



L-Band Digital Aeronautical Communications System Engineering—Preliminary Safety and Security Risk Assessment and Mitigation

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

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



L-Band Digital Aeronautical Communications System Engineering—Preliminary Safety and Security Risk Assessment and Mitigation

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

Prepared for the
International Civil Aviation Organization (ICAO) and Aeronautical Communications Panel (ACP)
Working Group Meeting No. 16
sponsored by the International Civil Aviation Organization (ICAO)
Paris, France, May 17–21, 2010

Prepared under NNC05CA85C

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

Trade names and trademarks are used in this report for identification only. Their usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

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

A safety hazard analysis was completed providing a preliminary safety assessment for the proposed L-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). It was delivered to NASA on December 19, 2009, under the fiscal year 2009 project-level agreement.

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 a preliminary safety hazard analysis. Section 3.6 details recommended triggers for risk reassessment. A detailed safety hazards analyses should be performed as a follow-on activity to assess particular components of the L-band communication system after the technology is chosen and system rollout timing is determined.

The security risk analysis resulted in identifying main security threats to the proposed system as well as noting additional threats recommended for a future security analysis conducted at a later stage in the system development process. The document discusses various security controls, including those suggested in the COCR Version 2.0 (Ref. 2).

Contents

1.0	INTRODUCTION	1
1.1	Document Overview.....	2
2.0	SCOPE	3
2.1	Risk Management Objective	3
2.2	Types of Identified Risks	4
2.3	System Safety Engineering and Information Security Engineering.....	5
3.0	SAFETY RISKS MANAGEMENT	6
3.1	Safety Analysis Requirement	6
3.2	Process.....	6
3.3	System Description.....	8
3.4	Safety Risk Identification	10
3.5	Safety Risks Analysis and Assessment.....	12
3.5.1	Hazard Severity Definition and Safety Likelihood Categories	12
3.5.2	L-band System Safety Risks Matrix.....	14
3.5.3	Unmanned Aircraft System (UAS)-Related Services Safety Risks	16
3.5.4	Airborne System Wide Information Management (SWIM) Suitable Services Safety Assessment.....	18
3.6	L-band Communication System Safety Risks Treatment.....	19
3.6.1	Risk Mitigation.....	19
3.6.2	Safety Risks Maintenance	21
4.0	INFORMATION SECURITY ENGINEERING AND SECURITY RISK MANAGEMENT	22
4.1	Information Security Engineering Objective and Scope	22
4.2	Information Security Engineering and Security Risk Management Process.....	22
4.3	Inputs to Information Security Engineering and Security Risk Management.....	27
4.4	Security Threat Identification.....	28
4.5	Security Risks Analysis and Assessment.....	29
4.6	Security Risks Treatment	32
4.6.1	Summary of the Applicable COCR Version 2.0 Security Analysis.....	32
4.6.2	Further Analysis Based on NIST SP800-53	34
4.6.3	Continued Security Assessment.....	34
	APPENDIX A.—ACRONYMS AND ABBREVIATIONS.....	35
	APPENDIX B.—HIERARCHICAL DIAGRAMS OF FUNCTIONAL REQUIREMENTS.....	39
	APPENDIX C.—SAFETY HAZARD ANALYSIS WORKSHEETS	47
	C.1 L-band Communication Safety Hazard Analysis (SHA) Table Cross Reference	47
	C.2 Hazard Analysis Worksheets.....	48
	APPENDIX D.—SUMMARY OF THE OPERATIONAL SAFETY ASSESSMENT FOR THE ATS SERVICES IDENTIFIED FOR L-BAND APPLICATION	65
	D.1 Safety Objectives Definitions.....	65
	D.2 Summary of the L-band ATS Services Operational Safety Assessment.....	65
	D.3 Service-Level Safety Assessment (L-band Services Only).....	67
	APPENDIX E.—EXISTING NATIONAL AIRSPACE SYSTEM COMMUNICATIONS SYSTEM SAFETY CONTROLS	69
	APPENDIX F.—SP 800-53 SECURITY CONTROLS APPLICABLE TO L-DACS	77
	REFERENCES	81

List of Figures

Figure 1.—Risk in system engineering (Ref. 6).	3
Figure 2.—Types of potential risks.	4
Figure 3.—Safety risk management—inputs to the process (Acronyms defined in Appendix A).	7
Figure 4.—Safety risk management process.	7
Figure 5.—Safety risk management decision flow chart (Ref. 7).	8
Figure 6.—Communications systems covered by this document (slightly altered Figure 1-1 from Ref. 11)	9
Figure 7.—Federal Aviation Administration risk management risk identification flow chart (Ref. 6).	10
Figure 8.—Functional hazard categories. Acronyms are defined in Appendix A.	11
Figure 9.—L-band system safety risk matrix air-traffic-services-to-aircraft communication.	15
Figure 10.—L-band system safety risk matrix aircraft-to-aircraft communication.	16
Figure 11.—Risk acceptance criteria (Ref. 1).	16
Figure 12.—Unmanned aircraft system (UAS) applications (from proposed changes to Ref. 13).	17
Figure 13.—Airborne SWIM and other NextGen programs (Ref. 14). Acronyms are defined in Appendix A.	19
Figure 14.—Risk strategy options.	20
Figure 15.—Correlation of information security methodology with Federal Aviation Administration (FAA) risk management model (Ref. 6). Acronyms are defined in Appendix A.	23
Figure 16.—Correlation between security threat analysis and safety hazard analysis.	24
Figure 17.—Federal Aviation Administration (FAA) security policy and guidance (slightly modified figure from Ref. 19).	28
Figure 18.—Security risk assessment matrix.	32
Figure 19.—L-band communications system high level.	39
Figure 20.—Decomposition of use L-band communications system (transmit/receive messages).	39
Figure 21.—Decomposition of transceive fixed-to-mobile message.	40
Figure 22.—Decomposition of transceive mobile-to-fixed message.	40
Figure 23.—Decomposition of transceive airborne-mobile-to-airborne-mobile messages.	41
Figure 24.—Generic decomposition of transceive data message.	41
Figure 25.—Generic decomposition of initiate data message.	41
Figure 26.—Generic decomposition of process data message for sending.	42
Figure 27.—Generic decomposition of send data message.	42
Figure 28.—Generic decomposition of process received data message.	42
Figure 29.—Generic decomposition of deliver data message.	42
Figure 30.—Generic decomposition of provide failure processing.	43
Figure 31.—Decomposition of operate L-band communications system.	43
Figure 32.—Decomposition of monitor L-band communications system.	43
Figure 33.—Decomposition of configure L-band communications system.	44
Figure 34.—Decomposition of maintain L-band communications system.	45
Figure 35.—Safety risk matrix—loss of service.	66
Figure 36.—Safety risk matrix—hazardously misleading information.	67

List of Tables

TABLE 1.—CHANGES REQUIRING SAFETY ANALYSIS	6
TABLE 2.—SAFETY HAZARDS CATEGORIES	11
TABLE 3.—DESCRIPTION OF HAZARD SEVERITY (REF. 2).....	13
TABLE 4.—SAFETY LIKELIHOOD CATEGORIES ^a	13
TABLE 5.—L-BAND COMMUNICATIONS SYSTEM SAFETY RISK SUMMARY	14
TABLE 6.—UNMANNED AIRCRAFT SYSTEM OPERATIONAL SCENARIOS	18
TABLE 7.—SECURITY SEVERITY CATEGORIES (REF. 10).....	25
TABLE 8.—L-BAND COMMUNICATION SYSTEM HIGH-LEVEL THREATS	28
TABLE 9.—INFORMATION SECURITY THREAT SEVERITY FOR L-BAND SYSTEM SERVICES ^{a,b}	30
TABLE 10.—THREAT LIKELIHOOD AND SEVERITY.....	31
TABLE 11.—PROPERTIES OF SECURITY CONTROLS ^a	33
TABLE 12.— SAFETY HAZARD ANALYSIS TABLE CROSS REFERENCE ^{a,b}	47
TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM	51
TABLE 14.—AIRCRAFT-TO-AIRCRAFT MESSAGE HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM	63
TABLE 15.—SAFETY OBJECTIVE DEFINITIONS (REF. 2).....	65
TABLE 16.—AIR TRAFFIC SERVICES OPERATIONAL SAFETY ASSESSMENT HAZARD SEVERITY AND SAFETY OBJECTIVES	66
TABLE 17.—SERVICE LEVEL SAFETY ASSESSMENT	67
TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS	69
TABLE 19.—SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS	77
TABLE 20.—SECURITY CONTROLS RELEVANT TO THE PROPOSED L-DACS.....	77

1.0 Introduction

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-EUROCONTROL cooperative research Action Plan (AP-17), also known as the Future Communications Study (FCS). NASA and 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 Next Generation Air Transportation System (NextGen) Integrated Work Plan (Ref. 3) and are represented in the National Airspace System (NAS) Enterprise Architecture Communications and Avionics Roadmaps.

Action Plan 30 (AP-30), a follow-on cooperative research to AP-17, is expected to start in fiscal year (FY) 2010 to ensure coordinated development of the FCI to help enable the advanced ATM concepts of operation 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 an FY09 Solution Set Work Plan for C-band and L-band future communications research under the section, "New Air Traffic Management (ATM) Requirements."

On 27 February 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 that solution set work plan that includes development of concepts of use, 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 document presents the preliminary safety and security risk assessment for L-band communications systems. The assessment draws on the functional system analysis conducted earlier and documented in the Concepts of Use (CONUSE), System Performance Requirements, and Architecture deliverable for Subtask 7-2A/B (Ref. 4).

In addition to potentially providing an alternative link technology suitable to support the FAA's Data Communications (Data Comm) Segment 3 requirements, including full four-dimensional trajectory-based operations, the L-band terrestrial en-route communications system is also envisioned to be able to support other future communications applications including mobile System Wide Information Management (SWIM) and unmanned aircraft system (UAS) safety-critical data communications, UAS command and control, and monitoring of UAS onboard sense-and-avoid and automation capabilities.

Safety hazards identification, analysis, and assessment are performed assuming the services identified as potential applications for the L-band system (Ref. 5). Recommendations for safety risk mitigation techniques follow the analysis.

This document also presents a security risk analysis following FAA security policy and appropriate National Institute of Standards and Technology (NIST) standards and includes security categorization, risks analysis, and controls.

Both safety hazards and security threat analyses rely on FAA guidance documents, such as the NAS System Engineering Manual (Ref. 6), the Safety Management System Manual (SMS) (Ref. 7), and the System Safety Handbook (SSH) (Ref. 8) for methodology and process.

1.1 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 2.0 describes methodology and presents the results of safety risk analysis.
- Section 3.0 discusses the issues related to information security and outlines results of the analysis.
- Appendix A presents a list of acronyms used in the report.
- Appendix B presents hierarchical diagrams of functional requirements for the proposed L-band communications system.
- Appendix C contains L-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 identified for L-band application adopted from the analysis presented in the Communications Operating Concept and Requirements (COCR) (Ref. 2).
- Appendix E lists the existing NAS communications system safety controls.
- Appendix F provides SP 800–53 security controls applicable to the L-band digital aeronautical communication system (L–DACS).

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 L-band communication system from both safety and security viewpoints.

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

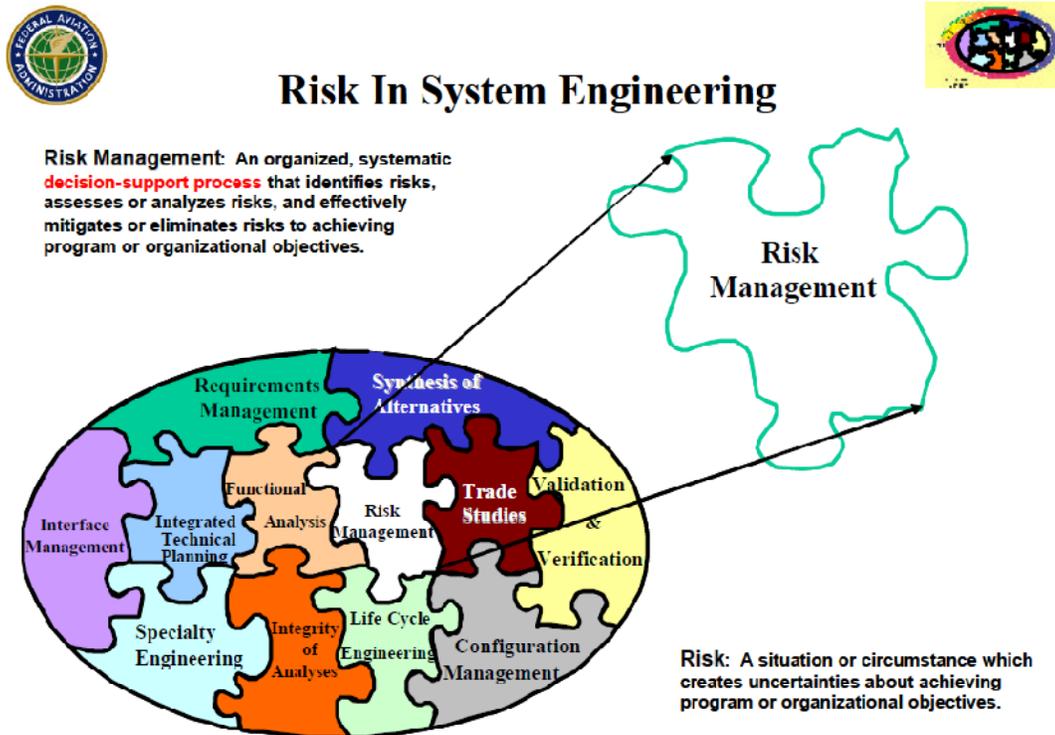


Figure 1.—Risk in system engineering (Ref. 6).

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 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 and the FAA information security methodology (defined within specialty engineering) is correlated with the FAA risk management model (Ref. 6).

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. 6). Rather “in the context of the SMS, safety is defined as freedom from unacceptable risk” (Ref. 7).

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, and business or cost-related.

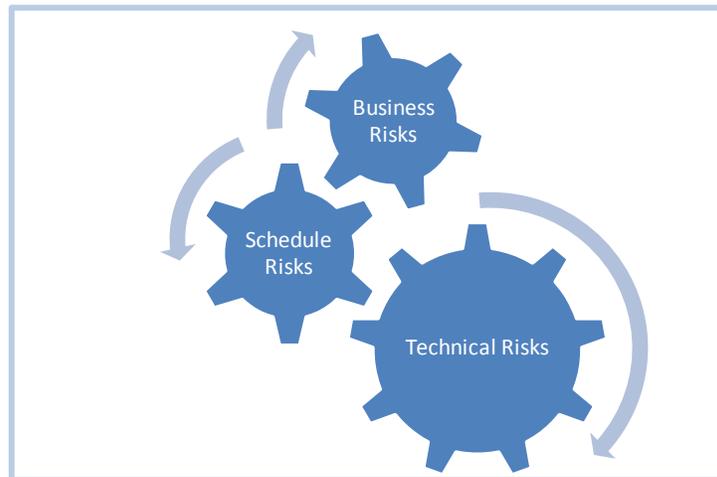


Figure 2.—Types of potential risks.

As explained in the NAS System Engineering Manual (SEM) (Ref. 6):

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 to be out of scope for this task and would significantly depend on system acquisition plan and schedule.

Only safety and security risks will be 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 ground-to-air and air-to-air communications, such as navigation systems and surveillance systems.

It should be noted, however, that the specifics of the L-band system development and dependency on the partnership with the Europeans through Action Plan 30 will affect the schedule and contribute to program risks. Because of recent schedule revisions in European L-band system technology research, development, and prototyping, tasks that include and/or depend on choosing a specific L-band technology or finalizing the requirements, have been postponed. Consequently, because of potential change in technology and operational assumptions, activities completed under Task 7–2, including this document, will need to be revisited when L-band technology decisions have been finalized. This document presents a preliminary risk assessment and mitigation.

At this time, two technologies, L–DACS–1 and L–DACS–2, are being considered for L-band system implementation (Ref. 9).

The first option represents the state of the art in commercial developments employing modern modulation techniques and may lead to utilization/adaptation of COTS products and standards. The second capitalizes on experience from aviation specific systems and standards such as the VHF digital link (VDL) 3, VDL 4, and UAT.

Final selection of the L-band data link technology will determine if any commercial off-the-shelf (COTS) products are used. The risk assessment should be revisited and hazards associated with the uses of COTS should be evaluated at that time as appropriate. COTS-based risk considerations identified in the SEM (Ref. 6) should be used as a starting point for the assessment.

2.3 System Safety Engineering and Information Security Engineering

Two disciplines of specialty engineering (SE), system safety engineering (SSE) and information security engineering (ISE), are applied to conduct the analyses 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. 6)

...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.

