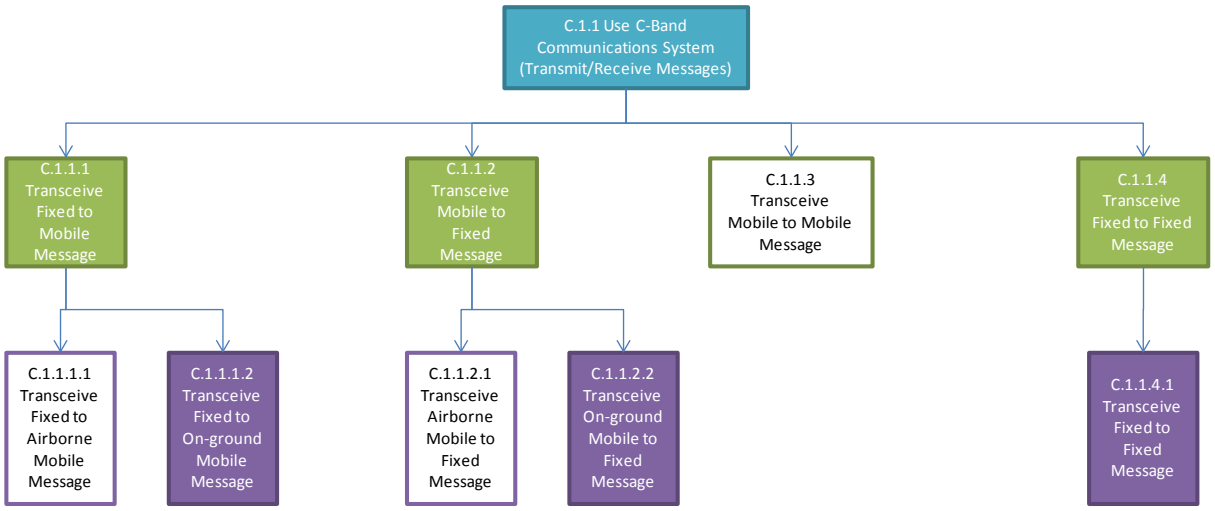

Figure 15.—Decomposition of use C-band communications system (transmit/receive messages).

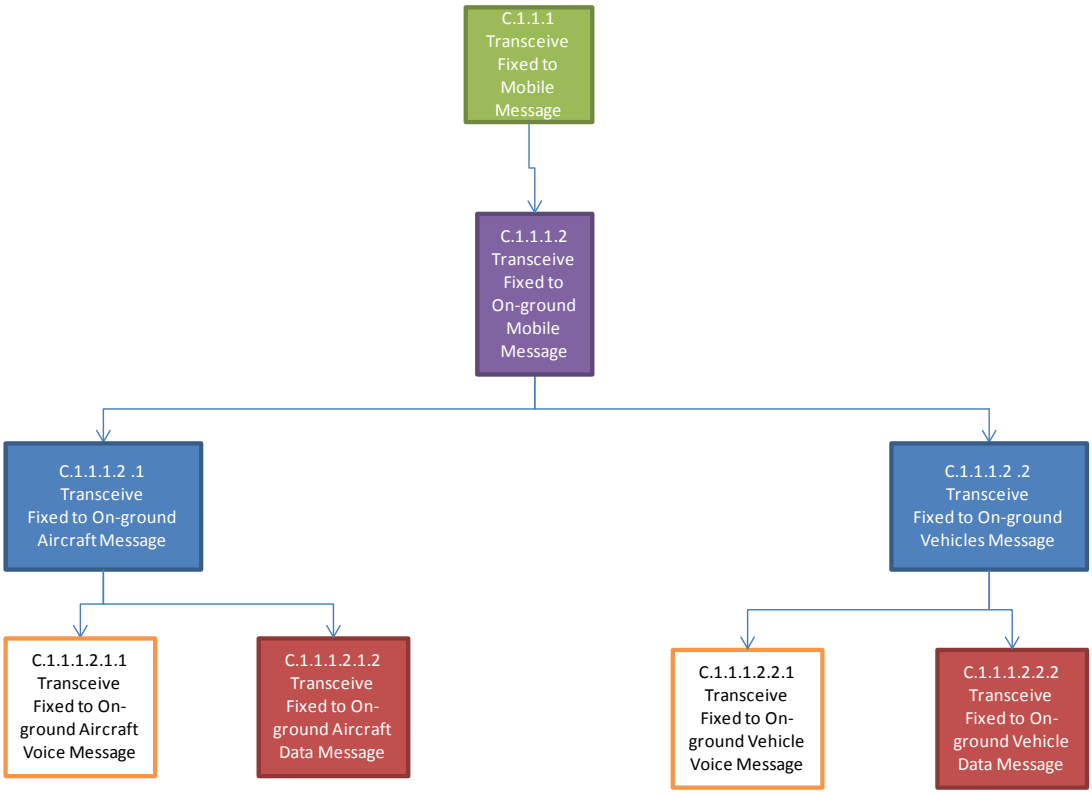

Figure 16.—Decomposition of transceive fixed-to-mobile message.

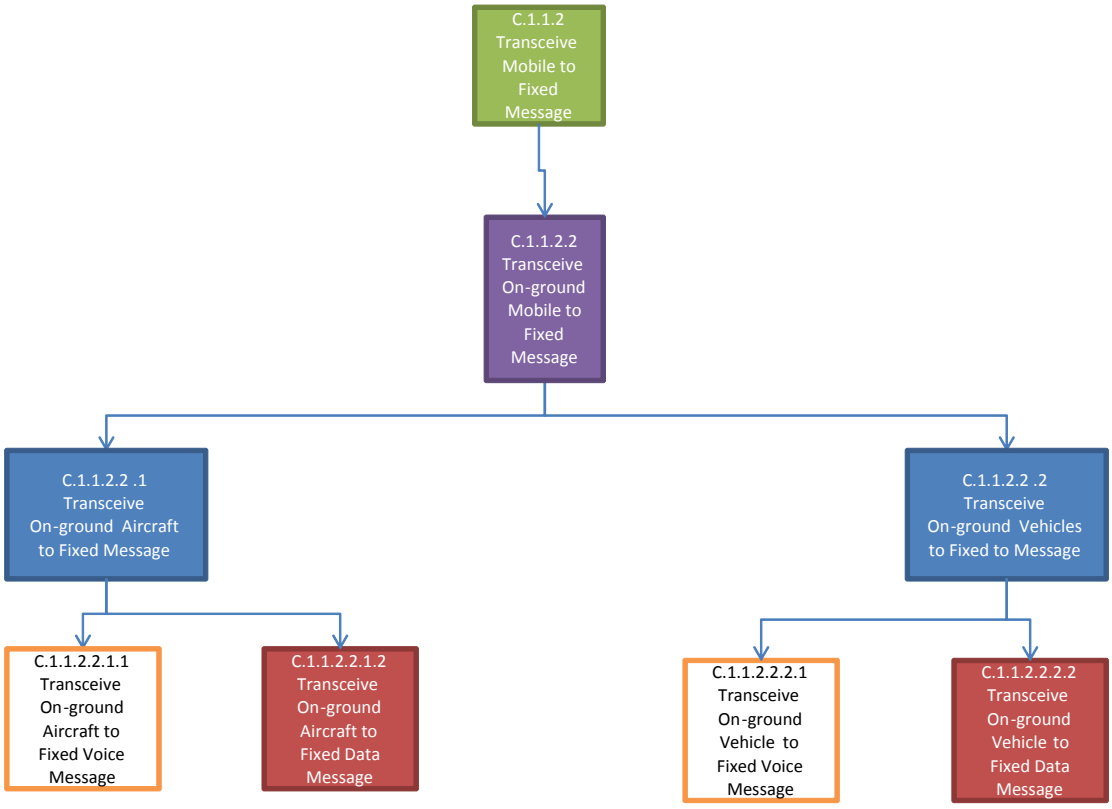

Figure 17.—Decomposition of transceive mobile-to-fixed message.

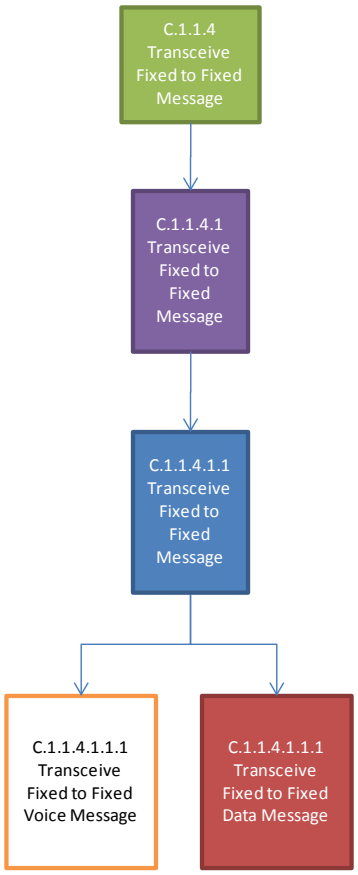

Figure 18.—Decomposition of transceive fixed-to-fixed messages.