For the purposes of this analysis, safety and security risk identification, assessment, and mitigation are addressed separately. However, similarities between the two types of the analysis are underlined throughout the document. Both are based on functional analysis of the L-band system, and both follow suggested FAA methodology for risk analysis. Furthermore, “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. 10). Thus, hazard severity levels can be assigned to the safety hazards that could be caused by security threats.

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 that need to be evaluated for safety risk (Ref. 7) and identifies the changes applicable to the proposed introduction of an L-band system. As noted, only technical aspects of safety risk analysis are covered by this document.

TABLE 1.—CHANGES REQUIRING SAFETY ANALYSIS

Categories of change		Changes applicable to L-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	No
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 (Ref. 6)

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.

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 risk 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. 7).



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.

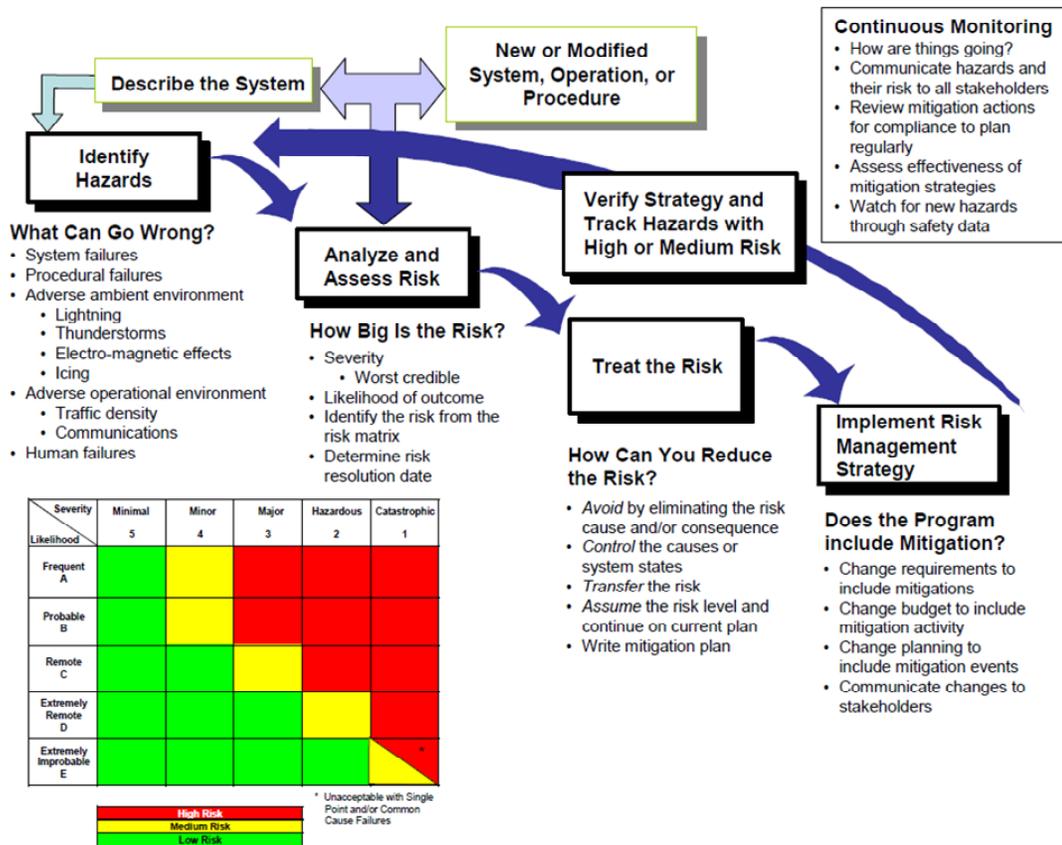


Figure 5.—Safety risk management decision flow chart (Ref. 7).

3.3 System Description

Accurate system description is the first step in a safety hazards analysis. As described in deliverable 7–2A under Task 7, L-band System Engineering Concepts of Use and Systems Performance Requirements (Ref. 4), the system covered by this document will provide air-to-ground communications services in support of ATM, and resides within the dashed red box shown in Figure 6, which 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 air-to-ground communications services; networking subsystems to provide ground-to-ground communications service connectivity to end systems and users; and usually some centralized M&C functionality to monitor and control system operations and performance.

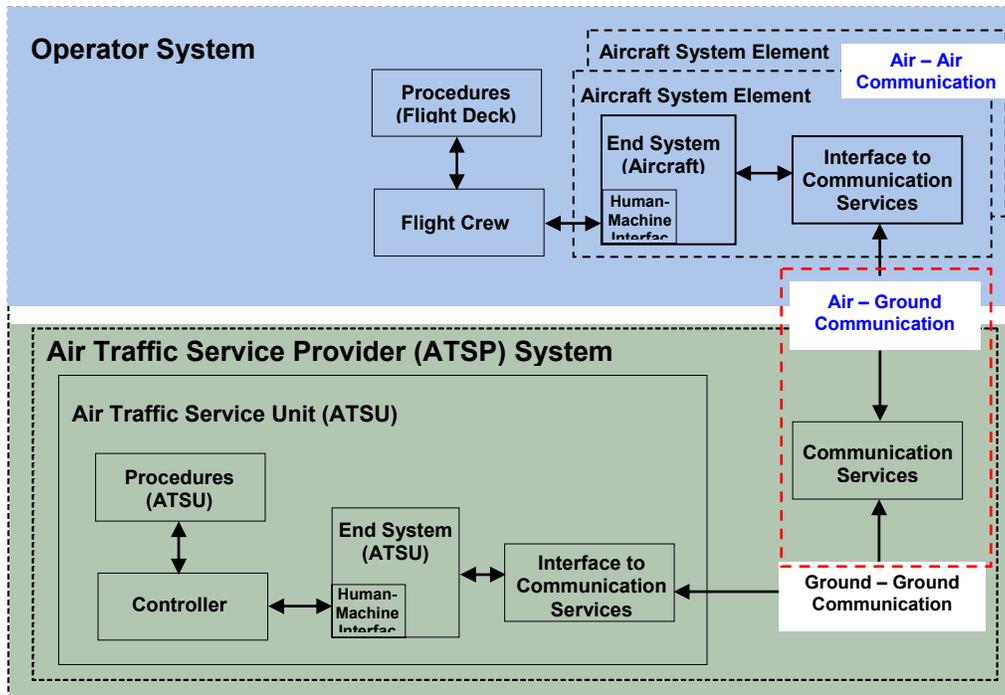


Figure 6.—Communications systems covered by this document (slightly altered Figure 1-1 from Ref. 11)

Although this document supports the development of FAA ground-based systems, the scope of the proposed L-band communications system covers systems providing both ground-to-air and air-to-air communications services. Air-to-air communications is depicted in Figure 6 by showing two aircraft system elements.

It should be noted that while Figure 6 effectively illustrates different types of communications provided by the proposed L-band system—air-to-air and air-to-ground—it depicts air traffic service provider (ATSP) systems only³.

The L-band communications system safety hazard analysis as based on an L-band system functional analysis. This analysis is detailed in the L-band System Engineering—Concepts of Use, Systems Performance Requirements, and Architecture document (Ref. 4). Appendix B of this document contains hierarchical diagrams of the functional requirements for the proposed L-band system. The functional breakdown and methodology are adopted from the NAS Communication System Safety Hazard Analysis and Security Threat Analysis (Ref. 10) and modified as appropriate to reflect the scope and requirements for the proposed L-band system.

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

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

³ 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 includes airport/aerodrome flight information service (AFIS) providers.

Because of regulation constraints governing the aeronautical mobile (route) services spectrum over which the proposed L-band system is intended to operate, fixed-point-to-fixed-point (i.e., nonmobile) communication was determined to be out of scope of the L-band communications system and is not covered by Task 7–2 documents, including this document.

Though the proposed L–DACS could enable ATS, AOC, and aeronautical administrative communication (AAC), ATS are likely to have the strictest safety and security requirements. As such, this document considers ATS being the worst case scenario from the safety view point.

3.4 Safety Risk Identification

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

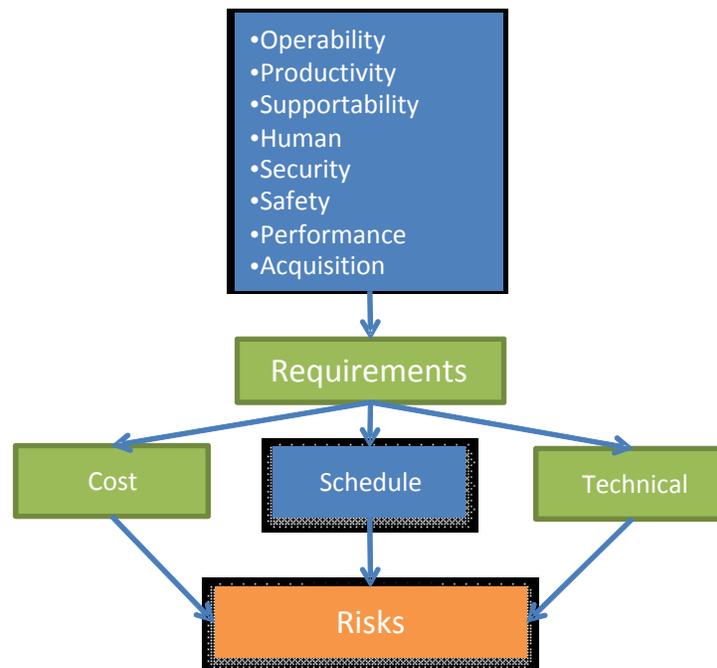


Figure 7.—Federal Aviation Administration risk management risk identification flow chart (Ref. 6).

Although, as identified in Figure 7, multiple factors contribute to the overall program and system risks, the scope of this document is limited to safety and security issues. Security risks are addressed later in this document.

To identify safety hazards for the proposed L-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. 10) were found to be applicable to the proposed L-band system, and the Table 2 shows 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 L-band communication system	L-band communication capability totally unavailable: L-band air traffic services (ATS) failure.
	L-band communication capability partially unavailable: L-band ATS failure.
	L-band system communication capability unavailable: sender to recipient of L-band ATS unavailable.
Hazards due to failures of the L-band communication system	L-band communication fails (e.g., aborts) with a given recipient for a single message.
	L-band communication fails (e.g., aborts) with multiple recipients for a single message per aircraft.
Hazards due to misdelivery of a message by the L-band communication system	The recipient accepts a message affecting separation from an L-band ATS that is not its control authority.
	The recipient accepts a message NOT affecting separation from an L-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 L-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 L-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 L-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 L-band communication system functions shown in Figure 8.

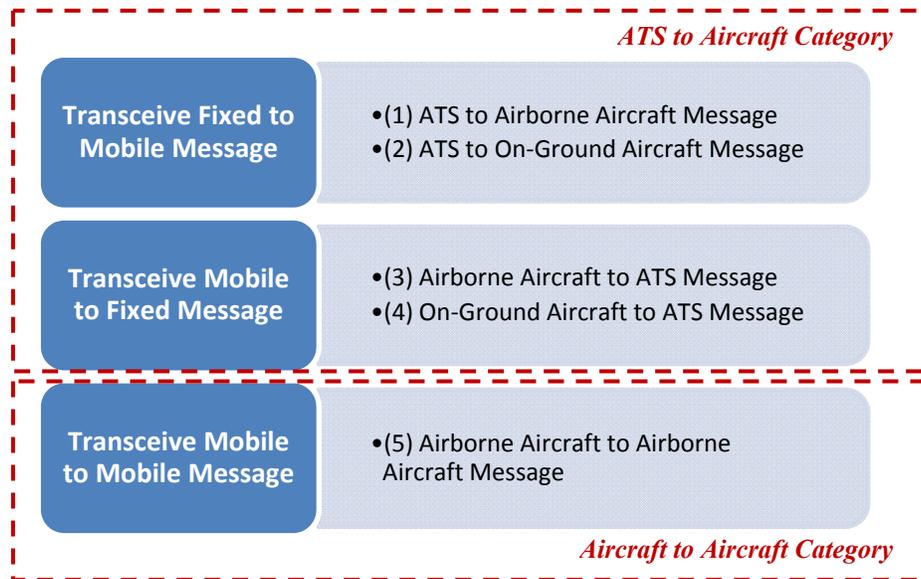


Figure 8.—Functional hazard categories. Acronyms are defined in Appendix A.

Following the methodology suggested in the National Airspace System Communications System Safety Hazard Analysis and Security Threat Analysis document (Ref. 10), fixed-to-mobile and mobile-to-fixed messages transmission functions were combined into one category, ATS to aircraft, for safety hazards analysis. Mobile-to-mobile transmissions hazards are shown in the aircraft-to-aircraft messages hazards category.

Based on this functional categorization of 15 hazard categories applied to each of the two functional categories, 30 L-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 Assessment

Once again, it is useful to borrow from the NAS SEM (Ref. 6) 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 L-band communication system safety hazards (summarized in Table 2 and detailed in Appendix C) the following process was followed (Ref. 10):

The 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.

Table 3 summarizes the criteria used to classify severity of each hazard. Worksheets in Appendix C present the severity of the worst credible effect (WCE) for each of the hazards identified during the analysis.

The system state leading to the WCE is the same for all hazards due to the L-band communication system:

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

Causes of identified hazards include

- Hardware failure
- Software failure
- Insufficient capacity
- 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. 2). It, in turn, is based on the FAA's SMS manual severity and likelihood definitions and EUROCONTROL's Safety Regulatory Requirement (ESARR 4) Set 1 Severity Indicators.

TABLE 3.—DESCRIPTION OF HAZARD SEVERITY (REF. 2)

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. Require actions are within operation's capabilities. Includes:	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 a low/moderate severity operational error, or significant reduction in ATC capability	Reduction in separation as defined by a high-severity operational error, or a total loss of ATC	Collisions with other aircraft, obstacles, or terrain
Flying public	No effect on flightcrew Has 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 flightcrew workload Significant reduction in safety margin or functional capability. Major illness, injury, or damage Physical distress	Large reduction in safety margin or functional capability Serious or fatal injury to small number Physical distress 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. 10) as well as in the COCR Version 2.0 (Ref. 2), this safety analysis was limited to hazards caused by L-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 $\geq 1 \times 10^{-3}$
B	Probable	Expected to occur several times in the life of an item	Probability of occurrence per operation/operational hour $< 1 \times 10^{-3}$, but $\geq 1 \times 10^{-5}$
C	Remote	Expected to occur sometime in the lifecycle of an item	Probability of occurrence per operation/operational hour $< 1 \times 10^{-5}$ but $\geq 1 \times 10^{-7}$
D	Extremely remote	Unlikely but possible to occur in an item's lifecycle	Probability of occurrence per operation/operational hour $< 1 \times 10^{-7}$ but $\geq 1 \times 10^{-9}$
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 $< 1 \times 10^{-9}$

^aAdopted from Ref. 1. Only part of the table found relevant to this analysis is presented.

^bQualitative definition for individual item/system as defined in Ref. 1 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.

^cThese qualitative definitions differ from the definitions used in the existing NAS System Safety Risk Analysis.

^dAssumes 24 hr/day each day of the year or approximately 8000 hr/yr for a single item or 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. 10) for the existing system as well as the COCR Version 2.0 (Ref. 2) as applied to individual services (described later in this document). They, in turn, are based on the recommendations provided in Safety Risk Management Guidance for System Acquisitions document (Ref. 1).¹⁵

3.5.2 L-band System Safety Risks Matrix

Finally, risk was determined for each L-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 L-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 L-band system safety hazards. A summary of the safety assessment for the subset of services applicable to the L-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 Data Comm Program. During the second phase, data communications is expected to become the primary means of air-ground communication supporting increased automation in the aircraft and on the ground.

The L-band system is proposed to be introduced during the second phase of the FRS implementation. As such, only the Phase II COCR data is adopted for Table 5.

The L-band system should support air to ground as well as air-to-air communications. Implementation of air-to-air communications would be considered to follow an air-to ground communications implementation.

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

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

Safety hazards	Safety risk likelihood and severity ^a			
	Air traffic services (ATS) to aircraft		Aircraft to aircraft	
	Exist. NAS	L-band FCS	Exist. NAS ^b	L-band FCS
1. Communication capability totally unavailable: ATS failure ^c	3D	3D	4E	2D
2. Communication capability partially unavailable: ATS failure	3D	3C ^d	4E	2D
3. System communication capability unavailable: sender to recipient of ATS unavailable	4D	4C	4D	2D
4. Communication fails (e.g., aborts) with a given recipient for a single message	4C	4B ^e	5	2D ^f
5. Communication fails (e.g., aborts) with multiple recipients for a single message per aircraft	4C	3C ^g	N/A ^h	2D
6. The recipient accepts a message affecting separation from an ATS system that is not its control authority.	2D	2D	N/A ^h	N/A
7. The recipient accepts a message NOT affecting separation from an ATS system that is its control authority.	5	5D	N/A ^h	N/A ⁱ

¹⁵It 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, and “E” is for Nearly Certain; 1 stands for low risk hazards, and while 5 is for High). This discrepancy does not affect the methodology or the essence of risk analysis.

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

Safety hazards	Safety risk likelihood and severity ^a			
	Air traffic services (ATS) to aircraft		Aircraft to aircraft	
	Exist. NAS	L-band FCS	Exist. NAS ^b	L-band FCS
8. A message affecting separation gets to unintended recipient.	2D	2D	NC ^c	2D
9. A message NOT affecting separation gets to unintended recipient.	5	5D	5	N/A ^f
10. Message affecting separation received too late (or expired).	2D	2D	N/A ^h	2D
11. Message NOT affecting separation received too late (or expired).	5	5D	N/A ^h	N/A ^f
12. A message affecting separation corrupted.	2D	3D ^d	2E	2D
13. A message NOT affecting separation corrupted.	5	5D	5	N/A ^f
14. A message affecting separation sent/received out of sequence.	4D	3D ^j	N/A ^h	2D
15. A message NOT affecting separation sent/received out of sequence.	5	5D	N/A ^h	N/A ^f

^aRisk likelihood and severity vary depending on stage of flight (i.e., an aircraft on final approach/terminal airspace would typically have a reduced separation vs. en route potentially increasing the risk and severity in terminal airspace). Severity assessment presented in this document is based on a worst case scenario.

^bIn existing NAS system analysis aircraft-to-aircraft hazards are considered second-level failures and apply only when ATS-aircraft communications has failed.

^cWhere hazard was split in two cases, the most significant risk is shown.

^dThe 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.

^eClassified as probable (B) and minor severity (4) because of the capability of retransmissions.

^fAt this time, only separation-related service has been defined as air-to-air communications on L-band.

^gConsidered less likely but potentially more severe than failure of communication with a given recipient.

^hNo NAS messages have been identified.

ⁱNo credible scenario having safety effect was envisioned.

^jAssumed 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 retransmission comes within latency requirements. If retransmission is too late, then Hazard 10 would apply.

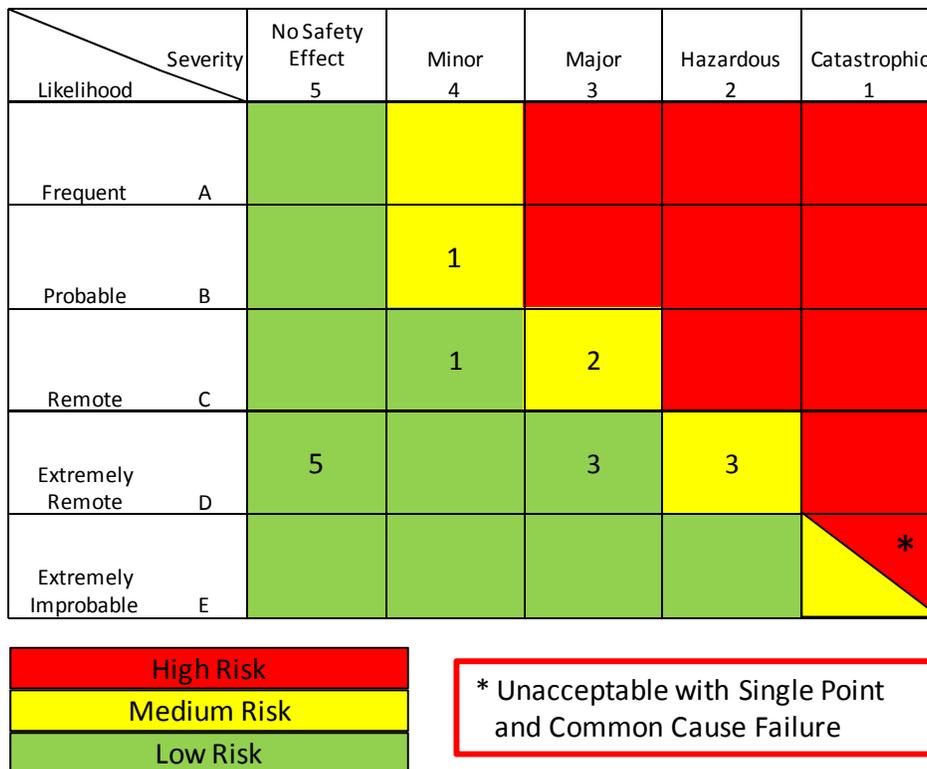


Figure 9.—L-band system safety risk matrix air-traffic-services-to-aircraft communication.

Severity Likelihood		No Safety Effect	Minor	Major	Hazardous	Catastrophic
		5	4	3	2	1
Frequent	A	Green	Yellow	Red	Red	Red
Probable	B	Green	Yellow	Red	Red	Red
Remote	C	Green	Green	Yellow	Red	Red
Extremely Remote	D	Green	Green	Green	9 Yellow	Red
Extremely Improbable	E	Green	Green	Green	Green	* Yellow/Red

High Risk
Medium Risk
Low Risk

* Unacceptable with Single Point and Common Cause Failure

Figure 10.—L-band system safety risk matrix aircraft-to-aircraft communication.

High risk – Unacceptable risk, proposal cannot be implemented unless hazards are further mitigated so that risk is reduced to medium or low level and AOV approves the mitigating controls.

Medium risk – Acceptable risk - minimum acceptable safety objective; proposal may be implemented, but tracking and management are required.

Low risk – Target - acceptable without restriction or limitation; hazards are not required to be actively managed but are documented.

Figure 11.—Risk acceptance criteria (Ref. 1).

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

3.5.3 Unmanned Aircraft System (UAS)-Related Services Safety Risks

Services related to (UAS) operations are also considered candidates for the L-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. 12). Studies considering the implications of operating a UAS 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. 2),

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.

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 ITU¹⁹ and illustrated in Figure 12, 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.

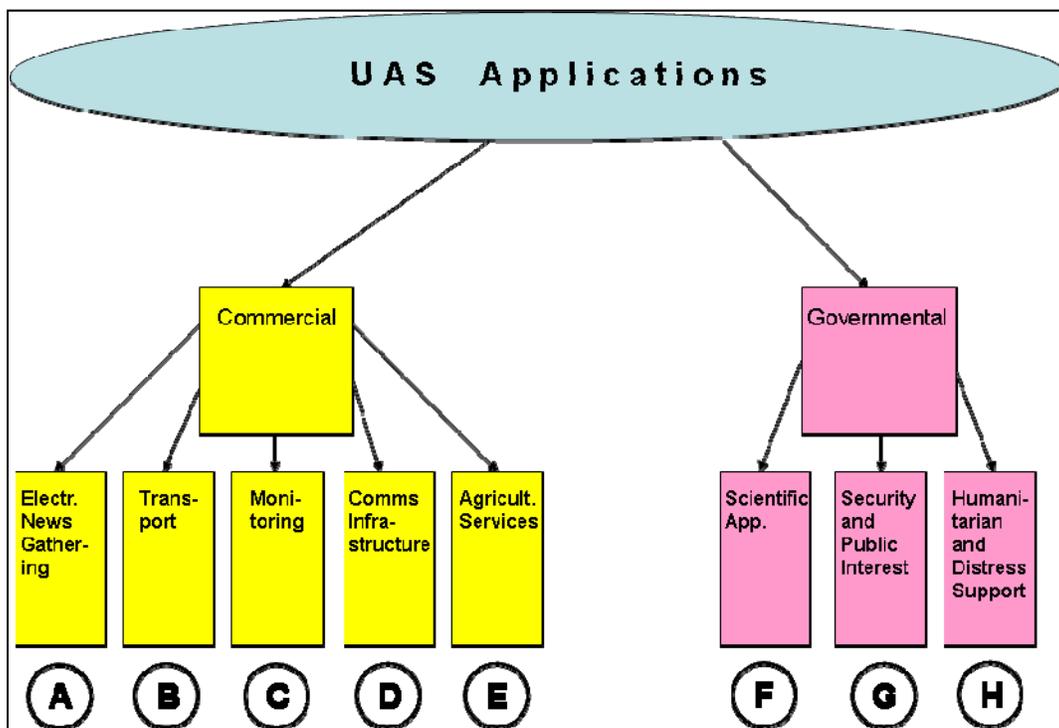


Figure 12.—Unmanned aircraft system (UAS) applications (from proposed changes to Ref. 13).

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

¹⁹ Proposed changes to Ref. 13.

TABLE 6.—UNMANNED AIRCRAFT SYSTEM OPERATIONAL SCENARIOS^{a,b}

	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, 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

^aProposed changes to Ref. 13.

^bAdditional scenarios and detail can be found in Ref. 12.

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, and NAS restrictions), might be implemented via ground-to-ground, air-to-ground, and air-to-air communications infrastructure components. Each of these components would enable efficient data exchange between authorized users in the respective domain. An L-DACS could provide means for the air-to-air and air-to-ground data transfer.

An implementation of the proposed L-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 airborne SWIM capabilities, an L-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 13 shows how airborne SWIM (with the communication links potentially provided over the L-band) fits in the overall FAA air-to-ground communications plan and illustrates interactions of SWIM elements with the other NextGen programs, such as ADS-B and Data Comm.

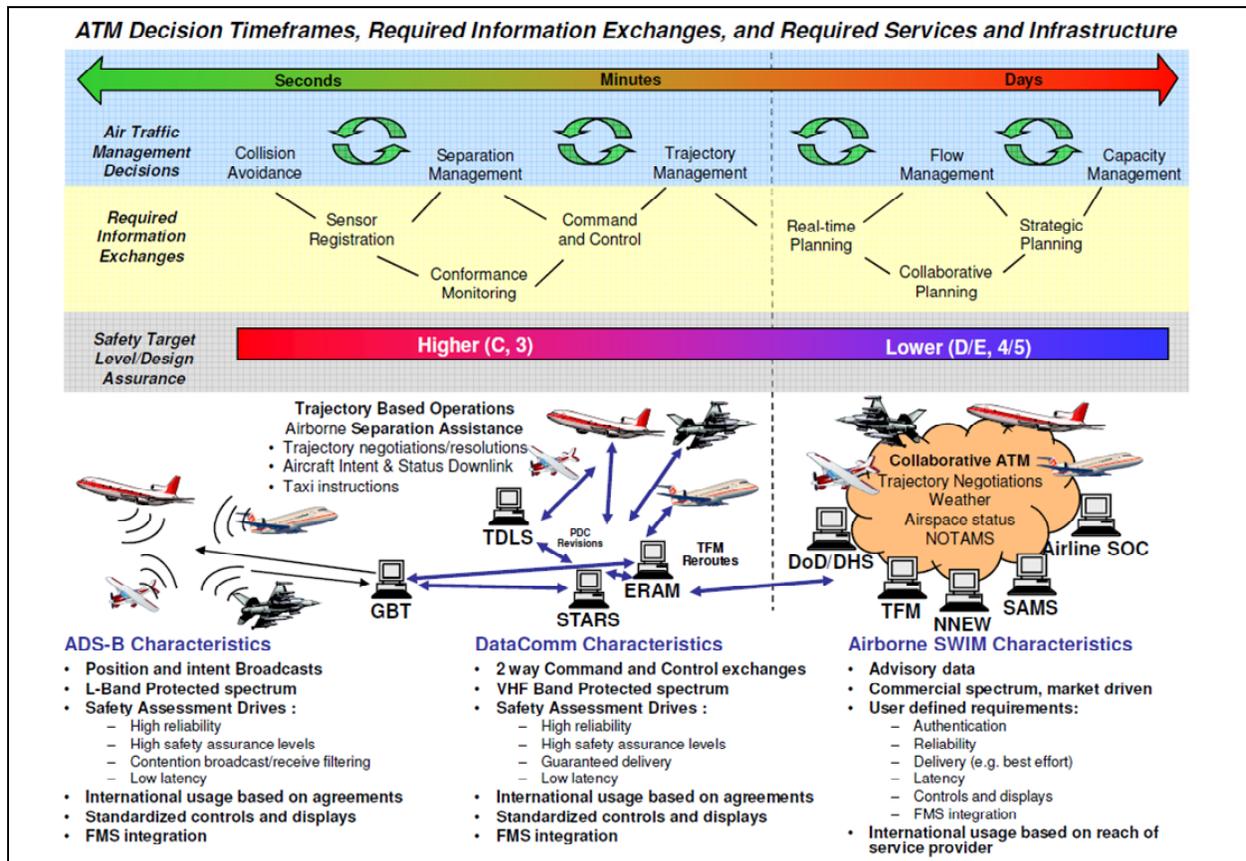


Figure 13.—Airborne SWIM and other NextGen programs (Ref. 14). Acronyms are defined in Appendix A.

As shown in Figure 13, L-DACS 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 13 shows a required level of C3 (medium risk) for Data Comm and D/E 4/5 9 (low risk) for SWIM.

3.6 L-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 14 illustrates the risk management strategies that were considered (Ref. 7).

Feasible risk strategy options identified by the risk management activity:			
<u>Risk avoidance:</u> select a different approach or do not participate in the operation, procedure, or system development	<u>Risk transfer:</u> shift the ownership of the risk to another party	<u>Risk assumption:</u> accept the likelihood, probability, and consequences associated with the risk	<u>Risk control:</u> develop options and alternatives and/or take actions to minimize or eliminate the risk

Figure 14.—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. Although operational controls could be applied to mitigate technical risks, for example, a decision not to have a particular service provided over the L-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 L-band safety risks.

Also, 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 would likely to apply to high-hazard risks only. Because none of the hazards were found to be high risk, the risk transfer strategy is not recommended for mitigation of the L-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. 7), 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 10, 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 L-band system implementation. Many of the controls can also be viewed as requirements (generally identified by “the system shall...”) and as such are included among functional or performance requirements in the L-band System Engineering, CONUSE, System Performance Requirements, and Architecture document (Ref. 4).

Table 18 is annotated with the existing controls that would not be relevant to the proposed system.

Additional controls specific to L–DACS might be added as part of system design and implementation. For example, the current trend points toward meeting QoS and 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 a Data Comm program, a backup system may be added at a later stage if and when critical services requiring higher reliability are added.

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 L-band communications system.

As noted earlier, this document presents a preliminary safety risk assessment. Safety hazards, their consequences, and probability of occurrence need to be reevaluated as the L-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.

Modification or deletion of any of the existing controls.—Existing NAS controls were assumed to be in place at the time of L-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, safety risks identification was limited to high-level, technology-independent risks. Additional risks may be identified as technology selection progresses. The risks may involve but not limited to interference to and from incumbent systems, capacity limitations, COTS use, and so on.

Schedule milestones.—Various risks exist in respect to the L-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 building an L-band communications system prototype, completion of interference testing, preparation of design documents, and final technology selection.

Additionally, the maturity and implementation schedule of other components of the FCS will affect L-band system development. For example, it is assumed throughout this document, as well as all the other Task 7 studies, that the FAA Data Comm system will be in place by the time an L-band system is introduced. As a more definitive timeline and technology details become available, potential interfaces between the proposed L-band system and C-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.

4.0 Information Security Engineering and Security Risk Management

4.1 Information Security Engineering Objective and Scope

Information security engineering (ISE) involves evaluation of the system vulnerability to unauthorized access and use or susceptibility to sabotage. It also involves assessment of the ability of the system to survive a security threat in the expected operational environment (Ref. 6).

As noted in the COCR Version 2.0 (Ref. 2), the goals of information security include

- Safety (mitigating attacks that contribute to safety hazards)
- Flight security (mitigating attacks that contribute to delays, diversions, or cancellations of flight)
- Protection of business interests (mitigating attacks that result in financial loss, reputation damage, or disclosure of sensitive information)

The proposed L-band system will be designed in accordance with the FAA security policy³¹ that states that

The FAA shall ensure that security is provided commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information for all agency information collected, processed, transmitted, stored, or disseminated in FAA information systems and in information systems used on behalf of the FAA. The FAA shall also ensure that systems and applications used by or for the FAA provide appropriate confidentiality, integrity, authenticity, and availability.

For the purposes of this analysis, confidentiality, integrity, and availability are defined as follows:

Confidentiality.—Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Integrity.—Assurance that an information system is operating without unauthorized modification, alteration, impairment, or destruction of any of its components.

Availability.—Assurance that information and communications services will be ready for use when expected.

It should be noted that in the context of a security threat assessment, integrity and availability provide assurance in the face of deliberate attacks as opposed to accidental errors typically addressed during safety risk analysis.

4.2 Information Security Engineering and Security Risk Management Process

Safety and security risk analyses are interrelated and should be addressed as such. For example, denying service to an aircraft that is unable to authenticate its identity and thus does not meet the security requirements may reduce safety.

As noted in both the COCR Version 2.0 (Ref. 2) in respect to the security analysis for a FRS as well as the security threat analysis of the existing NAS communications system (Ref. 10), information security is evolutionary, because the capabilities and motivations of attackers change over time. The evolutionary nature of information system security means that it is important to follow a defined process during security threat analyses of systems so that the motivation for requirements is well understood, and the analyses can be revisited and revised as attacks change.