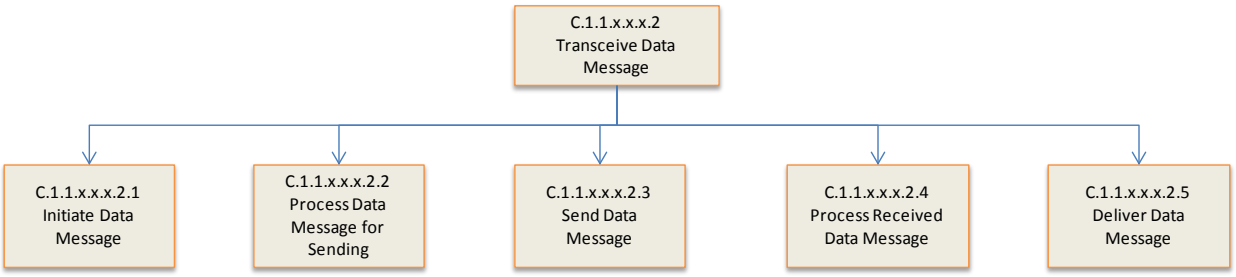

Figure 19.—Generic decomposition of transceive data message.

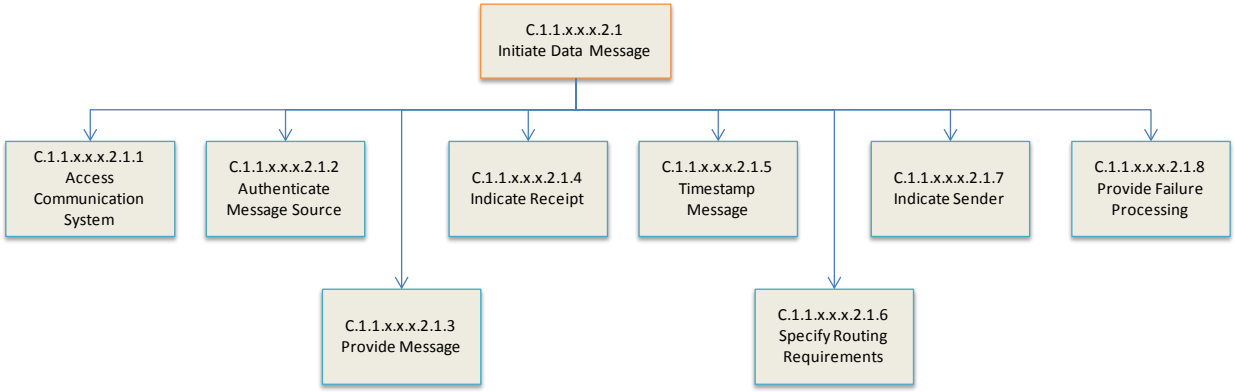

Figure 20.—Generic decomposition of initiate data message.

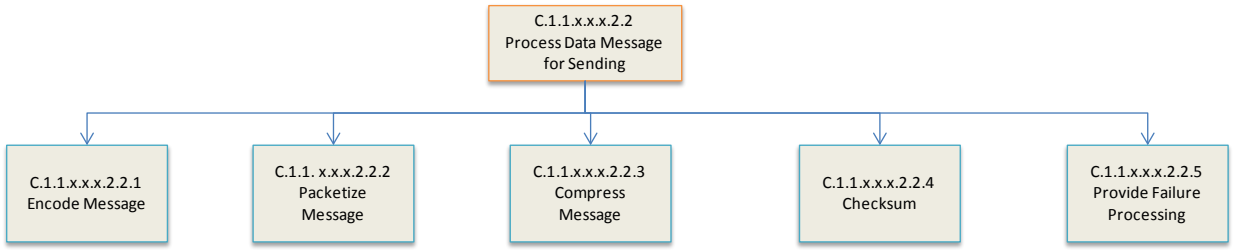

Figure 21.—Generic decomposition of process data message for sending.

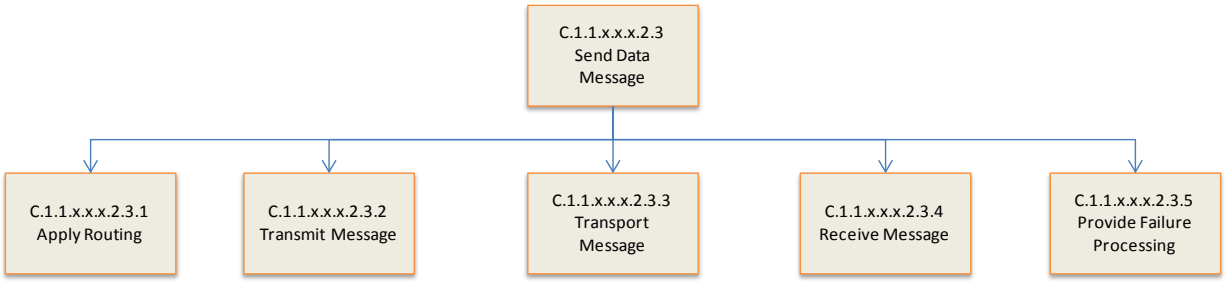

Figure 22.—Generic decomposition of send data message.

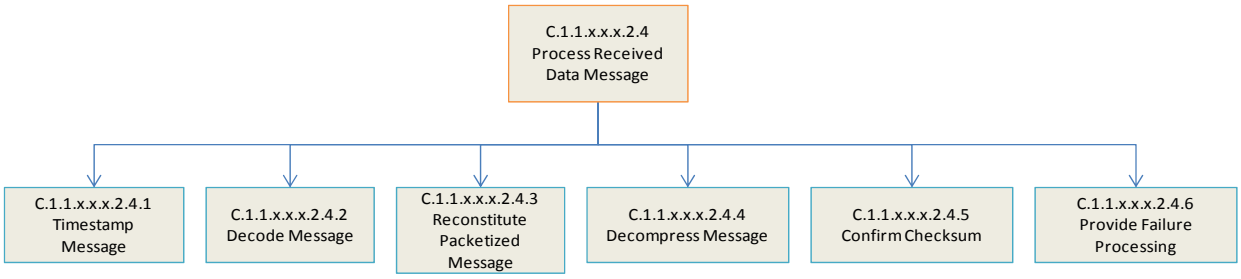

Figure 23.—Generic decomposition of process received data message.

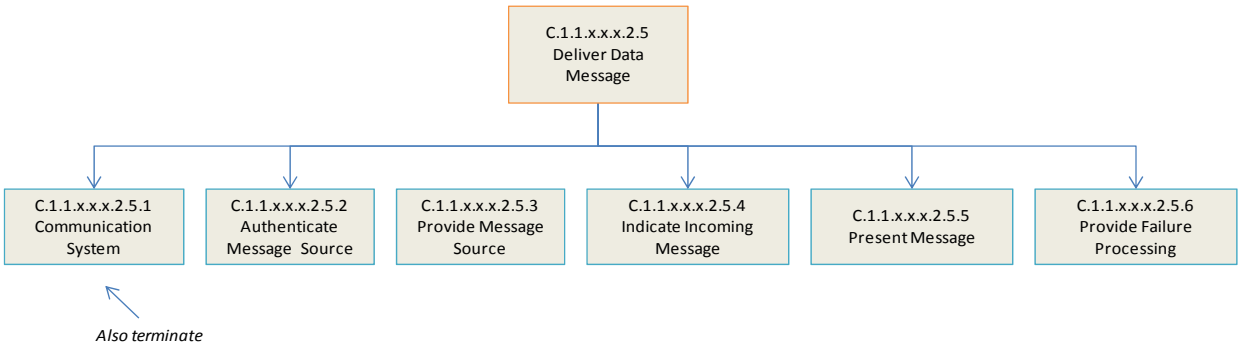

Figure 24.—Generic decomposition of deliver data message.

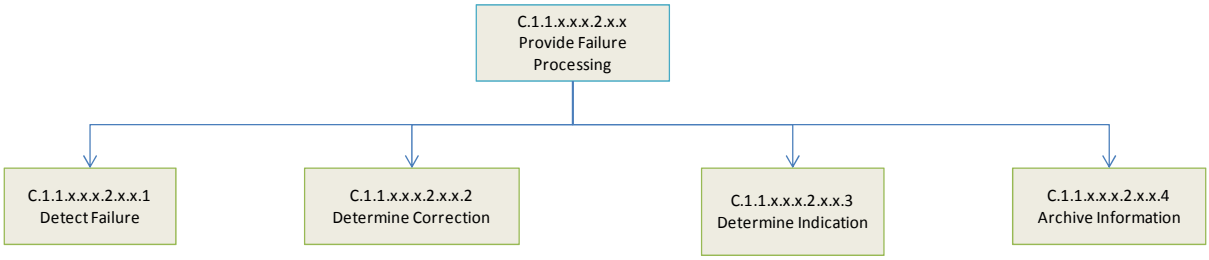

Figure 25.—Generic decomposition of provide failure processing.

List of failure detection subfunctions:

- Authentication failures
- Function unavailability
- Message unintelligible or garbles
- Message inaudible
- Message or message components missing or faulty
- Invalid or incorrect message components
- Checksum failures
- Invalid recipient

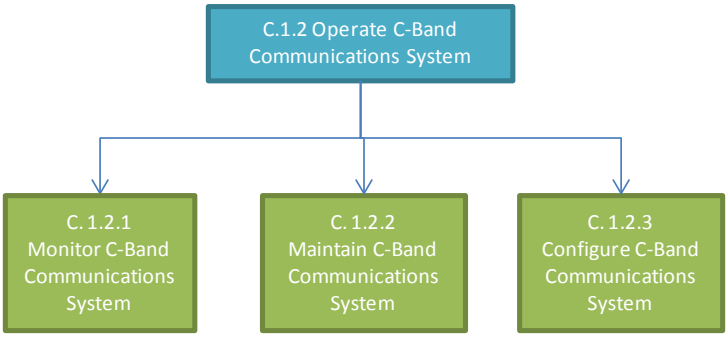

Figure 26.—Decomposition of operate C-band communications system.