Figure 15 shows a correlation between the risk management and closed-loop security risk management processes.

³¹ From Ref. 15, please note, this version of the document has been superseded.

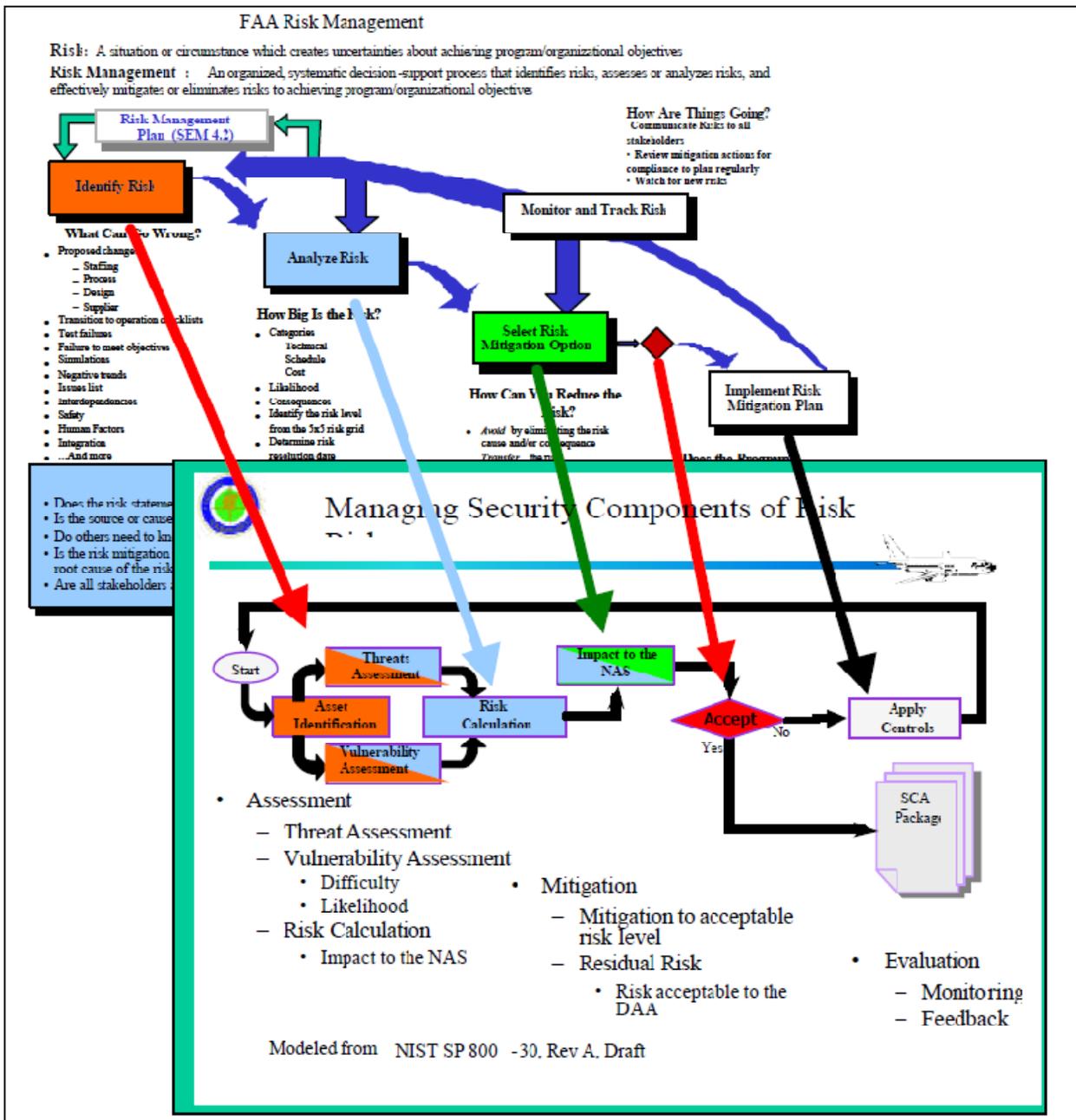


Figure 15.—Correlation of information security methodology with Federal Aviation Administration (FAA) risk management model (Ref. 6). Acronyms are defined in Appendix A.

Following the guidance provided in the NAS SEM, this document attempts to apply similar processes and methodologies to both safety and security analyses.

Figure 16 illustrates the correlation between the security threat analysis and safety hazards analysis methodologies (Ref. 10).



Figure 16.—Correlation between security threat analysis and safety hazard analysis.

The security threat analysis process adheres to the overall risk management model and is tailored to closely follow the safety threat analysis. The methodology is adopted from the NAS Communications System Safety Hazard Analysis and Security Threat Analysis document (Ref. 10).

The same functional analysis is used as a common starting point for both disciplines. Understanding functional requirements and physical architecture aids in identifying the information types handled by the proposed system.

Security categorization provides an initial assessment of the intrinsic sensitivity of the information being handled by the communications system in terms of confidentiality, integrity, and availability.

Next, risks are identified determining system vulnerabilities and threats. The high-level threats to the system are examined, focusing on areas that are the likely concerns based on the security categorization, and then the severity and likelihood of the threats are assessed.

Finally, the security requirements and recommendations are developed to address the threats. The proposed security requirements are coordinated with safety requirements to ensure they do not result in new safety hazards and vice versa.

Both security categorization and risk analysis use impact and severity rankings: none, low, medium, high-severe, and high-catastrophic. These categories roughly correspond to the standard safety hazard classes no safety effect, minor, major, hazardous, and catastrophic, respectively, although as noted above, security considers financial impact and impact on public perception in addition to safety-related impact. The detailed definitions for the categories are provided in Table 7.

TABLE 7.—SECURITY SEVERITY CATEGORIES (REF. 10)

Severity category/hazard class	Safety	Availability	Cost	Passenger privacy	Exposure of proprietary information	Public perception
None/5	General: no or negligible safety impact. Air traffic control (ATC): slight increase in ATC workload. Flying public: inconvenience	No impact	No financial loss	No impact	No impact	No impact
Low/4	General: limited safety impact; includes self-repairing and limited damage or disruption to system functions. ATC: degradation in mission capability to an extent and duration that the communication system is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; or significant increase in ATC workload. Flying public: slight increase in flight crew workload, or slight reduction in safety margin or functional capabilities, or minor illness or damage, or some physical discomfort.	Recoverable loss of redundancy or backup capability	Minor financial loss, or minor damage to assets	Exposure of limited private information of small number of people	Disclosure of nonsensitive airline operation information	Distrust of some passengers in aircraft

TABLE 7.—SECURITY SEVERITY CATEGORIES (REF. 10)

Severity category/hazard class	Safety	Availability	Cost	Passenger privacy	Exposure of proprietary information	Public perception
Medium/3	<p>General: serious safety impact. Example: system failure, damage or disruption that impairs the safe control of air traffic over time and/or requires local restoration of systems capabilities.</p> <p>ATC: significant degradation in mission capability to an extent and duration that the communication system is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; or reduction in separation as defined by a low/moderate severity operational error, or significant reduction in ATC capability; or significant damage to communication system assets.</p> <p>Flying public: significant increase in flight crew workload, or significant reduction in safety margin or functional capability, major illness, injury, damage, or physical distress.</p>	Significant flight delays	Significant financial loss or Significant damage to assets	Exposure of private information of small number of people	Disclosure of some sensitive airline operation information	Strong distrust of some passengers in aircraft
High-severe/2	<p>General: severe safety impact. Example: system failure, damage or disruption that immediately affects the safe control of aircraft or destroys system assets beyond recovery capabilities.</p> <p>ATC: severe degradation in, or loss of, mission capability to an extent and duration that the Communication System is not able to perform one or more of its primary functions; or reduction in separation as defined by a high severity operational error, or a total loss of ATC.</p> <p>Flying public: large reduction in safety margin or functional capability, serious or fatal injury to small number, or physical distress/excessive workload.</p>	Flight interruptions	Major financial loss or severe damage to assets	Exposure of private information of large number of people	Disclosure of lots of sensitive airline operation information, some security information	Strong distrust of many passengers in aircraft

TABLE 7.—SECURITY SEVERITY CATEGORIES (REF. 10)

Severity category/hazard class	Safety	Availability	Cost	Passenger privacy	Exposure of proprietary information	Public perception
High-catastrophic/1	General: catastrophic safety impact, or total loss of systems control. ATC: collision with other aircraft, obstacles, or terrain. Flying public: hull loss, multiple fatalities.	Fleet re-route	Huge financial cost, or destruction of aircraft	Exposure of private information of large number of people	Disclosure of highly sensitive airline operation information, security information	Complete distrust of many passengers in air traffic

The definitions of categories in Table 7 were developed during the security threat analysis for the current NAS systems and were designed to maximize the commonality with established safety terminology. The definitions were derived from a number of sources: the FAA’s Information Systems Security Program Handbook (Ref. 15), the FAA’s SSMP handbook (Ref. 8), NIST Federal Information Processing Standards (FIPS) 199 (Ref. 16), NIST Special Publication (SP) 800–30 (Ref. 17), and the European Union’s Security of Aircraft in the Future European Environment (SAFE) project (Ref. 18).

Note: For the categories shown in Table 7, the “None” and “Low” map to FIPS 199 “Low;” the “Medium” category maps to FIPS 199 “Medium;” and the “High—Severe” and “High—Catastrophic” map to FIPS 199 High.

To align the security and safety analyses, the likelihood ratings used in the safety analysis were applied here. These rankings are given in Table 4. However, only qualitative definitions of the safety likelihood rankings are used for the security analysis, because the presence of an attacker makes threat likelihood estimation considerably more difficult to quantify.

The security risk assessment matrix similar to the one resulted from the safety analysis was created based on threat severity and threat likelihood to determine if a particular threat represents an unacceptable risk.

In the matrix, a green cell indicates a likelihood-severity combination that represents an acceptable risk; a red cell indicates a likelihood-severity pair that shows an unacceptable risk requiring further mitigation; and a yellow cell indicates a likelihood-severity that represents a moderate risk, potentially requiring additional analysis to determine if mitigation is recommended.

Once the risks are identified and analyzed, the process applies effective and suitable technical, procedural, physical, and administrative controls to mitigate these risks to an acceptable level. ISE methodology combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of information technology assets (including information).

4.3 Inputs to Information Security Engineering and Security Risk Management

Figure 17 presents FAA security policy and guidance applied to the L-band system security risk management process. Some of the publications listed were quoted in the document; some were used indirectly as contributors to the studies and reports referenced throughout this document.

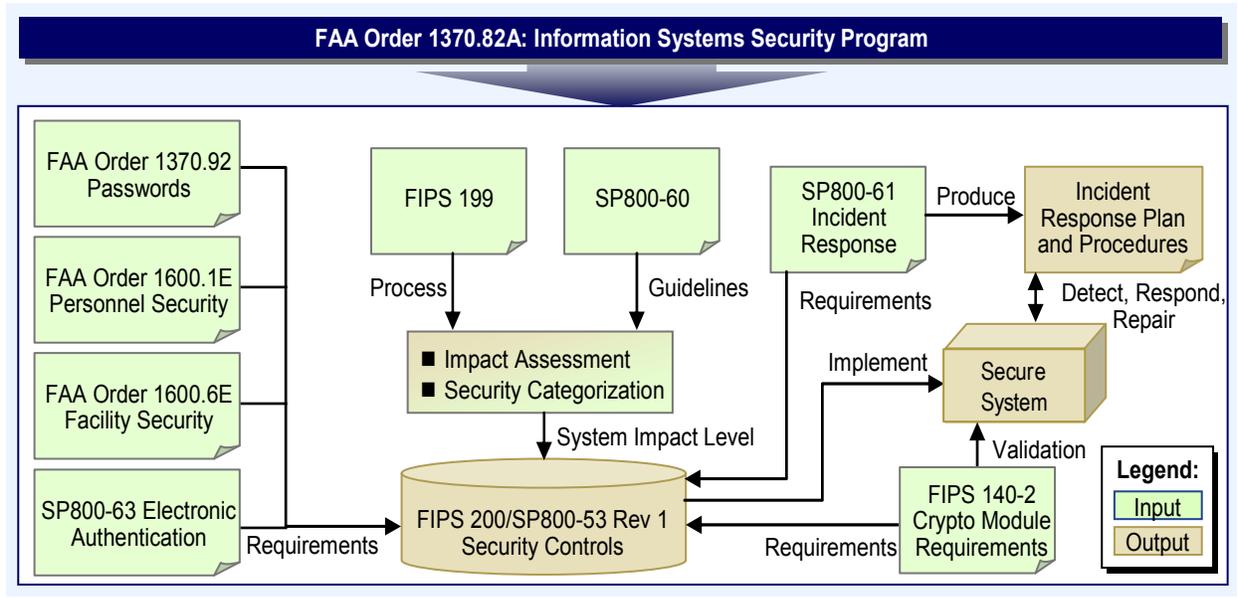


Figure 17.—Federal Aviation Administration (FAA) security policy and guidance (slightly modified figure from Ref. 19).

4.4 Security Threat Identification

Risks to the proposed L-band system may arise from events such as, but not limited to, the following (Ref. 6):

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or manmade disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT system

The main threats to the proposed system are listed in Table 8. Existing NAS communications system security threats (Ref. 10) and threats identified in the COCR Version 2.0 (Ref. 2) were reviewed. As a result of the analysis and based on the discussions with the FAA and NASA, a methodology followed by the COCR was adopted (Ref. 20).

The focus during threat identification is on communications threats, because these are the threats that are likely to be mitigated by the communications system itself and are likely to motivate FRS security requirements that will require standardization. As a result, threats like insider threats—which are important but which are unlikely to be mitigated by the communications system itself—and threats to the monitoring, maintenance, and control (MMC) of the FCI are not included in Table 8.

TABLE 8.—L-BAND COMMUNICATION SYSTEM HIGH-LEVEL THREATS

Threat Identifier	Threat description
T.DENIAL	System resources may become exhausted due to system error, nonmalicious user actions, or denial-of-service (DoS) attack.
T.DENIAL.FLOOD	An attacker floods a communications segment of the L-band system with injected messages in order to reduce the availability of the L-band system.
T.DENIAL.INJECT	An attacker injects malformed messages into a communications segment of the L-band system in order to reduce the availability of the L-band system.
T.DENIAL.INTERFERE	An attacker injects deliberate radiofrequency (RF) interference into an RF communication segment of the future communications infrastructure (FCI) in order to reduce the availability

TABLE 8.—L-BAND COMMUNICATION SYSTEM HIGH-LEVEL THREATS

Threat Identifier	Threat description
	of the L-band system.
T.ENTRY	An individual other than an authorized user may gain access via technical or non-technical attack for malicious purposes.
T.ENTRY.ALTER	An attacker delays, deletes, injects, modifies, redirects, reorders, replays, or otherwise alters messages on a communications segment of the L-band system in order to reduce the integrity of the L-band system.
T.ENTRY.EAVESDROP	An attacker eavesdrops on messages on a communications segment of the L-band system in order to reduce the confidentiality of the L-band system.
T.ENTRY.IMPERSONATE	An attacker impersonates a user of the L-band system in order to reduce the confidentiality or integrity of the L-band system, or simply to gain free use of the L-band system.

It is recommended for a future security analysis conducted at a later stage in system development process and completed outside the scope of this subtask to include, but not be limited to, the following additional threats:

- T.ACCESS (An authorized user may gain unauthorized access via technical or nontechnical attack for malicious or nonmalicious purposes.)
- T.DEVELOP (Security failures may occur as the result of problems introduced during design, development, and implementation of the system.)
- T.FAILURE (The secure state of the system could be compromised in the event of a system failure.)
- T.INSTALL (The system may be delivered or installed in a manner that undermines security.)
- T.MAINTAIN (The security of the system may be reduced or defeated due to errors or omissions in the administration and maintenance of the system.)
- T.OBSERVE (Events occur in system operation that compromise security, but the system, due to flaws in its specification, design, or implementation, may lead a competent user or technician to believe that the system is still secure.)
- T.OPERATE (Security failures may occur because of improper operation of the system.)
- T.PHYSICAL (Security-critical parts of the system may be subjected to a physical attack that may compromise security.)

4.5 Security Risks Analysis and Assessment

The risk assessment matrix was created to analyze individual security risks. “The matrix reflects the level of risk associated with the likelihood of a given threat source exploiting a given vulnerability and the impact of that threat source successfully exploiting the vulnerability” (Ref. 6). To create the matrix, the service-level threat severity analysis and assessment were reviewed. Table 9 contains the information security service-level threat severity assessment for the services identified as potential applications for the L-band communications system. The table is a subset of information presented in COCR Version 2.0. The column headers are defined as follows (Ref. 2):

- Service.—The acronym for the service name.
- Confidentiality.—The relative operational impact of violation of confidentiality.
- Integrity.—The relative operational impact of corruption of the integrity.
- Availability.—The relative operational impact of the loss of use/provision of the service.