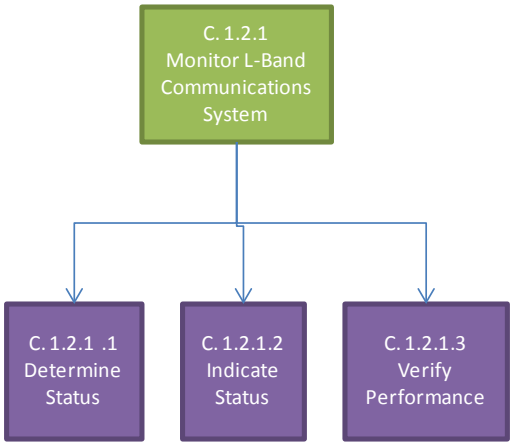

Figure 27.—Decomposition of monitor C-band communications system.

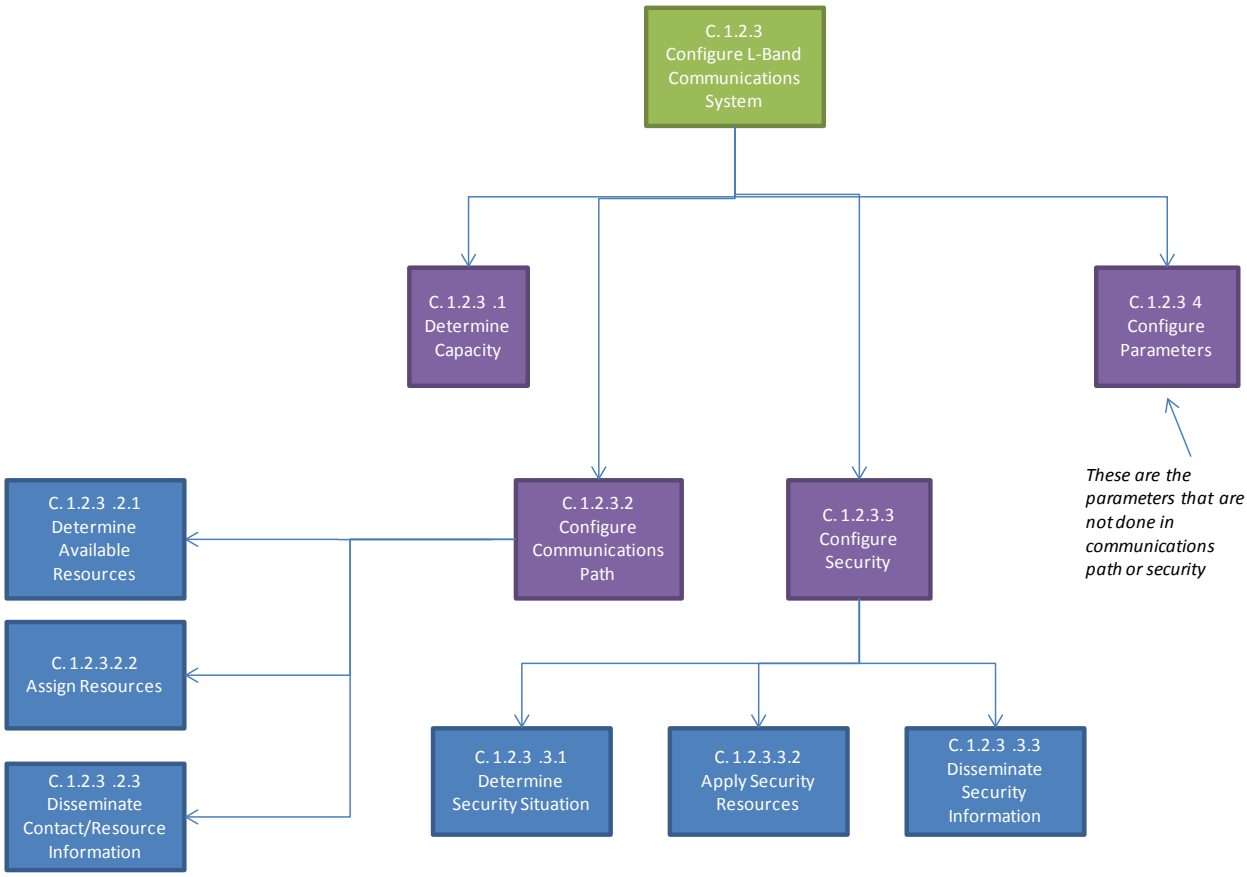

Figure 28.—Decomposition of configure C-band communications system.

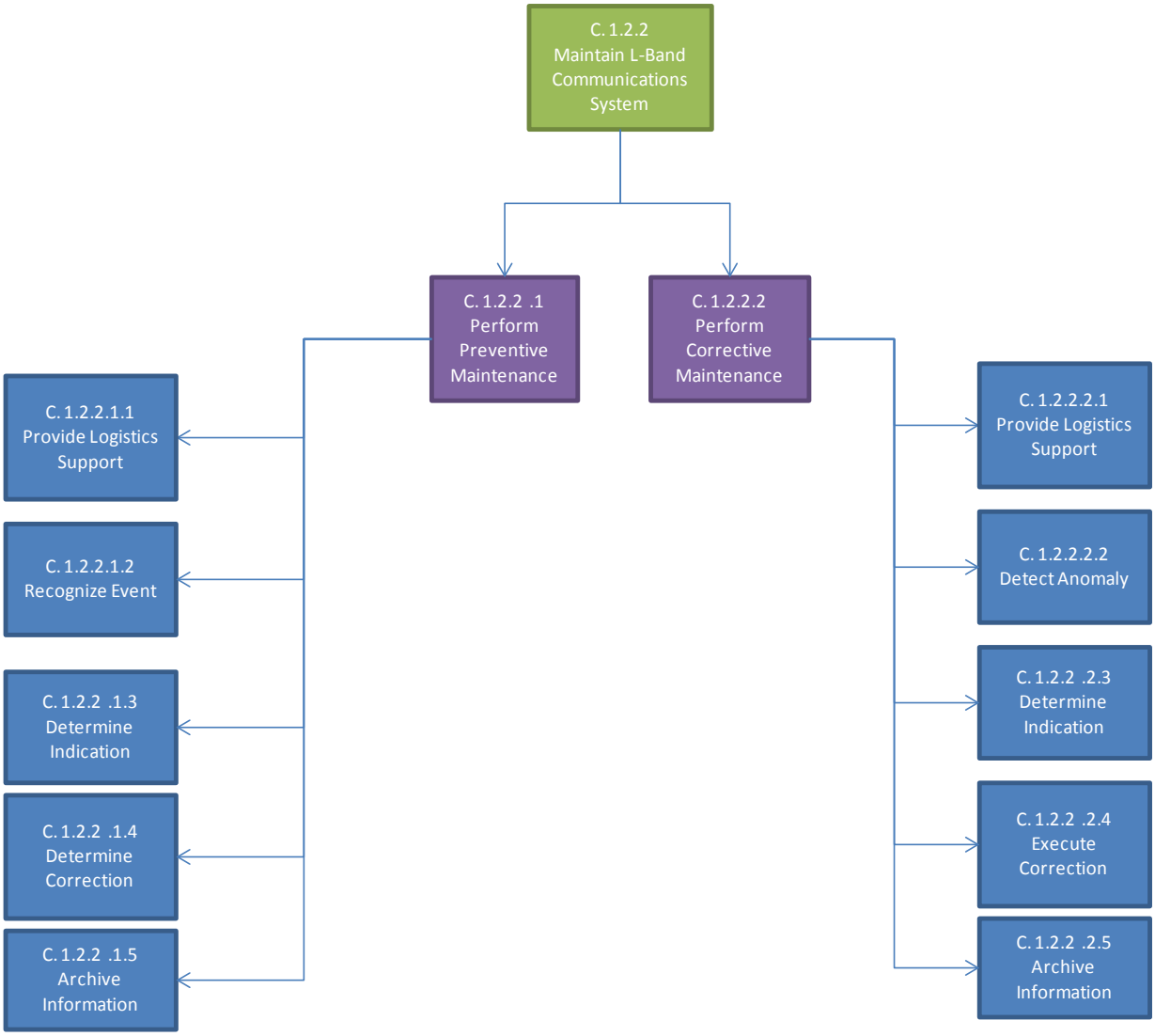

Figure 29.—Decomposition of maintain C-band communications system.

Appendix C.—Safety Hazard Analysis Worksheets

C.1 C-Band Communication SHA Table Cross Reference

For each of the five C-band communication system functions resulted from the functional system analysis, a typical list of the types of messages transmitted[5] is shown in Table 7. For some functions, the hazard scenarios were considered to be the same; and thus a single hazard worksheet table can be used for more than one function. The last column of Table 7 provides a cross reference to the function's hazard worksheet table.

TABLE 7.—SAFETY HAZARD ANALYSIS (SHA) TABLE CROSS REFERENCE[a]

	Information type (including corresponding function ID)	Message examples	Hazard table cross reference
1	Transceive ATS to Aircraft Message C.1.1.1.2.1	• Contract requesting data • Contract acknowledgments • OTIS reports, addressed or broadcast communications • SIGMET reports, addressed or broadcast communications, event basis only • Airport data to be displayed on board (D–SIG) • RVR information, addressed or broadcast communications	Table 8
	Transceive Aircraft to ATS Message C.1.1.2.2.1	• Requests (i.e., demand, periodic, or event contract) for reports • Contract acknowledgments • Current and periodic position (FLIPCY), addressed communications • Meteorological data (FLIPCY), addressed communications • Ground speed (FLIPCY), addressed communications • Broadcast of WAKE characteristics (e.g., aircraft type, weight, and flap and speed settings) • Flight limitations (e.g., maximum acceptable flight level) (PPD), addressed communications • Pilot flight preferences (PPD), addressed communications • Flight plan modification requests (e.g., desired route or speed limitations) (PPD), addressed communications	Table 8
2	Transceive ATS to Non-Aircraft Message C.1.1.1.2.2	• Contract requesting data • Contract acknowledgments • Reports, addressed or broadcast communication	Communication involving an aircraft was considered to present a higher safety risk compared with the communication with a non-aircraft vehicle. As such, only hazards associated with aircraft communications are included as they potentially lead to a WCE.
	Transceive Non-Aircraft to ATS Message C.1.1.2.2.2	• Contract requesting data • Contract acknowledgments • Reports, addressed or broadcast communication	

[5]Message types are based on services definitions presented in Reference 8.

TABLE 7.—SAFETY HAZARD ANALYSIS (SHA) TABLE CROSS REFERENCE[a]

	Information type (including corresponding function ID)	Message examples	Hazard table cross reference
3	Transceive Fixed to Fixed Message C.1.1.4.1.1	• Relaying meteorological data • Relaying surveillance data • Relaying air/ground communications data	Fixed messages will be represented by relay messages, for example, those carrying meteorological and surveillance information. Messages may also include other data being relayed for the air/ground data communication services. Thus, for the WCE, severity and likelihood ratings would be the same for fixed-fixed categories as they are for the fixed-to-mobile transmissions.

[a]Acronyms are defined in Appendix A.

C.2 Hazard Analysis Worksheets

For each of the hazards identified for the C-band communication system, the potential causes of the hazard were listed. The system state was also identified. The system state used is the state that fosters the worst credible outcome. The Safety Hazard Analysis (SHA) was captured in the tabular format in fixed messages (C.1.1.4.1.1 Transceive Fixed-to-Fixed Message Function) will be represented by relay messages, for example, those carrying meteorological and surveillance information. Messages may also include other data being relayed for the air/ground data communication services. Thus, for the WCE, severity and likelihood ratings would be the same for fixed-fixed categories as they are for the fixed-to mobile transmissions.

Possible effects are unrelated to the services currently planned for a C-band system; that is, the WCE would generally apply to using the data link for clearances related services that may be provided over a C-band system.

The worksheets are slightly modified worksheets from the tables provided in Reference 5. The modifications include but are not limited to different Risk/RAC assessments. The columns shown in each of the SHA tables are defined as follows:

- Column 1—Hazard identification, unique tag used to identify each hazard
- Column 2—Hazard description, description of the hazard
- Column 3—Causes, list of potential causes that could result the hazard occurring
- Column 4—Risk/RAC, using the risk categorization outlined earlier in this report, the column provides the worst possible credible effect and the likelihood of that effect should the hazard occur
- Column 5—Potential effects, provides a scenario leading to the worst credible effect if the hazard occurs
- Column 6—Comments: provides additional rational for the resulting Risk/RAC

Communication involving an aircraft was considered to present a higher safety risk compared with the communication with a nonaircraft vehicle. As such, only hazards associated with aircraft communications are included as they potentially lead to a WCE.
The section presents the 15 identified C-band communication system hazards as they apply to messages exchanged between an ATS and an aircraft on the ground. Hazard 1 is split into 2 cases (1a and 1b) to distinguish between total and partial loss of ATS ground communication.

Table 8 contains the hazard analysis worksheet for the following functions:

- C.1.1.1.2.1 Transceive ATS to On-Ground Aircraft Message
- C.1.1.2.2.1 Transceive On-Ground Aircraft to ATS Message

The system state leading to the worst credible effect (WCE) is the same for all ATS-aircraft hazards due to the C-band communication system:

- Heavy traffic conditions
- Instrument meteorological conditions (IMCs)
- Adverse weather conditions

Fixed messages (C.1.1.4.1.1 Transceive Fixed to Fixed Message Function) will be represented by relay messages, for example, those carrying meteorological and surveillance information. Messages may also include other data being relayed for the A/G data communication services. Thus, for the WCE, severity +and likelihood ratings would be the same for fixed-fixed categories as they are for the fixed-to-mobile transmissions.

Possible effects are unrelated to the services currently planned for a C-band system; that is, the WCE would generally apply to using the data link for clearances related services that may be provided over a C-band system.

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 1a	C-band communication capability totally unavailable—ground (facility wide). Ground cannot send/receive messages to any aircraft.	1. Hardware failure 2. Software failure 3. Radiofrequency (RF) interference	3D	**Case 1** • Controller needs to issue new/amended clearances to several aircraft. • When trying to transmit clearances, controller is informed that messages cannot be transmitted (voice nor data available). *OR* • Controller knows in advance that NAS aircraft communications is unavailable. • Controller transfers control to another control facility • This could result in a significant increase in controller workload. • This could also cause a slight increase in aircrew workload, but some could be time critical decisions. • Significant reduction in air traffic capability. **Case 2** • Aircrew attempts to send clearance response and finds out he/she is unable to do so. • Both current and new clearances are protected. • Workload remains within expected workload so no hazard.	Aircraft may or may not be aware of ground failure (e.g., until aircraft attempts a transmission and it is not acknowledged).
ATS—Aircraft Comm 1b	C-band communication capability totally unavailable—ground (a given sector/control position). Ground/sector cannot send/receive messages to any aircraft.	1. Hardware failure 2. Software failure 3. RF interference	3D	**Case 1** • Controller needs to issue new/amended clearances to several aircraft. • When trying to transmit clearances, controller is informed that messages cannot be transmitted (voice nor data available). *OR* • Controller knows in advance that NAS aircraft communications is unavailable. Controller transfers control to another sector. This could result in a significant increase in controller workload. • This could also cause a slight increase in aircrew workload, but some could be time critical decisions. • Significant reduction in air traffic capability. *OR* **Case 2** • Aircrew attempts to send clearance response and finds out he/she is unable to do so. • Both current and new clearances are protected. • Workload remains within expected workload so no hazard.	Aircraft may or may not be aware of ground failure (e.g., until aircraft attempts a transmission and it is not acknowledged).

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 2	C-band communication capability partially unavailable—ground. Ground cannot send/receive messages to one or more aircraft.	1. Hardware failure 2. Software failure 3. RF interference	3C	**Case 1** • Controller needs to issue new/amended clearances to several aircraft. • When trying to transmit the clearances, controller is informed that messages cannot be transmitted to all required aircraft. *OR* • Controller knows in advance that NAS communications is unavailable to some of the aircraft. • Controller must revert to transmitting clearances via alternative means (e.g., alternate frequency, transferring to another sector or relay). • This could result in a significant increase in controller workload. • This could also cause a slight increase in aircrew workload. • Significant reduction in air traffic capability. *OR* **Case 2** • Aircrew attempts to send clearance response. • Both current and new clearances are protected. • Workload remains within expected workload so no hazard.	This could be loss of communications for a sector within a facility.
ATS—Aircraft Comm 3	C-band system communication capability unavailable—aircraft (single aircraft) Aircrew cannot send/receive messages to ground,	1.Hardware failure 2. Software failure 3. Insufficient coverage 4. RF interference	4C	• Aircrew needs to request new/amended clearance. • When trying to request the new clearance, aircrew determines that message cannot be transmitted. *OR* • Aircrew knows in advance that NAS aircraft-ground communications are unavailable. • Aircrew must use alternative means of communication (e.g., relay). • This may cause a slight increase in aircrew workload. • This results in an increase in controller workload moving other aircraft. • Slight reduction in air traffic capability due to use of alternative procedures.	This could be one or all aircraft, but considered independent between aircraft
ATS—Aircraft Comm 4	Message fails with a given aircraft.	1. Ground message (or part) does not make it to aircraft. 2. Aircraft message (or part) does not make it to ground.	4B	• Controller issues a new clearance. • Controller does not receive response to clearance; either the aircrew did not receive the clearance; or the aircrew received the clearance and response is lost. • There is an ambiguity of whether the aircraft is executing the current or new clearance. However, both the current and new clearances are protected. • This results in increased controller workload in resolving the situation (e.g., retransmitting the message). • Slight loss of air traffic control capability in the affected area.	

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 5	Message fails with multiple aircraft.	1. Ground message (or part) does not make it to aircraft. 2. Aircraft message (or part) does not make it to ground.	3C	• Controller issues new clearances to multiple aircraft. • Controller does not receive response to the clearances; either the aircrew did not receive the clearance; or the aircrew received the clearance and responses are lost • There is an ambiguity of whether the aircraft are executing the current or new clearances. However; both the current and new clearances are protected. • This results in a significant increased controller workload in resolving the situation with multiple aircraft (e.g., retransmitting the message) • Slight reduction in air traffic capability	
ATS—Aircraft Comm 6	An aircraft acts on messages affecting separation (e.g., clearance) from a ground system that is not its control authority.	An unauthorized ground system sends a message affecting separation.	2D	• Aircrew accepts a clearance from a ground system not in control of the aircraft • The controlling authority is unaware of the clearance; and consequently the airspace is not protected • This could result in a loss of separation. • The loss of separation could result in large reductions in safety margins • Resolving the situation could also result in significantly increased ATC workload due to having to move several aircraft to re-establish or maintain separation. • Resolving the loss of separation could cause time critical aircrew decisions and excessive increased workload	
ATS—Aircraft Comm 7	An aircraft acts on messages NOT affecting separation from a ground system that is not its control authority.	An unauthorized ground system sends a message NOT affecting separation.	5D	• Aircrew accepts a message that does not affect separation from a ground system not in control of the aircraft • Time may be spent responding to a message that that does not apply • This does not result in a loss of separation.	