The threat severity categories (e.g., high and medium) are defined in Table 7.

TABLE 9.—INFORMATION SECURITY THREAT SEVERITY FOR L-BAND SYSTEM SERVICES^{a,b}

Service	Confidentiality	Integrity	Availability
D-ORIS	None	Medium	Low
D-OTIS	None	High-severe	Medium
D-SIG	None	Medium	Low
D-RVR	None	High-severe	Low
WAKE	None	High-severe	High-severe
FLIPCY	Low	High-severe	Medium
SAP	Low	Medium	Low
PPD	Low	Low	Low
D-SIGMET	None	High-severe	Medium
DYNAV	Low	High-severe	Medium
URCO	None	Medium	Medium
AIRSEP	Low	High-severe	High-severe

^aA portion of Table 4-11 from Ref. 2. This table contains information relevant to L-band system security only.

^bAcronyms are defined in Appendix A.

The COCR notes that the initial assessment of threat likelihood and threat severity assumes that the FCI contains no specific security controls or intrinsic security mitigations. While current L-band technology proposals do not include technologies with the inherent mitigation of deliberate RF interference as do certain spread spectrum radio systems, security features will vary depending on technology chosen.

Table 10 contains likelihood and severity assessments for the each of the threats identified above. Threat likelihood is ranked based on its potential for realization and is determined based on its motivation and required capabilities.

- Motivation.—A ranking of how strong the motivation is to realize the threat. A value in the range 1 to 3 is assigned to motivation, with 3 representing strong motivation and 1 representing weak motivation.
- Required capabilities.—A ranking of how much financial and technical capability is required to realize the threat. A value in the range 1 to 3 is assigned to required capabilities, with 3 representing a low requirement, and 1 representing a high requirement.

Threat likelihood values are determined by multiplying the motivation and required capabilities values (Ref. 2).

A result of 1 corresponds to E, extremely improbable, 2 corresponds to D, extremely remote, 3 corresponds to C, remote, 4 or 6 corresponds to B, probable, and 9 corresponds to A, frequent.⁴⁹

Threat severity is ranked based on the potential impact of the threat if it is realized, using the following categories:

- None: There is no perceivable impact on safety, flight regularity, or business interests.
- Low: There is a limited adverse effect on safety, flight regularity, or business interests.
- Medium: There is a serious adverse effect on safety, flight regularity, or business interests.
- High-severe: There is a severe adverse effect on safety, flight regularity, or business interests.
- High-catastrophic: There is a catastrophic effect on safety, flight regularity, or business interests.

⁴⁹ Note that COCR (Ref. 2) ranking is unlikely, 1 to 3, likely 4 to 6, and highly likely, 7 to 9.

To calculate severity, potential impacts on safety, flight regularity, and business needs are considered, and a value in the range 1 to 5 assigned to each, with 1 being the most serious impact and 5 being the least serious impact. Threat severity is then determined based on the maximum of the three values assigned, with a maximum value of 1 corresponding to high-catastrophic, 2 corresponding to high-severe, etc. (Ref. 2).

TABLE 10.—THREAT LIKELIHOOD AND SEVERITY

Threat identifier	Likelihood			Severity ^c			
	Motivation ^a	Required capabilities ^b	Overall	Safety	Flight regularity	Business needs	Overall ^d
T.DENIAL							
T.DENIAL.FLOOD	3	2	B	2	3	3	High severe
T.DENIAL.INJECT	3	2	B	2	3	3	High severe
T.DENIAL.INTERFERE	3	3	A	2	3	3	High severe
T.ENTRY							
T.ENTRY.ALTER	3	2	B	2 ^d	4	3 ^d	High severe
T.ENTRY.EAVESDROP	3	3	A	5	5	3 ^e	Medium
T.ENTRY.IMPERSONATE	3	2	B	2 ^d	4	3 ^d	High severe

^aMotivation: 1 = weak; 3 = strong

^bRequired capabilities: 1 = high; 3 = low

^cSeverity: 1 = most serious; 5 = least serious

^dThe COCR notes a safety rating of 1 and business needs rating of 3 for this category. A less strict rating was found to be more applicable for the L-band based on the services selected as applications for the L-band. The most severe rating identified in the COCR for L-band service is high-severe.

^eThe COCR notes a business needs rating of 2 for this category. A less strict rating was found more applicable for the L-band based on the services selected as applications for the L-band.

Figure 18⁵¹ shows the security risk assessment matrix created based on the results of the above analysis.

⁵¹ Note that the risk grid shown in the FAA SEM (Ref. 6) is slightly different being equivalent to categorizing 3B, 2C, and 1D and E as medium risk. The presented matrix follows the format and methodology suggested by Ref. 1.

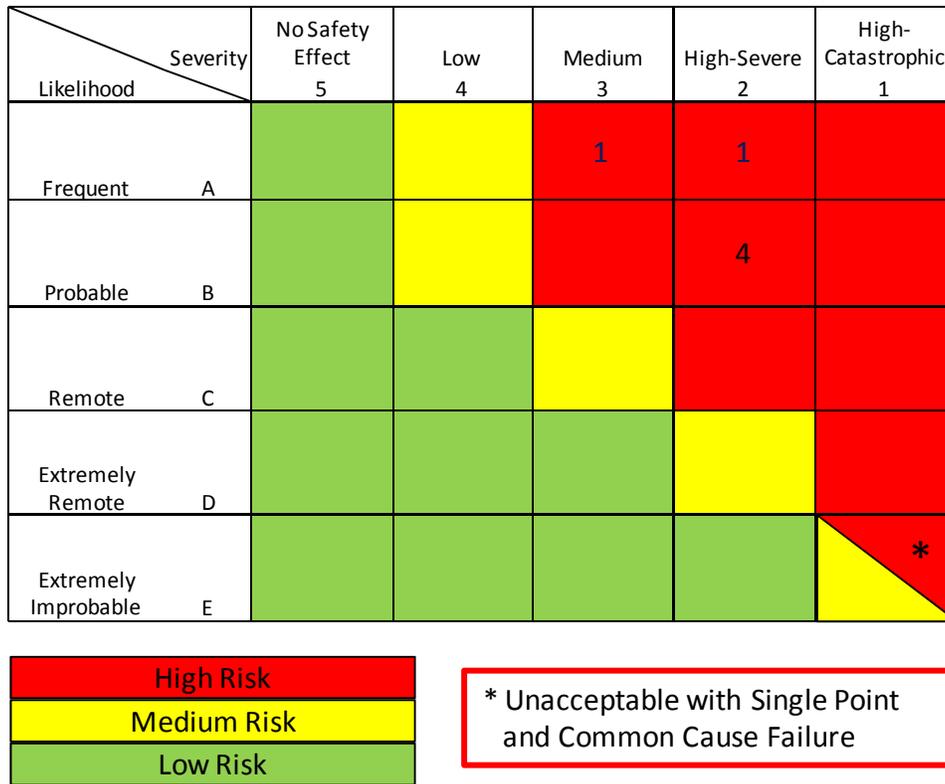


Figure 18.—Security risk assessment matrix.

4.6 Security Risks Treatment

As pointed out in NIST SP800–53 (Ref. 20):

The selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

4.6.1 Summary of the Applicable COCR Version 2.0 Security Analysis

Various controls were discussed in the COCR Version 2.0 in respect to FCS information security. The section of the COCR describing the security controls for FRS was found applicable and as such is presented below (Ref. 2).

There are a wide variety of security controls or countermeasures and it is necessary to consider various architectural issues in order to determine which controls should be used to protect the FCI.

Controls based on cryptography and encryption can be applied at a variety of protocol layers. One important question is which layer or layers of the FCI should include cryptographic protection. The answer to this question will clarify the extent to which controls impinge on the specification of the FRS.

In addition, procedural controls such as voice read-back and waveform controls such as frequency hopping can be used to mitigate certain threats. Redundancy can be built into the provision of any part of the FCI, through duplication of elements such as radios, and alternate network paths. A firewall can be placed at any network interconnection, and apply rules for packet filtering based on parameters such as originator and destination address.

The properties of these controls are summarized in Table 11.

TABLE 11.—PROPERTIES OF SECURITY CONTROLS^a

Procedural controls	Involves	Example	Good for
	Human users	Voice read-back	T.ENTRY.ALTER
End-to-end cryptographic protection	End systems	Aeronautical Telecommunications Network (ATN) Security, S/MIME, SSL/TLS	T.ENTRY.ALTER T.ENTRY.EAVESDROP T.ENTRY.IMPERSONATE
Network level cryptographic protection	Boundary intermediate systems (BIS)	IPSec	T.ENTRY.ALTER T.ENTRY.EAVESDROP T.ENTRY.IMPERSONATE
Link level cryptographic protection	Radio, logical characteristics	Wireless LAN, GSM security measures	T.DENIAL.FLOOD T.DENIAL.INJECT T.ENTRY.ALTER T.ENTRY.EAVESDROP T.ENTRY.IMPERSONATE
Waveform controls	Radio, radiofrequency characteristics	Spread spectrum	T.DENIAL.FLOOD T.DENIAL.INTERFERE
Redundancy	Second radio system (same or different technology)	VHF voice alternate radio site (ground), spare channels	T.DENIAL.FLOOD T.DENIAL.INTERFERE
Firewall	Routers	COTS firewall products	T.DENIAL.FLOOD T.DENIAL.INJECT

^aAcronyms are defined in Appendix A.

The conclusions of the architectural discussion are (from Ref. 2):

- Cryptographic protection appears to be the preferred approach to mitigate T.ENTRY.ALTER, T.ENTRY.EAVESDROP, and T.ENTRY.IMPERSONATE.
- Cryptographic protection at the link layer, network layer, or application layer can be used to mitigate T.ENTRY.ALTER, and T.ENTRY.IMPERSONATE. There are trade-offs involved in deciding which protocol layer to protect. For example, application layer protection may be preferred from a security perspective since it secures the packet end-to-end. But link layer protection may be preferred from a cost perspective since a single secure channel can be used to protect a large number of services.
- Cryptographic protection at the link layer, network layer, or application layer can also be used to mitigate T.ENTRY.EAVESDROP. However since only a small number of services require mitigation of T.ENTRY.EAVESDROP and encryption could affect the safety of ATS, it is expected that end-to end cryptographic protection will be used in this case.
- One control that mitigates T.DENIAL.INJECT is link level cryptographic protection. This would impact the FRS specification. Use of a firewall to selectively filter received data is an alternative, which would not impact the FRS specification.
- A system configuration, which involves radio set and channel redundancy may be a cost effective way to mitigate T.DENIAL.INTERFERE and T.DENIAL.FLOOD, since such redundancy is already expected to be required to address safety issues associated with equipment failure.

4.6.2 Further Analysis Based on NIST SP800–53

The NIST SP800–53 (Ref. 20) document presents a security controls catalog listing management, operational, and technical security controls for low-, moderate-, and high-impact information systems.

According to the classification suggested in Reference 20, and based on the COCR Version 2.0 (Ref. 2) analysis of confidentiality, integrity, and availability for various services summarized in Table 9, the proposed L-band system security category is high-impact.

Security controls documented in the catalog were reviewed; those found applicable to the proposed L-band system are included in the Appendix F.

Common security controls account for the controls that “can be applied to one or more organizational information systems” (Ref. 20). Controls proposed for other data communications systems as well as the controls currently implemented in NAS should be examined as available.

4.6.3 Continued Security Assessment

Many of the security attacks against communications systems exploit threats not considered during system design and implementation. This document presents a preliminary security risk analysis only. The assessment will need to be regularly revisited and revised to ensure that it remains up-to-date with attack innovations and development decisions. As noted in NIST SP800–53 (Ref. 20),

an effective information security program should include periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.

Additionally, the analysis presented here was conducted as a high-level analysis and was not intended to replace a more detailed security risk analysis required at a later stage in system development process.

Appendix A.—Acronyms and Abbreviations

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

AAC	aeronautical administrative communication
ADS	automatic dependent surveillance
ADS-B	automatic dependent surveillance—broadcast
ADS-C	automatic dependent surveillance—contract
ADS-R	automatic dependent surveillance—rebroadcast
AFIS	airport/aerodrome flight information service
AIM	aeronautical information management
AIRSEP	air-to-air self separation
AM(R)S	aeronautical mobile (route) service
ANSP	air navigation service provider
AOA	autonomous operations area
AOC	aeronautical (airline) operational control
AP-17	Action Plan 17
AP-30	Action Plan 30
APT	airport
ARNS	Aeronautical Radio Navigation Services
ARTCC	air route traffic control center
ATC	air traffic control
ATCO	air traffic control officer (controller)
ATCRBS	air traffic control radar beacon system
ATCSCC	air traffic control system command center
ATCT	air traffic control tower(s)
ATN	Aeronautical Telecommunications Network
ATM	air traffic management
ATS	air traffic services
ATSP	air traffic service provider
ATSU	air traffic service unit
AVS	advisory services
CDM	collaborative decision making
CNS	communication, navigation, surveillance
COCR	Communications Operating Concepts and Requirements
CONOPS	concepts of operations
CONUSE	concepts of use
COTS	commercial off-the-shelf
CPFSK	continuous phase frequency shift keying
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
DYNAV	dynamic route availability

E3	electromagnetic environmental effects
EIS	emergency information services
ER	en route
FAA	Federal Aviation Administration
FCI	Future Communications Infrastructure
FCS	Future Communications Study
FDD	frequency division duplex
FIS	flight information services
FLIPCY	flight plan consistency
FRS	Future Radio System
GSM	Global System for Mobile Communications
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers, Inc
IFR	instrument flight rules
IOC	initial operating capability
ISE	information security engineering
ITU	International Telecommunication Union
IWP	integrated work plan
JPDO	Joint Planning and Development Office
JTIDS	Joint Tactical Information Distribution System
L-DACS	L-band Digital Aeronautical Communications System
LDL	L-band digital link
LOS	Line-of-sight
M&C	monitoring and control
MAC	medium access control
MTBF	mean time between failures
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NextGen	Next Generation Air Transportation System
NEXRAD	Next-Generation Weather Radar
NNEW	NextGen Network Enabled Weather
NOCC	National Operations Control Center
NOTAM	Notices to Airmen
OFDM	orthogonal frequency division multiplexing
OI	operational improvement
OPA	operational performance assessment
ORP	oceanic, remote, polar
OSED	operational services and environment description
OSHA	Occupational Safety and Health Administration
PIREP	pilot report
PLA	project-level agreement
PPD	pilot preferences downlink
QoS	quality of service
RAC	risk analysis code
RAM	requirements allocation matrix
RF	radiofrequency
RFI	radiofrequency interference

RNAV	area navigation
RNP	required navigation performance
RNSS	radio navigation satellite system
RTCA	RTCA, Inc. (founded as Radio Technical Commission for Aeronautics)
RVR	runway visual range
SAMS	Special Use Airspace Management System
SAP	system access parameters
SBS	surveillance and broadcast services
SE	system engineering
SEM	System Engineering Manual
SESAR	Single European Sky ATM Research
SHA	Safety Hazard Analysis
SMS	Safety Management System
SRM	safety risk management
SSE	system safety engineering
SSH	System Safety Handbook
SSR	secondary surveillance radar
STARS	Standard Terminal Automation Replacement System
SUA	special use airspace
Surv	surveillance
SWIM	System Wide Information Management
SYSCO	system supported coordination
TACAN	tactical air navigation
TBO	trajectory-based operations
TCAS	Traffic Collision Avoidance System
TFM	traffic flow management
TFR	temporary flight restrictions
TIS-B	traffic information services, broadcast
TMA	terminal maneuvering area
TVS	terminal voice switch
UA	unmanned aircraft
UAS	unmanned aircraft system
URCO	urgent contact
VDL	VHF digital link
VHF	very high frequency
WAKE	wake vortex
WCE	worst credible effect
WRC	World Radio Communications Conference

Appendix B.—Hierarchical Diagrams of Functional Requirements

Appendix B contains the functional analysis of the L-band communication system presented as a series of hierarchical diagrams. Details are discussed in Reference 4. The functional analysis was used to structure both the safety and security analyses. The “L” preceding all of the numerical functional levels is used to represent L-band.

The analysis and diagrams are adopted from the National Airspace System Communications System Safety Hazard Analysis and Security Threat Analysis document (Ref. 10).