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 8	A message affecting separation is acted on by an unintended recipient.	1. Address is corrupted 2. Misdelivered 3. Step-on	2D	**Case 1** • A clearance is transmitted and reaches an unintended aircraft. The aircrew does not realize that the clearance is not for them and accepts the clearance. (When the unintended recipient is not under the control authority, see ATS-Aircraft COMM-6.) • Upon receipt of the WILCO to the clearance, the controller (a) does not realize that the WILCO is from a different aircraft than the intended one or (b) the controller realizes that the WILCO is from an unintended aircraft. (The difference between case a and case b; is just how soon the controller realizes that there is a situation that needs resolution.) • In either case, the airspace is not protected and could result in a loss of separation. • The loss of separation could result in large reductions in safety margins. • Resolving the situation could also result in increased ATC workload due to having to move several aircraft to reestablish or maintain separations. • Resolving the loss of separation could cause time-critical aircrew decisions and increased workload. **Case 2** • The response to a clearance is sent and reaches an unintended ground system. • The unintended ground system receives a message that is unexpected, but is no more than a nuisance. • The ground system that should have received the response message does not receive any message, and the clearance message expires.	
ATS—Aircraft Comm 9	A message NOT affecting separation is acted on by an unintended recipient.	1. Address is corrupted 2. Misdelivered 3. Step-on	5D	**Case 1** • A message NOT affecting separation reaches an unintended aircraft. The aircrew does not realize that the message is not for them and acts on it. • If the message requires a response, upon receipt of the response, the controller (a) does not realize that the response is from a different aircraft than the intended one or (b) the controller realizes that the response is from an unintended aircraft. • If the message does not require a response, the controller may not be aware that message went to an unintended recipient, unless flight crew expecting a message, queries for missing message. • This does not result in a loss of separation. • At most this could result in a slight increase in ATC workload due to either resending message to the intended aircraft. In general this would be well within the normal workload. • There may be a slight increase in aircrew workload (of the unintended aircraft) in responding to a message not applicable to them. In general this would be well within the normal workload. **Case 2** • A request message reaches an unintended ground system. • The controller does not realize that request is not for them and responds with a clearance. • This ground system is not the control authority of the aircraft.	

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 10	A message affecting separation received too late (or expired)	1. Late delivery 2. Ground and air time is out of sync	2D	• Clearance is sent and expires before a response is received. *OR* • Aircrew accepts a clearance after it has expired. • The controller reverts to alternate solution due to the clearance expiry, and the airspace of the new clearance is no longer protected. • This could result in a loss of separation. • The loss of separation could result in large reductions in safety margins. • Resolving the situation could also result in significantly increased ATC workload due to having to move several aircraft. • Resolving the loss of separation could cause time-critical aircrew decisions and excessively increased workload.	So far no incidents due to this (Ref. 5)
ATS—Aircraft Comm 11	Message NOT affecting separation received too late (or expired)	1. Late delivery 2. Ground and Air time is out of sync	5D	**Case 1** • A message not affecting separation is transmitted and expires before a response is received. • The controller reverts to alternate solution due to the messages expiry. • Aircrew responds to message after it has expired. • Because the expired message does not affect separation, this does not result in a loss of separation. • At most this could result in a slight increase in ATC workload due to either retransmitting the message. In general this would be well within the normal workload. • There may be a slight increase in aircrew workload. In general this would be well within the normal workload. **Case 2** • A request message is transmitted and expires before a response is received. • At most this could result in a slight increase in aircrew workload due to retransmitting the request message. In general this would be well within the normal workload.	

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 12	A message affecting separation corrupted	The communication system corrupts a message	3D	**Case 1** • A clearance is sent and the contents are corrupted but still credible. • The aircrew accepts the corrupted clearance. • Because the clearance has been corrupted, its airspace is not protected. • This could result in a loss of separation (if the accepted corrupted clearance converges with other aircraft clearances). • The loss of separation could result in large reductions in safety margins. • Resolving the situation could also result in significantly increased ATC workload due to having to move several aircraft to reestablish or maintain separations. • Resolving the loss of separation could cause time critical aircrew decisions and excessively increased workload. **Case 2** • The response to clearance is sent and the contents are corrupted, but still credible (readback is corrupted and credible). • Once the clearance response has been received; either the old clearance airspace or the new clearance airspace becomes unprotected, but it is precisely the opposite of what the aircraft is doing. • This could result in a loss of separation (if the accepted corrupted clearance converges with other aircraft clearances). • The loss of separation could result in large reductions in safety margins. • Resolving the situation could also result in significantly increased ATC workload due to having to move several aircraft to reestablish or maintain separations. • Resolving the loss of separation could cause time critical aircrew decisions and excessively increased workload. **Case 3** • The address/call sign is the part of the message that becomes corrupted.	
ATS—Aircraft Comm 13	A message NOT affecting separation corrupted	The communication system corrupts a message	5D	**Case 1** • A message not affecting separation is transmitted and the contents are corrupted but still credible. • At most this could result in a slight increase in ATC workload due to retransmitting a message. In general this would be well within the normal workload. • There may be a slight increase in aircrew workload in responding to a corrupted message. In general this would be well within the normal workload. **Case 2** • A request is sent and the contents are corrupted but still credible. • The ground responds with a clearance meeting the corrupted request message. • The airspace is the clearance is protected so this does not result in a loss of separation. • There may be a slight increase in aircrew workload if they send a second request. In general this would be well within the normal workload.	

TABLE 8.—AIRCRAFT HAZARDS DUE TO THE C-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS—Aircraft Comm 14	A message affecting separation sent/received out of sequence	1. Message sent second is received prior to message sent first 2. Communication system does not deliver messages in order	3D	**Case 1** • Two (or more) clearances are transmitted and do not arrive in the order in which they were sent. • This could result in an aircraft executing a clearance out of order; and the airspace may not be protected. • The loss of separation could result in large reductions in safety margins. • Resolving the situation could also result in increased ATC workload due to having to move several aircraft. to reestablish or maintain separations. • Resolving the loss of separation could cause time critical aircrew decisions and increased workload. **Case 2** • Two (or more) responses to clearances are sent and do not arrive in the order in which they were sent. • All clearances response messages referenced to the clearance to which they apply. Therefore, if they are received out of order there is no impact.	
ATS—Aircraft Comm 15	A message NOT affecting separation sent/received out of sequence	1. Message sent second is received prior to message sent first 2. Communication system does not deliver messages in order	5D	**Case 1** • Two (or more) messages are sent not affecting separation and do not arrive in the order in which they were sent. • If the messages are different, there may be a slight increase in aircrew workload figuring thing out. In general this would be well within the normal workload. **Case 2** • Two (or more) requests are sent and do not arrive in the order in which they were sent. • If the requests are different, there may be some increased workload for both the air and ground in determining which clearance the aircrew wants to fly.	

Appendix D.—Summary of the Operational Safety Assessment for the ATS Services Identified for C-Band Application

Communications Operating Concepts and Requirements (COCR) Version 2.0 documents operational and safety requirements for air traffic services (ATS) data communications services and information security requirements for ATS and autonomous operations services (AOS). A service-level operational safety assessment (OSA) is performed to derive safety requirements (Ref. 8).

The following subsections summarize the assessment for the services applicable to the proposed C-band communications system as proposed by the Future Communications Infrastructure (FCI) Aeronautical Data Services Definition Task Report (Ref. 2).

D.1 Safety Objectives Definitions

Table 8 outlines the hazard effects and the classification scheme used to describe the severity of the ATS service hazards.

Based on the fact that each class hazard can be tolerated to a different degree, COCR derives safety objectives quantifying the degree of tolerance for each hazard class as shown in Table 9.

TABLE 9.—SAFETY OBJECTIVE DEFINITIONS (REF. 8)

Hazard class	Safety objective	Definition, per flight hour
5, no safety effect	Frequent	≥1 occurrence in 10^{-3}
4, minor	Probable	≤1 occurrence in 10^{-3}
3, major	Remote	≤1 occurrence in 10^{-5}
2, hazardous	Extremely remote	≤1 occurrence in 10^{-7}
1, catastrophic	Extremely improbable	≤1 occurrence in 10^{-9}

D.2 Service-Level Safety Assessment (C-Band Services Only)

The COCR provides a useful operational safety assessment summary applicable to the C-band ATS services case (Ref. 8):

> At the highest level the ATS services operational safety hazards are (1) loss of service, and (2) hazardously misleading information. Loss of service is defined the lack of availability of a service when it is required. Hazardously misleading information consists of undetected corrupted messages, undetected mis-delivered messages, undetected late or missing messages and undetected out-of-sequence messages. The safety analyses were based on the operational use of the services as described in Sections 2 and 3[of the COCR], in conjunction with the operational environment characteristics and conditions described in Sections 3.2.1 and 3.4.1 [of the COCR].