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

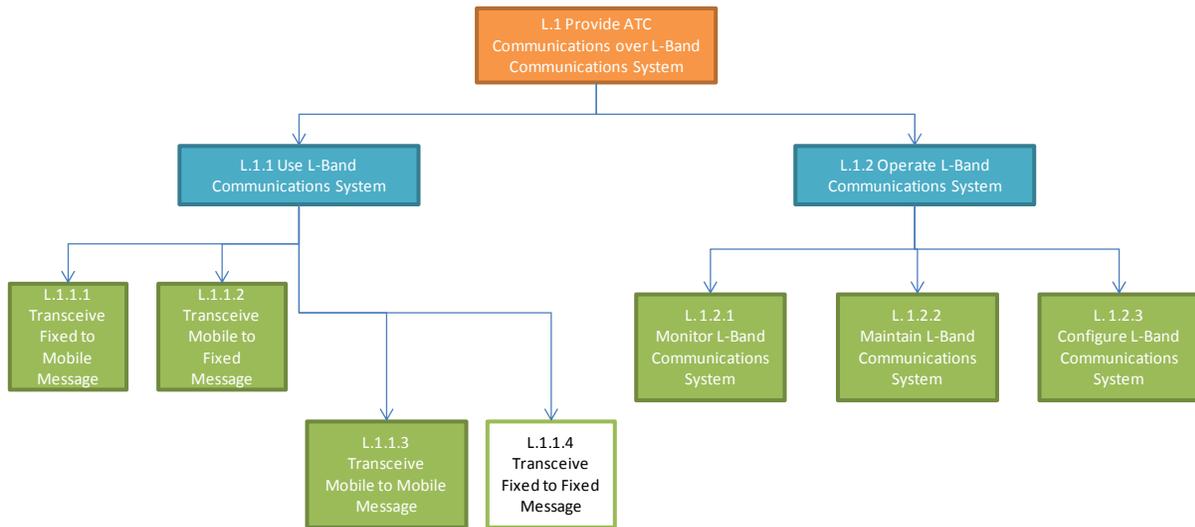


Figure 19.—L-band communications system high level.

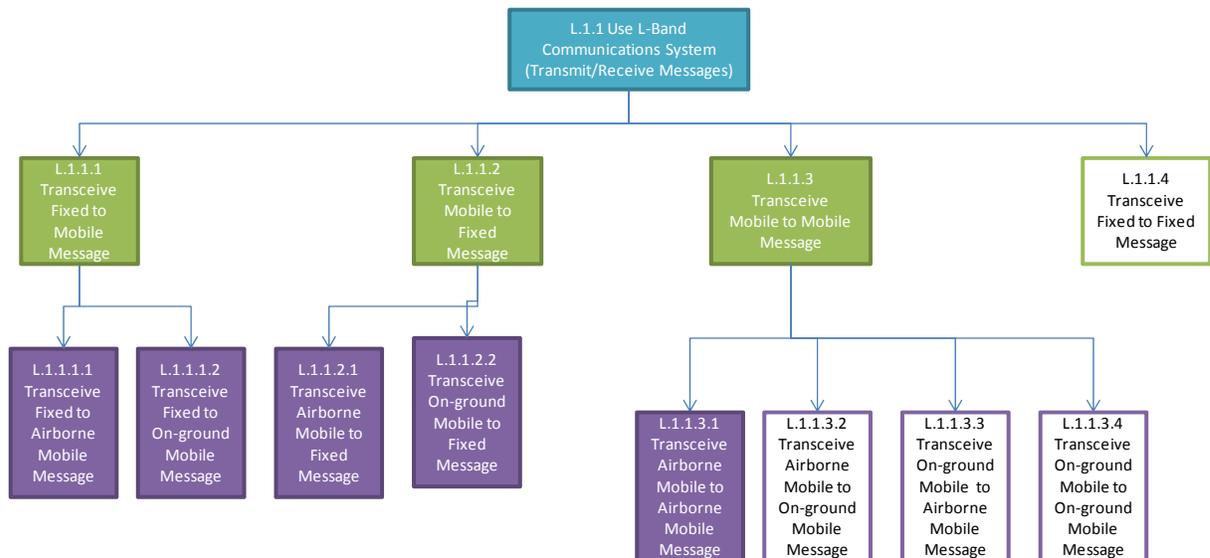


Figure 20.—Decomposition of use L-band communications system (transmit/receive messages).

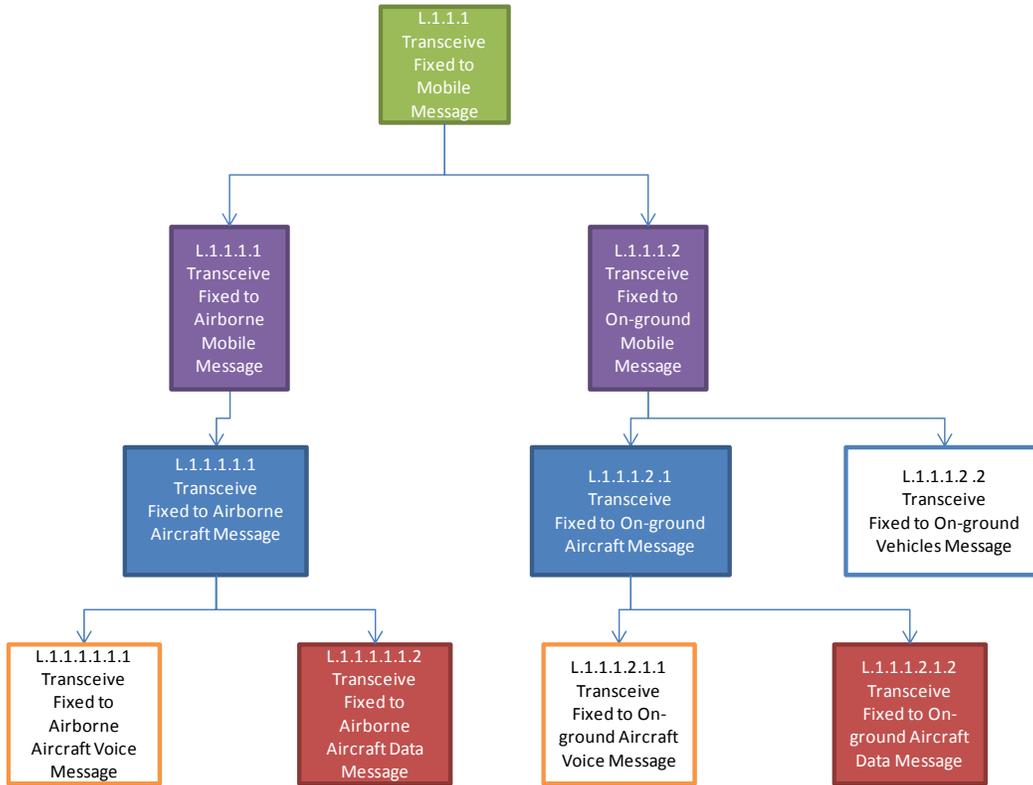


Figure 21.—Decomposition of transceive fixed-to-mobile message.

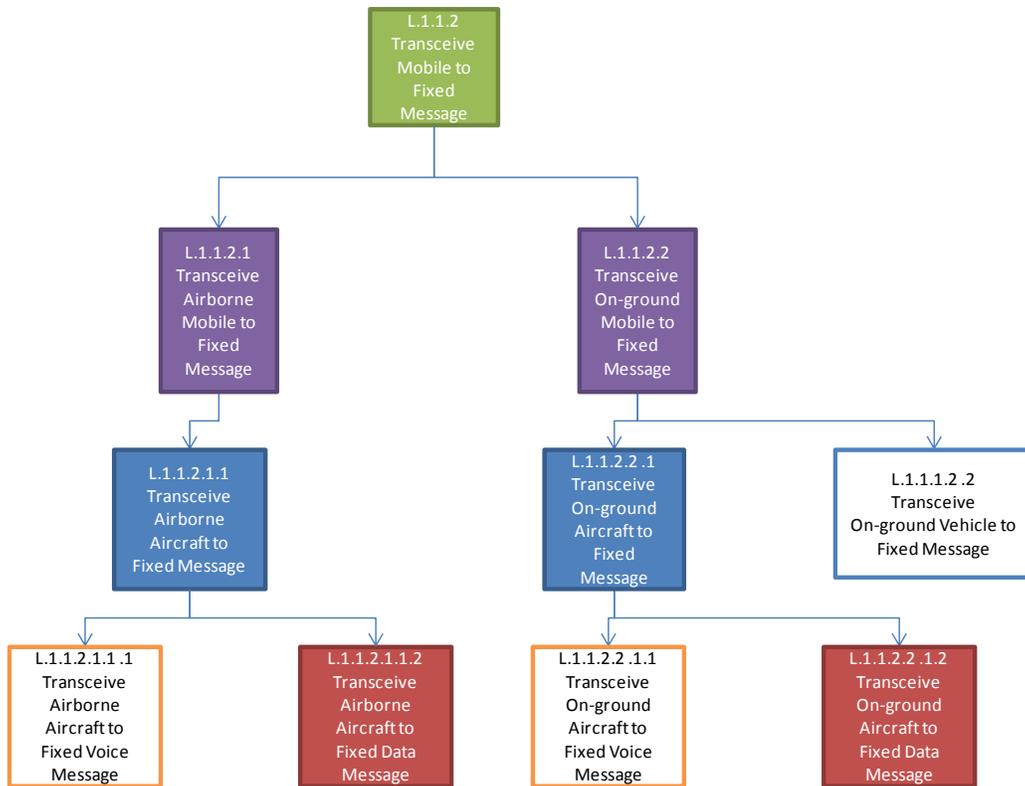


Figure 22.—Decomposition of transceive mobile-to-fixed message.

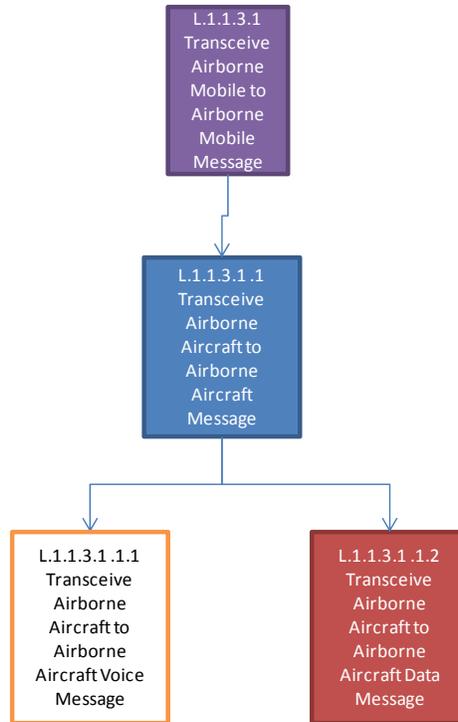


Figure 23.—Decomposition of transceive airborne-mobile-to-airborne-mobile messages.

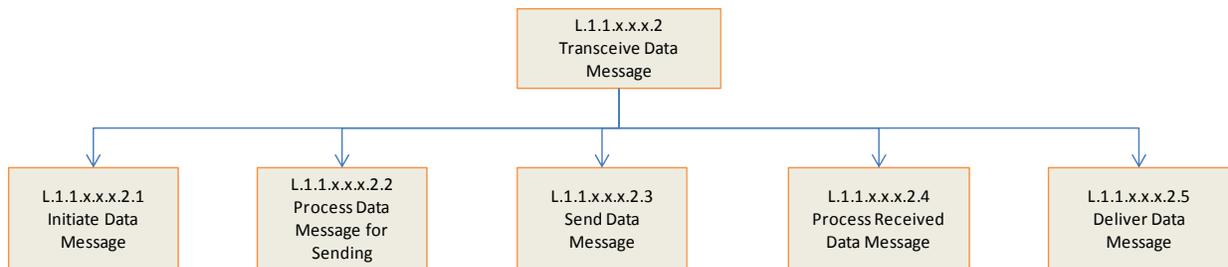


Figure 24.—Generic decomposition of transceive data message.

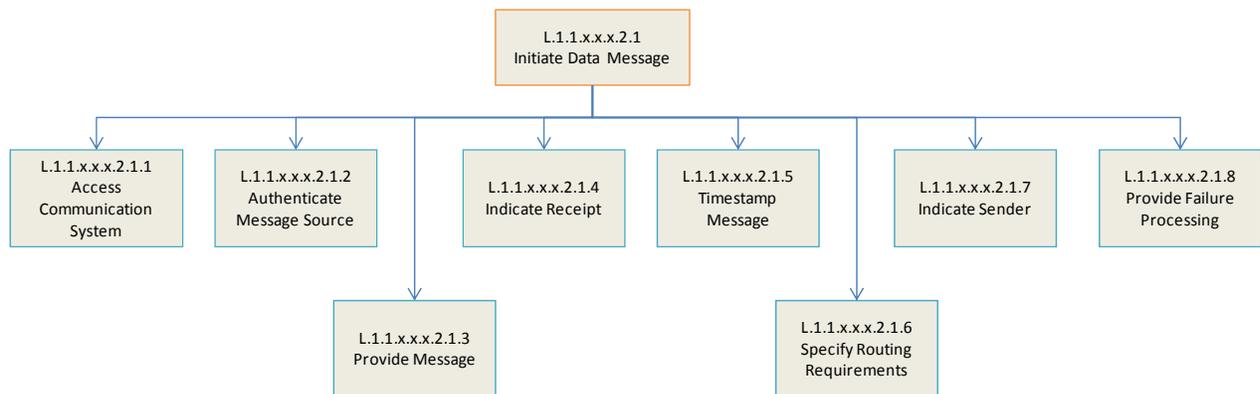


Figure 25.—Generic decomposition of initiate data message.

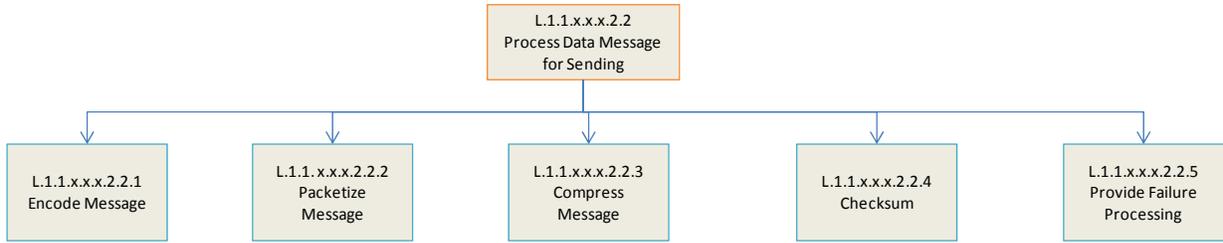


Figure 26.—Generic decomposition of process data message for sending.

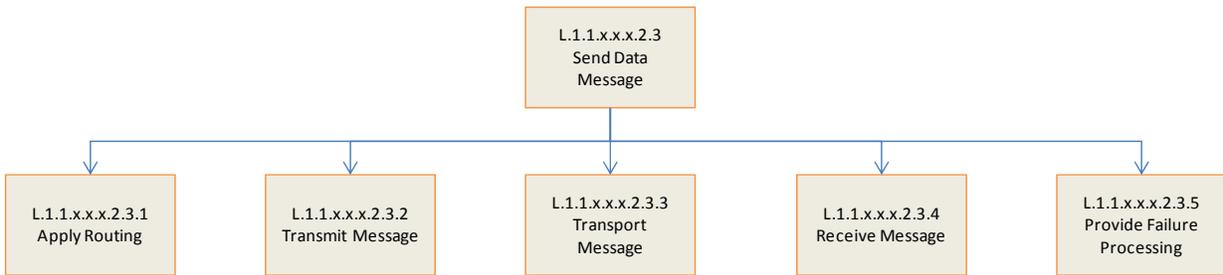


Figure 27.—Generic decomposition of send data message.

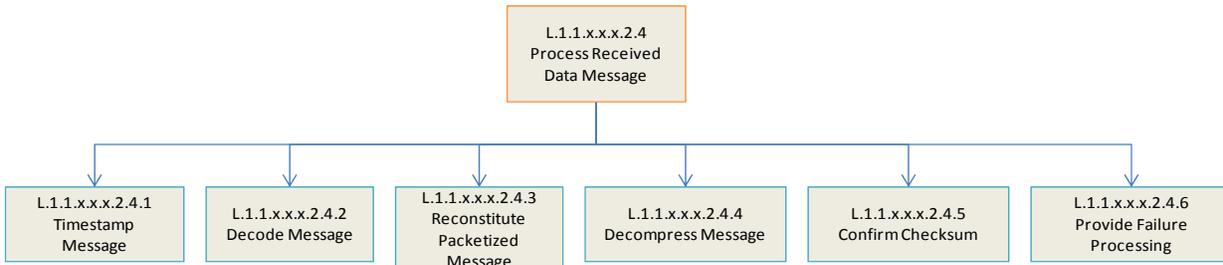


Figure 28.—Generic decomposition of process received data message.