Note that only services identified as potential applications for the proposed C-band system (Ref. FCI Aeronautical Data Services Definition Task Report) are included in this document, thus presenting only a subset of the corresponding section and tables of the COCR.

Table 10 presents the OSA hazard severity and corresponding safety objectives for service categories for the two high-level safety hazards. As discussed earlier, introduction of a C-band system is assumed to correspond to Phase II future radio system (FRS) evolution.

TABLE 10.—AIR TRAFFIC SAFETY OPERATIONAL SAFETY ASSESSMENT HAZARD SEVERITY AND SAFETY OBJECTIVES

Service category	Loss of service		Hazardously misleading information	
	Severity	Safety objective	Severity	Safety objective
Flight information services (FIS)	4	Probable	2	Extremely remote
Flight position/intent/preferences service (FPS)	3	Remote	2	Extremely remote

Figure 30 and Figure 31 present safety risk matrices for loss of service and hazardously misleading information hazards, respectively.

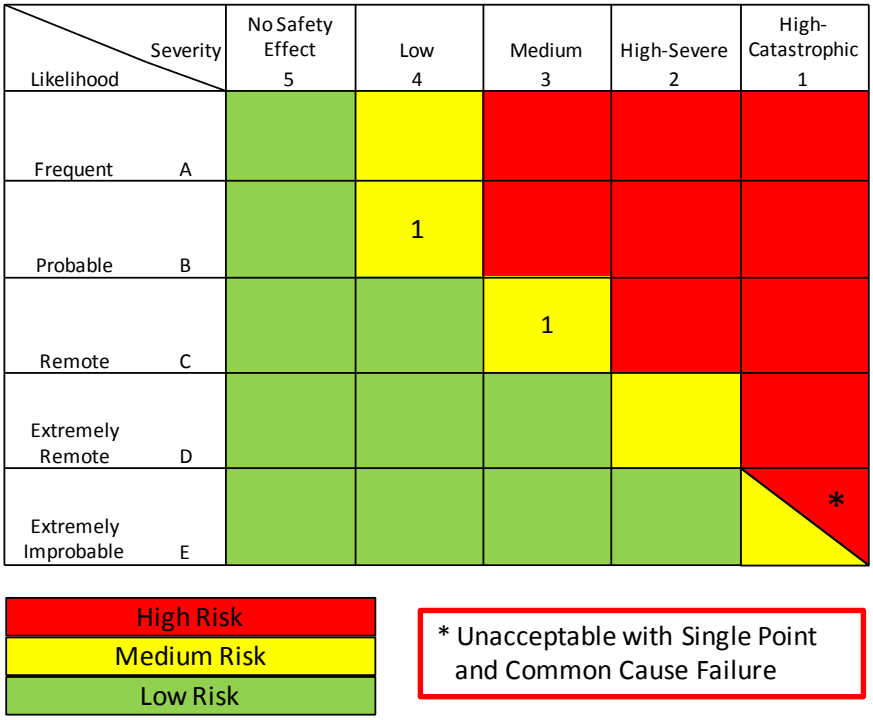

Figure 30.—Safety risk matrix, loss of service.

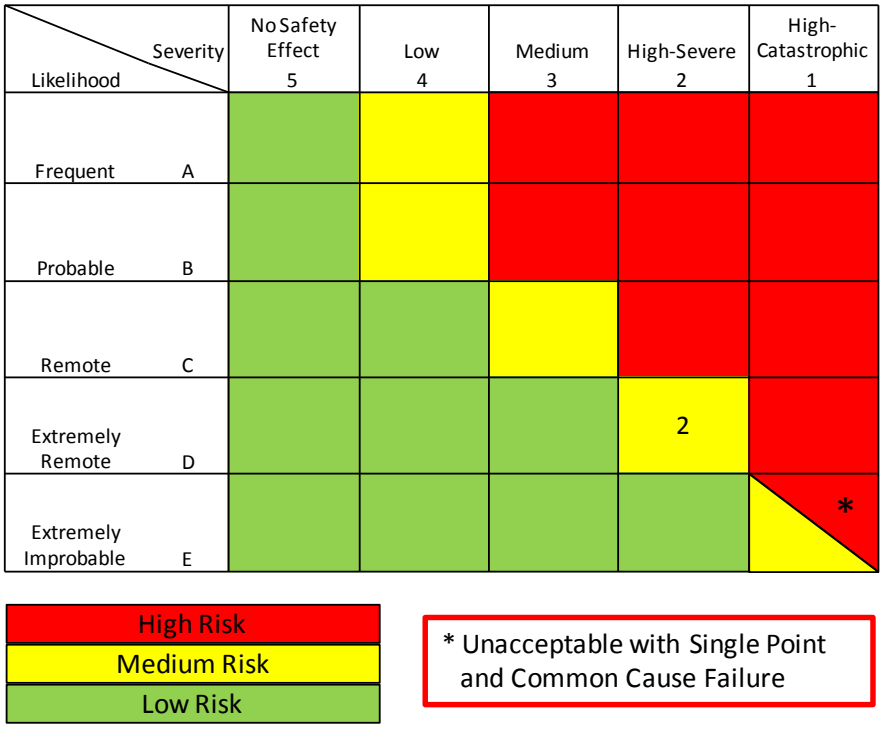

Figure 31.—Safety risk matrix, hazardously misleading information.

As described in the COCR (Ref. 8), Table 11 provides safety assessment for each ATS service. The column headers are defined as follows:

- **Service**.—The acronym for the ATS service.
- **Integrity**.—The safety effect when an undetected error occurs.
- **Continuity**.—The safety effect when communications fails once started.
- **Availability of Provision**.—The safety effect when unable to communicate to all aircraft.
- **Availability of Use**.—The safety effect when unable to communicate with one aircraft.

TABLE 11.—SERVICE-LEVEL SAFETY ASSESSMENT[a]

Service	Continuity	Integrity	Availability (provision)	Availability (use)
D-OTIS	Minor	Hazardous	Major	Minor
D-SIG	Minor	Hazardous	Minor	Minor
D-RVR	Minor	Hazardous	Major	Minor
WAKE	Major	Hazardous	Minor	Minor
FLIPCY	Major	Hazardous	Hazardous	Major
PPD	No safety effect	Minor	No safety effect	No safety effect
D-SIGMET	Minor	Hazardous	Minor	Minor

[a]Acronyms are defined in Appendix A.

It should be noted that the COCR Version 2.0 document safety assessment focused on safety objectives and possible consequences of safety lapses and did not identify causes of potential safety hazards and/or performance degradation.

Appendix E.—Existing National Airspace System Communications System Safety Controls

Existing National Airspace System (NAS) communications system safety controls provided in the NAS Communications System Safety Hazard Analysis and Security Threat Analysis document (Ref. 5) were reviewed. Most, but not all, of the controls were found applicable to the proposed C-band system. Additional controls were considered. The new AeroMACS shall comply with the performance and infrastructure requirements.

Table 12 includes the required controls and identifies procedures, environment, requirements, etc. that reduce the probability of occurrence of the hazard, limit the severity, and/or reduce the likelihood of occurrence of the worst credible effect (WCE) and shall be implemented by program to meet the identified risk or risk assessment code (RAC) for each hazard.

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
1	The air-ground terminal communications (TCOM) and en route communications (ECOM) communication shall be in accordance with Communication Diversity Order 6000.36A.	Existing control applies
2	The NAS shall provide air-ground (A/G) communications capabilities on a continuous basis (NAS–SR–1000 3.6.1.E).	The NAS shall provide A/G communications continuously (NAS SR–1000, part of 20330). Control applies to air/air (A/A) and A/G communications.
3	The A/G communication system shall comply with critical services performance requirements: Availability: 0.99999. No single point of failure of equipment, system, installation or facility shall cause loss of service to the user/specialist. The goal for a single loss of critical service to a user/specialist shall not exceed the duration of 6 seconds. The frequency of occurrence goal for any loss of service shall not exceed one per week (NAS SR–1000 Section 3.8.1 Operational Readiness, Table 3.6.1).	The NAS shall provide service availability not less than that provided by existing capabilities. Critical Services: 0.99999 Essential Services: 0.999 Routine Services: 0.99 (NAS SR 1000, 21470) The NAS shall strive to restore critical system service to users/specialists within 6 seconds of failure (NAS SR–1000, 22900). The NAS shall strive to restore routine system service to users/specialists within 1.68 hours of failure (NAS SR–1000, 22920). The NAS shall strive to restore essential system service to users/specialists within 10 minutes of failure (NAS SR–1000, 22910). No single point of failure of equipment, system, installation or facility shall cause loss of service to the user/specialist.
4	The NAS shall provide specialists with the capability to communicate with aircraft and vehicles in the airport movement area. Alternative forms of communication, such as visual signals transmitted by specialists, shall be provided in case normal A/G voice and data communications fail or are unavailable (NAS–SR–1000 3.2.11.F).	Existing control applies. Reference not found in the new version of the NAS SR–1000.
5	The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft (FAA Order 7110.65 91.3(a)).	Existing control applies.
6	Standard no com procedures: Lost communications procedures are prescribed. (Aeronautical Information Manual (AIM) 4–2–13) and Standard pilot procedures two-way radio communication failure Federal Aviation Regulation (FAR) 91.113 • Alternate control procedure (i.e., light gun instructions from towers) • See-and-avoid procedures are prescribed (AIM 5–5–8 and FAR 91.113).	Existing control applies.