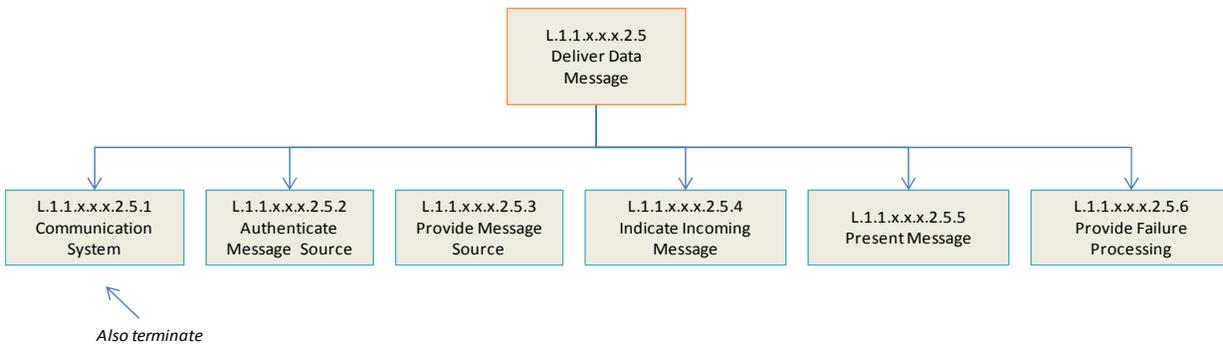


Figure 29.—Generic decomposition of deliver data message.

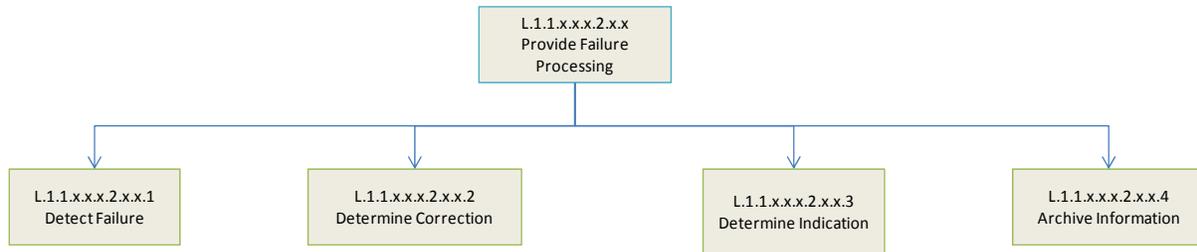


Figure 30.—Generic decomposition of provide failure processing.

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

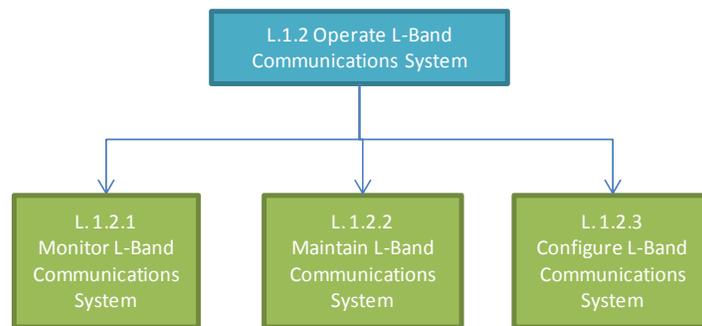


Figure 31.—Decomposition of operate L-band communications system.

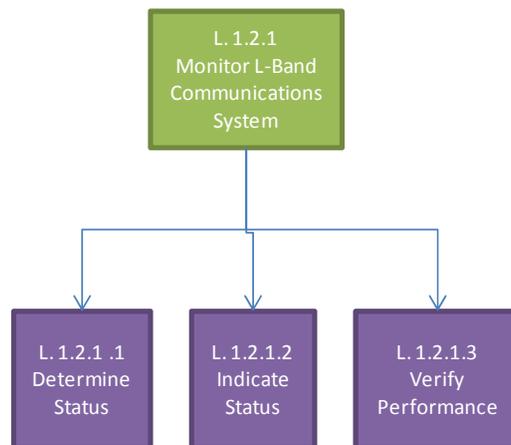


Figure 32.—Decomposition of monitor L-band communications system.

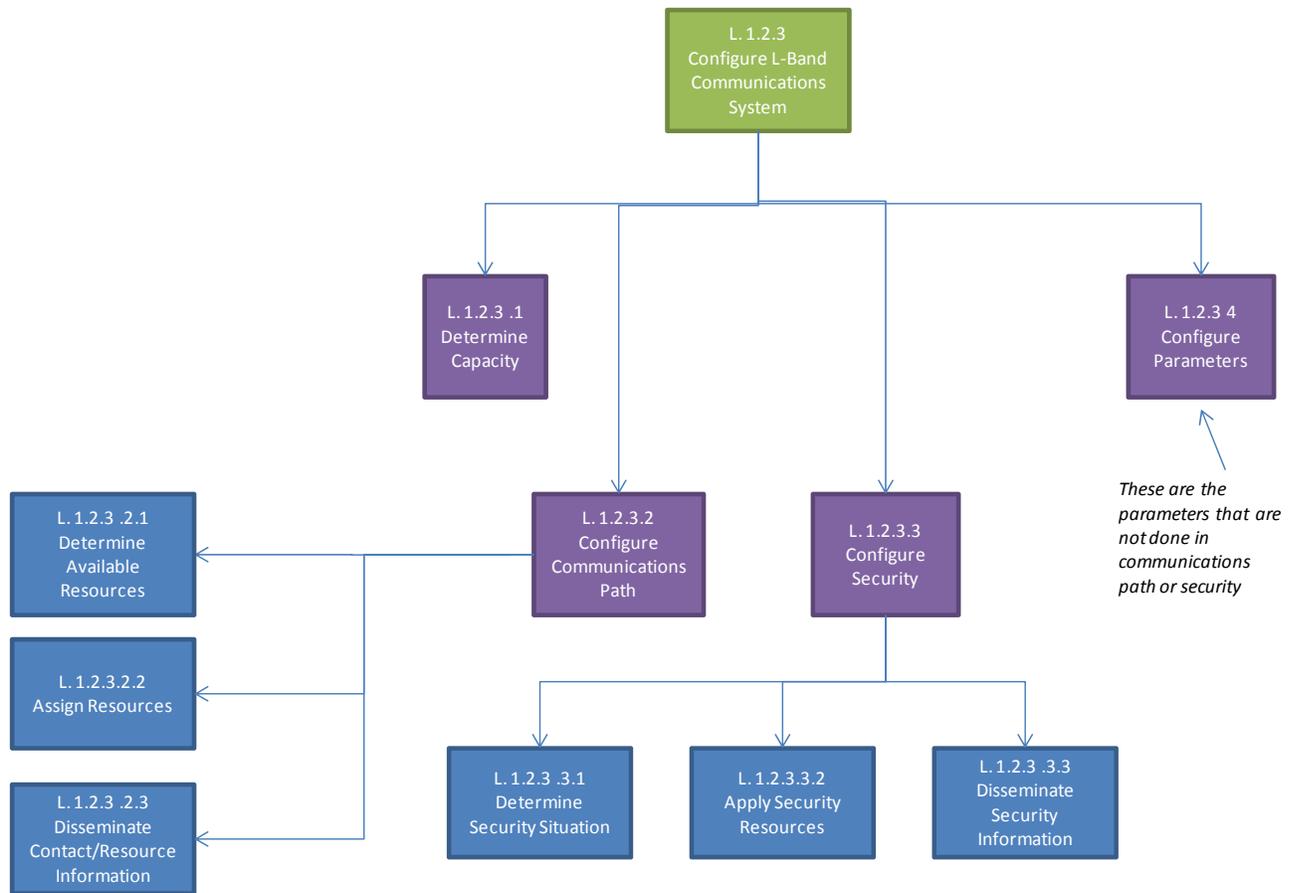


Figure 33.—Decomposition of configure L-band communications system.

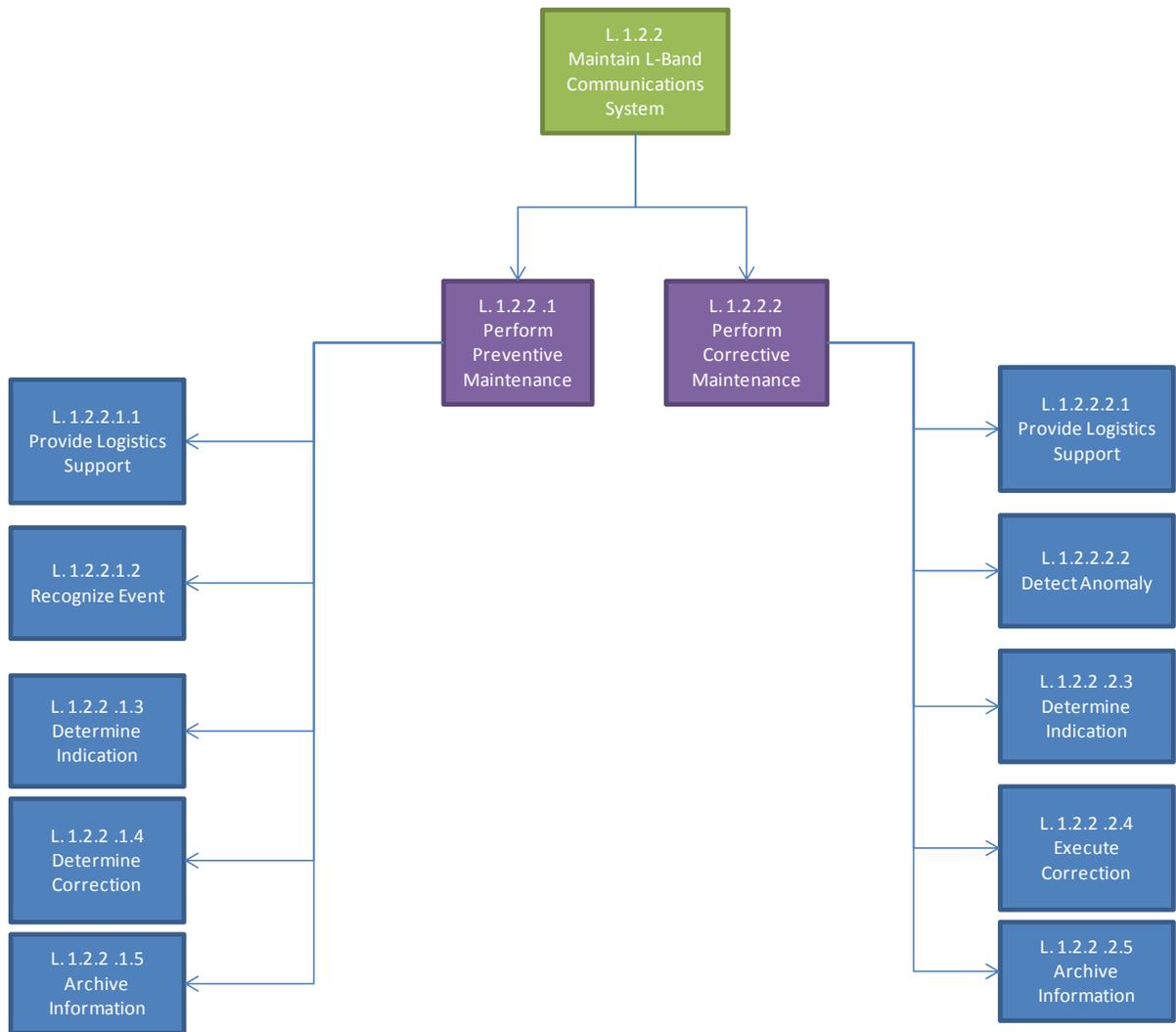


Figure 34.—Decomposition of maintain L-band communications system.

Appendix C.—Safety Hazard Analysis Worksheets

C.1 L-band Communication Safety Hazard Analysis (SHA) Table Cross Reference

For each of the five L-band communication system functions resulted from the functional system analysis and shown in Appendix A, a typical list of the types of messages transmitted is shown in Table 12. 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 12 provides a cross reference to the function’s hazard worksheet table.

TABLE 12.— SAFETY HAZARD ANALYSIS TABLE CROSS REFERENCE^{a,b}

	Information type (including corresponding function ID)	Message examples	Hazard table cross reference
1	Transceive ATS to airborne aircraft message L.1.1.1.1	<ul style="list-style-type: none"> • Contract requesting data • Contract acknowledgements • OTIS reports, addressed or broadcast communications • ORIS 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 • Available alternative routes (DYNAV), addressed communication • Urgent contact message (URCO), addressed and/or broadcast communications 	Table 13
	Transceive airborne aircraft to ATS message L.1.1.2.1	<ul style="list-style-type: none"> • Requests (i.e., demand, periodic, or event contract) for reports • Contract acknowledgements • Current and periodic position (FLIPCY), addressed communications • Meteorological data (FLIPCY), addressed communications • Ground speed (FLIPCY), addressed communications • Indicated heading, indicated air speed or match, vertical rate, selected level, and wind vector (SAP), 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 • Urgent contact message (URCO), addressed and/or broadcast communications 	Table 13
2	Transceive ATS to on-ground aircraft message L.1.1.1.2	<ul style="list-style-type: none"> • Contract requesting data • Contract acknowledgements • OTIS reports, addressed or broadcast communications • ORIS 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 • Available alternative routes (DYNAV), addressed communication • Urgent contact message (URCO), addressed and/or broadcast communications 	Table 13
	Transceive on- ground aircraft to ATS message	<ul style="list-style-type: none"> • Requests (i.e., demand, periodic, or event contract) for reports • Contract acknowledgements • Current and periodic position (FLIPCY), addressed communications 	Table 13

TABLE 12.— SAFETY HAZARD ANALYSIS TABLE CROSS REFERENCE^{a,b}

	Information type (including corresponding function ID)	Message examples	Hazard table cross reference
	L.1.1.2.2	<ul style="list-style-type: none"> • Meteorological data (FLIPCY), addressed communications • Ground speed (FLIPCY), addressed communications • Indicated heading, indicated air speed or mach, vertical rate, selected level, and wind vector (SAP), 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 • Urgent contact message (URCO), addressed and/or broadcast communications 	
3	Transceive airborne aircraft to airborne aircraft message L.1.1.3.1	<ul style="list-style-type: none"> • Trajectory intent exchange (AIRSEP), addressed and/or broadcast communications • Conflict negotiation (AIRSEP), addressed and/or broadcast communications • Resolution accept/confirmation 	Table 14

^aMessage types are based on services definitions presented in Ref. 2.

^bAcronyms are defined in Appendix A.

C.2 Hazard Analysis Worksheets

For each of the hazards identified for the L-band communication system, the potential causes of the hazard were listed. The worksheets are slightly modified worksheets from the tables provided in Reference 10. The modifications include but are not limited to different risk and risk analysis code (RAC) assessments. The system state was also identified. The system state used is the state that fosters the worst credible outcome. The safety hazard analysis was captured in the tabular and table format.

The columns shown in the safety hazard analysis 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 analysis code: 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 rationale for the resulting risk/RAC

C.2.1 L-band Air Traffic Services to Aircraft Hazards

The section presents the 15 identified L-band communication system hazards as they apply to messages exchanged between an ATS and an aircraft. The aircraft may be either airborne or 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 13 contains the hazard analysis worksheet for the following functions:

- L.1.1.1.1 Transceive ATS to Airborne Aircraft Message
- L.1.1.1.2 Transceive ATS to On-Ground Aircraft Message

- L.1.1.2.1 Transceive Airborne Aircraft to ATS Message
- L.1.1.2.2 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 L-band communication system:

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

Possible effects are unrelated to the services currently planned for an L-DACS; for example, the WCE would generally apply to using the data link for clearance-related services that may be provided over L-DACS.

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
<p>ATS— Aircraft Comm 1a</p>	<p>L-band communication capability totally unavailable—ground (facility wide). Ground cannot send/receive messages to any aircraft.</p>	<p>1. Hardware failure 2. Software failure 3. Radiofrequency (RF) interference</p>	<p>3D</p>	<p>Case 1</p> <ul style="list-style-type: none"> • 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). <p><i>OR</i></p> <ul style="list-style-type: none"> • 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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. <p>Case 3</p> <ul style="list-style-type: none"> • Aircraft diverts from route and aircrew attempts to send message indicating diversion and finds out he/she is unable to do so. • Airspace is NOT protected and results in potential conflict. • Ground system realizes aircraft position from surveillance information, out-of-conformance alert, or conflict alert. • Controller cannot contact aircraft and must transfer control to another control facility to move the aircraft in conflict with the diverting aircraft. • 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. 	<p>Aircraft may or may not be aware of ground failure (e.g., until aircraft attempts a transmission and it is not acknowledged).</p>

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 1b	L-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	<p>Case 1</p> <ul style="list-style-type: none"> • Controller needs to issue new or amended clearances to several aircraft. • When trying to transmit clearances, controller is informed that messages cannot be transmitted (voice nor data available). <p><i>OR</i></p> <ul style="list-style-type: none"> • 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. <p><i>OR</i></p> <p>Case 2</p> <ul style="list-style-type: none"> • 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. <p><i>OR</i></p> <p>Case 3</p> <ul style="list-style-type: none"> • Aircraft diverts from route and aircrew attempts to send message indicating diversion and finds out he or she is unable to do so. • Airspace is NOT protected and results in potential conflict. • Ground system realizes aircraft position from surveillance information, out-of-conformance alert, or conflict alert. • Controller cannot contact aircraft and must transfer control to another control facility to move the aircraft in conflict with the diverting aircraft. • 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. 	Aircraft may or may not be aware of ground failure (e.g., until aircraft attempts a transmission and it is not acknowledged).