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
7	Current separation standards (FAA order 7110.65)	Existing control applies.
8	Procedures for maintaining clearance limits (definitions of clearance limit are FAA Pilot/Controller Glossary also the ICAO definition, ATC Clearance limit procedures are prescribed (7110.65, 4-6-1a Clearance Limit and FAR 91.185)) • ICAO PANS–RAC 4444: paragraph 5.2.1.1 "No clearance shall be given to execute any maneuver that would reduce the spacing between two aircraft to less than the separation minimum."	Existing control applies.
9	Aircraft under radar and/or visual surveillance (except ocean and some ground environments in IMC). (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5, Radar and Visual, p. 7-2-1.)	Existing control applies.
10	Aircraft-to-aircraft communications remains available (airborne or on-ground).	Existing control applies.
11	ATC procedures to transfer communication functions (after communication failure) to other positions/sectors/facilities are prescribed (7110.65, 10-4-4).	Existing control applies.
12	Possible alternative communications capabilities (e.g., cell phone, public telephone, AOC, satellite phone when available relay (neighboring facility). Local SOP tailored to that facility and good operating procedures or FAA Order 7110.65P Effective Data August 4, 2005 Chapter 10 Emergencies section 1 General 10-1-1d.	Existing control applies.
13	TCAS is available for transport category aircraft (FAR 14CFR Part 129.18).	Existing control applies.
14	Procedures requiring "pilot acknowledgement/read back" when ATC issues clearances or instructions (7110.65, 2-4-3).	Existing control applies.
15	Controllers can also determine aircraft action through surveillance; IDENT, observing radar screen (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5, Radar).	Existing control applies.
16	Controllers are required to order a clearance such that the critical information cannot be lost due to a failure truncating a message.	Existing control applies.
17	A/A communications still available, so another aircrew may hear a step on or incorrect read-back and notify, and/or aircraft can announce intentions on party line.	Existing control applies.
18	Procedures requiring aircraft identification for clearance (7110.65, 2-4-20) • Call sign/runway ID (not shortened call sign) • Procedures for identification of the aircraft requesting clearances • Procedures for giving aircraft ID in granting clearances	Existing control applies.
19	Procedures requiring facility identification (7110.65, 2-4-8) for the ATC facility giving the clearances.	Existing control applies.
20	ICAO Annex 11: paragraph 3.5.1 "A controlled flight shall be under the control of only one air traffic control unit at any given time." • The aircraft shall accept clearances/instructions only from the current control authority.	Existing control applies.
21	The intended recipient is also listening so he/she may query or chime in (party line).	Existing control applies.
22	Voice procedures • Procedures for giving aircraft ID in granting clearances • Procedures for communication when aircraft have same or similar call signs	Existing control applies. Voice would provide backup communication.

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
23	Voice and data communications shall have the following response capabilities: • Initiation of one-way A/G voice transmissions shall be possible within 250 milliseconds of keying the specialist's microphone. • The G/A transmission time for data messages shall not exceed 6 seconds (NAS–SR–1000 3.6.1.A.5).	The NAS shall assure G/A transmission time for data messages not exceed 6 seconds (NAS SR–1000, 20090).
24	Time-critical clearance can be sent with constraint (e.g., to reach by, cross at or before etc.). Thus if message was too late then aircrew would have send an UNABLE response. FAA Order 7110.65P (Chapter 4, Section 3 Departure Procedures 4-3-4 a. Clearance Void Times).	Existing control applies.
25	ADS report (surveillance) can provide aircraft position (FAA Order 7110.65P Effective Data August 4, 2005, Chapter 5 Radar).	Existing control applies.
26	CPDLC pilot position reports can provide aircraft position.	Existing control applies.
27	Oceanic separation standards (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 8 Offshore/Oceanic Procedures).	N/A
28	Clearly intelligible A/G voice communications shall be provided (NAS-SR-1000 3.6.1.A).	The NAS shall provide intelligible air-ground voice communications (NAS SR-1000, 20040).
29	Procedures requiring Emphasis for Clarity (7110.65, 2-4-15).	Existing control applies.
30	Only one pre-departure clearance (PDC) is sent (thus cannot get out of order).	Existing control applies.
31	Airport design minimizes runway and taxiway crossing by vehicles.	Existing control applies.
32	Standard no com procedures.	Covered by Control 6.
33	Vehicle operation training/ licensing for airport operations Part 139.329(e) requires that "each certificate holder shall -- ensure that each employee, tenant, or contractor who operates aground vehicle on any portion of the airport that has access to the movement area is familiar with the airport's procedures for the operation of ground vehicles and the consequences of noncompliance." To comply with Part 139.329(e), airport operators should have a ground vehicle guidebook for training personnel authorized to operate a ground vehicle on the airport. Part 139.301 Records – ground vehicle training; 139.303 Personnel Sufficient Qualified Personnel (303a), Properly Equipped (303b), Trained (303c), Record of Training for 24 CCM (303d).	Existing control applies.
34	Vehicles all yield to aircraft: AC 150/5210-20 Ground Vehicle Operations on Airports - guidance to airport operators in developing training programs for safe ground vehicle operations, Sample Ground Vehicle Operations Training Manual Appendix B 1.7.10. No vehicle operator shall enter the movement area— a. Without first obtaining permission of the (AIRPORT OPERATOR) and clearance from the ATCT to enter the movement area; b. Unless equipped with an operable two-way radio in communication with the ATCT; or c. Unless escorted by an (AIRPORT OPERATOR) vehicle and as long as the vehicle remains under the control of the escort vehicle.	Existing control applies.
35	Vehicles under visual surveillance or radar/multi-lateration surveillance: FAA Order 7110.65, Air Traffic Control Handbook, paragraph 3-1-3, "Use of Active Runways," states, "The local controller has primary responsibility for operations conducted on the active runway and must control the use of those runways." Paragraph 3-1-12, "Visually Scanning Runways," states that, "Local controllers shall visually scan runways to the maximum extent possible."	Existing control applies.
36	Mobile-to-mobile communications still available	Existing control applies.

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
37	The NAS shall provide specialists with the capability to communicate with aircraft and vehicles in the airport movement area. Alternative forms of communication, such as visual signals transmitted by specialists, shall be provided in case normal A/G voice and data communications fail or are unavailable (NAS–SR–1000 3.2.11.F).	Covered by Control 4.
38	Possible alternative communications capabilities e.g., cell phone, ATCT light gun procedures.	Covered by Control 12.
39	Title 14, Code of Federal Regulations (CFR), Part 139 (14 CFR Part 139] requirement to familiarize vehicles for operating on a given airport.	Existing control applies.
40	FAA Order 7110.65, Air Traffic Control Handbook, paragraph 3-1-3, Use of Active Runways, The local controller has primary responsibility for operations conducted on the active runway and must control the use of those runways.	Existing control applies.
41	AC 150/5340-18D Standards for Airport Sign Systems Part 139.311 CFR MARKING, SIGNS AND LIGHTING AC 150/5210-22 Airport Certification Manual (ACM): Paragraph 302(a) “Airport sign and marking plans must receive FAA approval before they are implemented” Chapter 5. Section 139.311 “Include in the ACM a legible color diagram of the airport sign and marking systems.”	Existing control applies.
42	FAA Order 7110.65 Paragraph 3-1-12, Visually Scanning Runways - Local controllers shall visually scan runways to the maximum extent possible.	Existing control applies.
43	CFR Part 139.329(b) airport operators are required to establish and implement procedures for operation of ground vehicles in the safety area as well as the movement area.	Existing control applies.
44	CFR Part 139.205(b)(19) requires that these procedures be included in the Airport Certification Manual (ACM).	Existing control applies.
45	Controller use of full call sign/runway ID (not shortened) (FAA Order 7110.65P 3-7-1 Ground Traffic Movement Phraseology).	Existing control applies.
46	Controllers must establish position before moving vehicle (FAA Order 7110.65 Section 1 General 3-1-7 Position Determination).	Existing control applies.
47	Procedures for identification of vehicles requesting clearances (Part 139CFR ground vehicle guidebook for training).	Existing control applies.
48	Controller procedures for giving vehicle ID in granting clearances (FAA Order 7110.65 Section 7 Taxi and Ground Movement Procedures 3-7-2 Taxi and Ground Movement Operations).	Existing control applies.
49	Vehicle readback procedures (voice) (Part 139CFR ground vehicle guidebook for training).	Existing control applies.
50	Intrafacility communication requirements have been minimized due to automation of many functions.	N/A
51	Controller/assistant/supervisor can walk over and talk to other controller.	N/A
52	Voice messages would not get a proper acknowledgement, when truncated due to a failure (Procedure between interphone intra/interfacility communication that utilize numeric position identification, the caller must identify both position and facility (FAA Order 7110.65P 2-4-12 Interphone Message Format) e. The receiver states the response to the caller's message followed by the receiver's operating initials. f. The caller states his or her operating initials).	N/A
53	SR-1000: 3.6.2A 1: The NAS shall provide direct-access voice communications connectivity between specialist in on ATC facility and designated specialist in another facility as shown in Table 3-1. The number of direct-access calls that are blocked because of saturation of equipment shall not exceed 1 in 1000 calls.	N/A

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
54	Other facility can be reached by other means (Local Contingency Plan—FAA Order 7210.3 Facility 2-1-7 Air Traffic Service (ATS) Continuity a. Facilities shall develop and maintain current operational plans and procedures to provide continuity of required services during emergency conditions (e.g., power failures, fire, flood) b. Contingency plans). · Relay through aircraft · Cell phones · Public phone system (FAA Order 7210.3 Section 3, 3-3-1. SERVICE "F" COMMUNICATIONS Facility AT managers shall establish procedures to provide interim communications in the event that local or long-line standard Service "F" fail. These shall include the use of telephone conference circuits and the use of airline or other facilities; 3-3-2. TELEPHONE COMMUNICATIONS).	N/A
55	Facilities periodically check availability of communications with other facilities and would be aware of loss of communications.	N/A
56	Procedures exist to transfer control to another facility in case of failure. (e.g., primarily redundancy: ARTCC to ARTCC and ARTCC to Command Center rely through third party) FAA Order 7210.3 Facility Operation and Administration; Section 3. Letters of Agreement (LOA) 4-3-1. LETTERS OF AGREEMENT; 4-3-2. APPROPRIATE SUBJECTS Examples of subjects of LOAs are: a. Between ARTCCs: 1. Radar handoff procedures.2. Interfacility coordination procedures.3. Delegation of responsibility for IFR control jurisdiction.	N/A
57	Procedures exist to have aircraft initiate transfer with receiving facility (FAA Order 7110.65P 8-2-2 Transfer of Control and Communications).	N/A
58	Automation and visual alerts to detect • Aircraft positions • Out-of-conformance • Potential conflicts	N/A
59	7110: IFR operations in any class of controlled airspace, a pilot must receive an appropriate ATC clearance prior to entering in the airspace.	N/A
60	Interfacility data communications shall be provided with error detection and correction capabilities (NASSRS 3.6.3.A.11) NAS systems digital circuits basic requirement to provide in excess of 99.9% error-free seconds.	N/A
61	NAS–SR–1000 p3.6.2.A.3 Ground-Ground Interfacility Communications Connectivity 5) Clearly intelligible interfacility voice communications shall be provided.	N/A
62	FTI Attachment J.1, FAA Telecommunications Services Description (FTSD): Voice Quality Mean Opinion Score (MOS) equal to or greater than 4.3.	N/A
63	ATC uses judgment whether or not to clear aircraft to land (FAA Order 7110.65P 3-1-5. Vehicles/equipment/ personnel on runways).	N/A
64	The NAS shall provide the specialist with an unobstructed view of the airport movement area (NAS–SR–1000 3.2.11.D).	N/A
65	The NAS shall be capable of continuously broadcasting the latest approved aerodrome and terminal area conditions on communications media that can be accessed by aircraft in flight and on the ground (NAS–SR–1000 3.3.3.B).	N/A
66	Aeronautical information shall be continuously (24 hours a day) accessible to specialists (NAS–SR–1000 3.1.2.B).	N/A
67	Aeronautical information shall be continuously (24 hours a day) accessible to users upon request with or without the aid of specialists (NAS–SR–1000 3.1.2.C).	N/A
68	Aeronautical information shall be obtainable along a specified route, or in conjunction with specified locations or areas, or by reporting location. (NAS–SR–1000 3.1.2.D).	N/A

TABLE 12.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no.[a]	Existing National Airspace System (NAS) controls	Proposed controls
69	Real-time required communication between FIRs has been minimized; most transfers can be done sufficiently in advance. (FAA Order 7110.65P Section 8-2-1 Coordination)	N/A
70	Foreign ATC can be reached by other means • Relay through aircraft • Cell phones • Public phone system	N/A
71	In a two-way exchange; usually getting cut-off etc. would be detected by one or both parties and coordination would be attempted again; it would be rare for the failure to go undetected.	N/A
72	Boundary coordination times are agreed by memorandum of understanding between FIRs (FAA Order 7110.65P 8-2-2).	N/A
73	Receiving ground system has flight plan (FAA Order 7110.65P 8-2-1 a).	N/A
74	Receiving ground system would initiate coordination/transfer (FAA Order 7110.65P 8-2-2).	N/A
75	ICAO format boundary coordination messages are tagged and time stamped.	N/A
76	AOC-ATC messages cannot affect separation.	N/A
77	Aircraft have highly reliable systems (AC-25-11 viii, Loss of all communication functions must be improbable; RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware; AC 25.1309-1A (Air Transport) SYSTEM DESIGN AND ANALYSIS; AC 23.1309-1C (General Aviation) EQUIPMENT, SYSTEMS, AND INSTALLATIONS IN PART 23 AIRPLANES;FAA FAR 121 requirement of "two means of communication for the intended operating environment").	Existing control applies.
78	Standard operating procedures/pilot training.	Existing control applies.
79	Redundancy to prevent interruption, centers can talk to multiple facilities (2 or 3 facilities typical) and command center.	N/A
80	Diverse entry points into facilities (Communication Diversity Order 6000.36 A).	N/A
81	Procedure to switch to emergency operational AT procedures. (FAA Order 7210.3 Facility Operation and Administration Section 3 letters of agreement (LOAs) 4-3-1 Letters of Agreement; g. Establish responsibilities for: 2. Providing emergency services).	N/A
82	Procedure to switch to FAA-owned communications systems—FAATSAT transportable equip., RCL, portable A/G radio.	N/A
83	IDAT parity and checksum to reliably detect corruption of the message.	N/A
84	ATC able to transmit command clearances and receive pilot feedback via equipment other than com radio (e.g., transponder, navigation radio) (FAA Order 7110.65, 10-4-4, 3-2-1, FARs 91.215, 91.205)	Existing control applies.
85	Data link messages are time stamped so order can be determined.	Existing control applies.
86	Data link response message indicate to which message they refer.	Existing control applies.
89		The NAS shall comply with national standards to avoid the interference of new systems with existing systems (NAS SR-1000, 19310).
90		C-band system shall comply with the performance and infrastructure requirements.

[a]Control numbers 1 to 83 correspond to the Existing Controls, Table 2-3 of Ref. 5. Controls 84 to 86 are noted in the above document but not listed in Table 2-3. Controls beyond 86 are additional controls suggested for the proposed L-DACS

References

1. Safety Risk Management Guidance for System Acquisitions (SRMGSA), U.S. Department of Transportation Federal Aviation Administration Air Traffic Organization, Safety Services February 8, 2007.
2. FCI Aeronautical Data Services Definition Task Report, ITT AES, March 31, 2009.
3. National Airspace System (NAS) System Engineering Manual, Version 3.1, Federal Aviation Administration ATO Operations Planning, June 6, 2006.
4. FAA Air Traffic Organization Safety Management System Manual, Version 2.1, 2008.
5. National Airspace System Communication System Safety Hazard Analysis and Security Threat Analysis, Federal Aviation Administration, February 21, 2006.
6. Hall, E., Issacs, J.; Zelkin, N.; and Henriksen, S. C-Band Airport Surface Communications System Standards Development. Phase I Final Report. NASA/CR—2010-216324, 2010.
7. RTCA DO–290, Safety and Performance Requirements Standard for Air Traffic Data Link Services in Continental Airspace (Continental SPR Standard), April 29, 2004.
8. Communications Operating Concept and Requirements for the Future Radio System (COCR), Eurocontrol/FAA, Version 2.0, May 2007.
9. RTCA SC–203 Operational Services and Environmental Definition (OSED), Draft, October 23, 2009.
10. Preliminary Draft New Report ITU–R M. [UAS–SPEC], Characteristics of Unmanned Aircraft Systems (UAS) and Spectrum Requirements to Support their Safe Operation in Non Segregated Airspaces, August 4, 2009.
11. System Wide Information Sharing (SWIM), FAA, Presented to: SWIM TIM on Infrastructure and Technology by Mike Hritz FAA SWIM Planning and Prototyping Lead, May 14, 2008.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-02-2011	Final Contractor Report	

4. TITLE AND SUBTITLE
C-Band Airport Surface Communications System Engineering--Initial High-Level Safety Risk Assessment and Mitigation

5a. CONTRACT NUMBER
NNC05CA85C

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Zelkin, Natalie; Henriksen, Stephen

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
WBS 031102.02.03.02.0677.09

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
ITT Corporation Advanced Engineering & Sciences Division
12975 Worldgate Drive
Herndon, Virginia 20170

8. PERFORMING ORGANIZATION REPORT NUMBER
E-17259

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITOR'S ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER
NASA/CR-2011-216325

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category: 04
Available electronically at http://ww.sti.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 443-757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document is being provided as part of ITT's NASA Glenn Research Center Aerospace Communication Systems Technical Support (ACSTS) contract: "New ATM Requirements--Future Communications, C-Band and L-Band Communications Standard Development." ITT has completed a safety hazard analysis providing a preliminary safety assessment for the proposed C-band (5091- to 5150-MHz) airport surface communication system. The assessment was performed following the guidelines outlined in the Federal Aviation Administration Safety Risk Management Guidance for System Acquisitions document. The safety analysis did not identify any hazards with an unacceptable risk, though a number of hazards with a medium risk were documented. This effort represents an initial high-level safety hazard analysis and notes the triggers for risk reassessment. A detailed safety hazards analysis is recommended as a follow-on activity to assess particular components of the C-band communication system after the profile is finalized and system rollout timing is determined. A security risk assessment has been performed by NASA as a parallel activity. While safety analysis is concerned with a prevention of accidental errors and failures, the security threat analysis focuses on deliberate attacks. Both processes identify the events that affect operation of the system; and from a safety perspective the security threats may present safety risks.

15. SUBJECT TERMS
Aircraft communication; Wireless communications; Airports; Air traffic control

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email:help@sti.nasa.gov)
U	U	U	UU	62	19b. TELEPHONE NUMBER *(include area code)* 443-757-5802