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 2	L-band communication capability partially unavailable— ground. Ground cannot send or receive messages to one or more aircraft.	1. Hardware failure 2. Software failure 3. RF interference	3C	<p>Case 1</p> <ul style="list-style-type: none"> • 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. <p><i>OR</i></p> <ul style="list-style-type: none"> • 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. <p><i>OR</i></p> <p>Case 2</p> <ul style="list-style-type: none"> • Aircrew attempts to send clearance response. • Both current and new clearances are protected. • Workload remains within expected workload so no hazard. <p><i>OR</i></p> <p>Case 3</p> <ul style="list-style-type: none"> • Aircraft diverts from route and aircrew attempts to send message indicating diversion and finds out he or she is unable to do so. • Airspace is NOT protected and results in potential conflict. • Ground system realizes aircraft position from surveillance information, out-of-conformance alert, or conflict alert. • Controller cannot contact aircraft and must transfer control to another sector or control facility to move the aircraft in conflict with the diverting aircraft. • 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. 	This could be loss of communications for a sector within a facility.

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 3	L-band system communication capability unavailable—aircraft (single aircraft). Aircrew cannot send or receive messages to ground.	1. Hardware failure 2. Software failure 3. Insufficient coverage 4. RF interference	4C	<ul style="list-style-type: none"> Aircrew needs to request new or amended clearance. When trying to request the new clearance, aircrew determines that message cannot be transmitted. <p>OR</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 reestablish or maintain separation. Resolving the loss of separation could cause time-critical aircrew decisions and excessive increased workload. 	

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
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	<ul style="list-style-type: none"> 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. 	
ATS— Aircraft Comm 8	A message affecting separation is acted on by an unintended recipient.	<ol style="list-style-type: none"> Address is corrupted Misdelivered Step-on 	2D	<p>Case 1</p> <ul style="list-style-type: none"> 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. (<i>When the unintended recipient is not under the control authority, see ATS-Aircraft COMM-6.</i>) Upon receipt of the WILCO to the clearance, the controller: <ul style="list-style-type: none"> (a) does not realize that the WILCO is from a different aircraft than the intended one or 9b) 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. <p>Case 2</p> <ul style="list-style-type: none"> 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. 	

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 9	A message NOT affecting separation is acted on by an unintended recipient.	<ol style="list-style-type: none"> 1. Address is corrupted 2. Misdellivered 3. Step-on 	5D	<p>Case 1</p> <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> (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 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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. 	
ATS— Aircraft Comm 10	A message affecting separation is received too late (or expired).	<ol style="list-style-type: none"> 1. Late delivery 2. Ground and air time is out of sync 	2D	<ul style="list-style-type: none"> • Clearance is sent and expires before a response is received. <p><i>OR</i></p> <ul style="list-style-type: none"> • 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. 10).

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 11	Message NOT affecting separation is received too late (or expired).	<ol style="list-style-type: none"> 1. Late delivery 2. Ground and air time is out of sync 	5D	<p>Case 1</p> <ul style="list-style-type: none"> • 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. • Since 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 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS – Aircraft Comm 12	A message affecting separation is corrupted.	The communication system corrupts a message.	3D	<p>Case 1</p> <ul style="list-style-type: none"> • A clearance is sent and the contents are corrupted, but still credible. • The aircrew accepts the corrupted clearance. • Since 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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. <p>Case 3</p> <ul style="list-style-type: none"> • The address or all sign is the part of the message that becomes corrupted. 	

TABLE 13.—AIRCRAFT HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect	Comments
ATS— Aircraft Comm 13	A message NOT affecting separation is corrupted.	The communication system corrupts a message.	5D	<p>Case 1</p> <ul style="list-style-type: none"> • 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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. 	
ATS— Aircraft Comm 14	A message affecting separation is sent or received out of sequence.	<ol style="list-style-type: none"> 1. Message sent second is received prior to message sent first. 2. Communication system does not deliver messages in order. 	3D	<p>Case 1</p> <ul style="list-style-type: none"> • 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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 is sent or received out of sequence.	<ol style="list-style-type: none"> 1. Message sent second is received prior to message sent first. 2. Communication system does not deliver messages in order. 	5D	<p>Case 1</p> <ul style="list-style-type: none"> • 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. <p>Case 2</p> <ul style="list-style-type: none"> • 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. 	

C.2.2 Aircraft-to-Aircraft Message

This section presents the 15 identified NAS communication hazards as they apply to ATS-only messages exchanged between aircraft. Table 14 contains the hazard analysis worksheet for the following function:

L.1.1.3.1.1 Transceive Airborne Aircraft to Airborne Aircraft Message

The system state leading to WCE is the same for all aircraft-to-aircraft hazards due to the L-band communication system:

- Peak traffic conditions
- IMCs (see-and-avoid may not be possible)
- Adverse weather conditions

TABLE 14.—AIRCRAFT-TO-AIRCRAFT MESSAGE HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect
Aircraft— Aircraft Comm 1	Aircraft-aircraft communication capability totally unavailable (known)	1. Hardware failure 2. Software failure 3. Insufficient capacity 4. Radiofrequency (RF) interference	2D	If L-DACS is used to enable an AIRSEP service, complete or partial loss of communication could result in a loss of situational awareness and loss of separation.
Aircraft— Aircraft Comm 2	Aircraft-aircraft communication capability partially unavailable (known)	1. Hardware failure 2. Software failure 3. Insufficient capacity 4. RF interference	2D	
Aircraft— Aircraft Comm 3	There is a total loss of communication between a single aircraft and all other aircraft.	1. Hardware failure 2. Software failure 3. Insufficient coverage 4. RF interference	2D	
Aircraft— Aircraft Comm 4	Aircraft-aircraft communication fails	1. Message (or part) does not make it to recipient. 2. Response message (or part) does not make it back to initiator.	2D	
Aircraft— Aircraft Comm 5	Message fails with multiple aircraft		2D	
Aircraft— Aircraft Comm 6	N/A		N/A	
Aircraft— Aircraft Comm 7	N/A		N/A	
Aircraft— Aircraft Comm 8	A message affecting separation is acted on by an unintended recipient.	1. Aircraft address is corrupted. 2. Misdelaivered	2D	
Aircraft— Aircraft Comm 9	A message NOT affecting separation is acted on by an unintended recipient.	1. Address is corrupted. 2. Misdelaivered	N/A	
Aircraft— Aircraft Comm 10	A message affecting separation received too late (or expired)		2D	

TABLE 14.—AIRCRAFT-TO-AIRCRAFT MESSAGE HAZARDS DUE TO THE L-BAND COMMUNICATION SYSTEM

Hazard no.	Hazard description	Causes	Risk analysis code (RAC)	Possible effect
Aircraft— Aircraft Comm 11	Message NOT affecting separation received too late (or expired)		N/A	
Aircraft— Aircraft Comm 12	A message affecting separation corrupted	The communication system corrupts a message.	2D	
Aircraft— Aircraft Comm 13	A message NOT affecting separation corrupted (undetected)		N/A	
Aircraft— Aircraft Comm 14	A message affecting separation sent/received out of sequence		2D	
Aircraft— Aircraft Comm 15	A message NOT affecting separation sent/received out of sequence		N/A	

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

Communications Operating Concepts and Requirements (COCR) Version 2.0 documents operational and safety requirements for ATS data communications services and information security requirements for air traffic services (ATS) and autonomous operations services (AOS). A service-level operational safety assessment (OSA) is performed to derive safety requirements (Ref. 2).

The following subsections summarize the assessment for the services applicable to the proposed L-band communications system as proposed by the Future Communication Infrastructure (FCI) Aeronautical Data Services Definition Task Report (Ref. 5).

D.1 Safety Objectives Definitions

Table 14 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 15.

TABLE 15.—SAFETY OBJECTIVE DEFINITIONS (REF. 2)

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 Summary of the L-band ATS Services Operational Safety Assessment

The COCR (Ref. 2) provides a useful operational safety assessment summary applicable to the L-band ATS services case:

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 misdelivered 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 L-band system (Ref. 5) are included in this document, thus presenting only a subset of the corresponding section and tables of the COCR.

Table 16 presents the OSA hazard severity and corresponding safety objectives for service categories for the two high-level safety hazards. As discussed earlier, introduction of an L-band system is assumed to correspond to Phase II future radio system (FRS) evolution.

TABLE 16.—AIR TRAFFIC SERVICES 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
Advisory services (AVS)	3	Remote	2	Extremely remote
Emergency information services (EIS)	4	Probable	3	Remote
Flight position/intent/preferences service (FPS)	3	Remote	2	Extremely remote
Miscellaneous services (MCS)	1	Extremely improbable	1	Extremely improbable

Figure 35 and Figure 36 present safety risk matrices for loss of service and hazardously misleading information hazards, respectively.

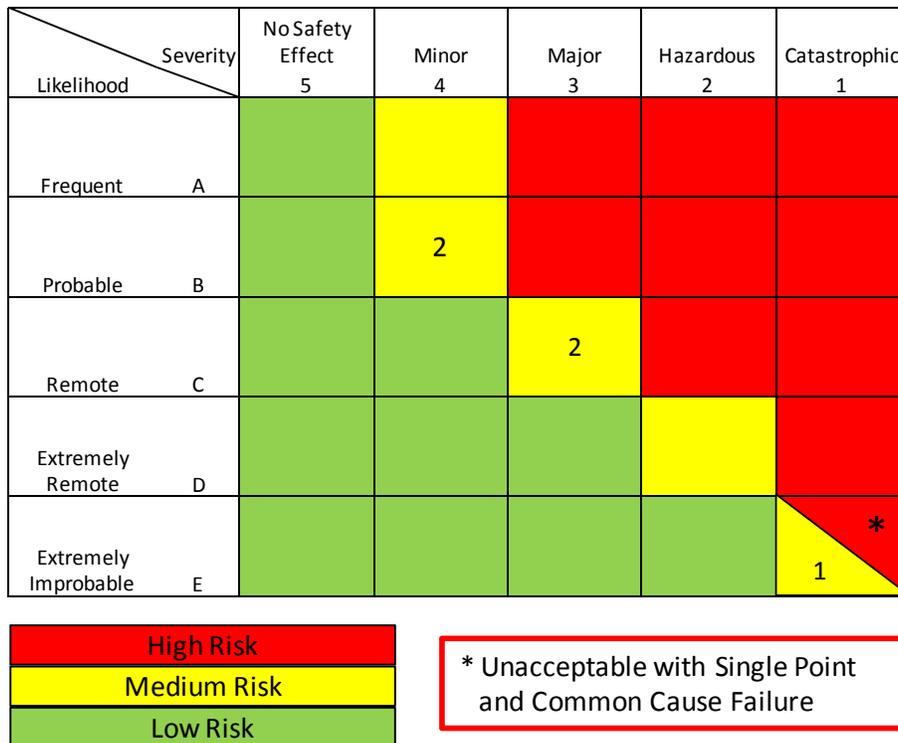


Figure 35.—Safety risk matrix—loss of service.

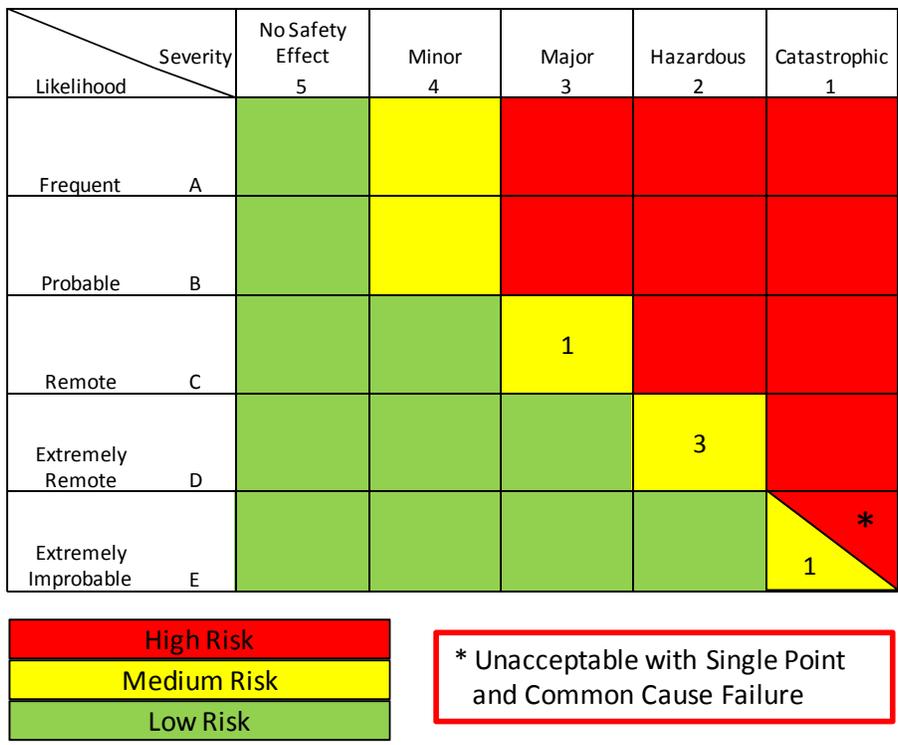


Figure 36.—Safety risk matrix—hazardously misleading information.

D.3 Service-Level Safety Assessment (L-band Services Only)

As described in the COCR (Ref. 2), Table 17 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 17.—SERVICE LEVEL SAFETY ASSESSMENT

Service ^a	Continuity	Integrity	Availability (provision)	Availability (use)
D-ORIS	Minor	Hazardous	Major	Minor
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
SAP	Minor	Major	Major	Minor
PPD	No safety effect	Minor	No safety effect	No safety effect
D-SIGMET	Minor	Hazardous	Minor	Minor
DYNAV	No safety effect	Minor	No safety effect	No safety effect
URCO	Major	Major	Minor	Minor
AIRSEP	Major	Hazardous	Hazardous	Major

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 (Ref. 10) document were reviewed. Most, but not all, of the controls were found applicable to the proposed L-band system. Additional controls were considered.

Table 18 includes the required controls (i.e., 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 analysis code (RAC) for each hazard.

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing 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 to the proposed air/ground communication system hazards.
2	The NAS shall provide air-ground communications capabilities on a continuous basis (NAS-SR-1000 3.6.1.E).	The NAS shall provide air-ground communications continuously (NAS SR-1000, part of 20330). Control applies to air/air and air/ground communications.
3	The air-ground 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).	<p>The following controls apply to air/air and air/ground communications:</p> <p>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).</p> <p>The NAS shall strive to restore critical system service to users/specialists within 6 seconds of failure (NAS SR-1000, 22900).</p> <p>The NAS shall strive to restore routine system service to users/specialists within 1.68 hours of failure (22920).</p> <p>The NAS shall strive to restore essential system service to users/specialists within 10 minutes of failure (NAS SR-1000, 22910).</p> <p>No single point of failure of equipment, system, installation or facility shall cause loss of service to the user/specialist.</p>
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 air-ground 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.

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
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 to the proposed air/air and air/ground communication system hazards.
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 Regulations [FAR] 91.113 <ul style="list-style-type: none"> • Alternate control procedure (i.e., light gun instructions from towers) • “See and Avoid” procedures are prescribed. (Aeronautical Information Manual [AIM] 5-5-8 and Federal Aviation Regulations [FAR] 91.113) 	Existing control applies to the proposed air/air and air/ground communication system hazards.
7	Current separation standards. (FAA order 7110.65)	Existing control applies to the proposed air/air and air/ground communication system hazards.
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)] <ul style="list-style-type: none"> • 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 to the proposed air/air and air/ground communication system hazards.
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 to the proposed air/air and air/ground communication system hazards.
10	Aircraft-to-aircraft communications remains available (airborne or on-ground)	Existing control applies to the proposed air/ground communication system hazards.
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 to the proposed air/air and air/ground communication system hazards.
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 to the proposed air/air and air/ground communication system hazards.
13	TCAS is available for Transport Category Aircraft. (FAR 14CFR Part 129.18)	Existing control applies to the proposed air/air and air/ground communication system hazards.
14	Procedures requiring “pilot acknowledgement/read back” when ATC issues clearances or instructions (7110.65, 2-4-3).	Existing control applies to the proposed air/air and air/ground communication system hazards.
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 to the proposed air/air and air/ground communication system hazards.
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 to the proposed air/ground communication system hazards.
17	Air-to-air communications still available, so another aircrew may hear a step on or incorrect readback and notify, and/or aircraft can announce intentions on party line.	Existing control applies to the proposed air/air communication system hazards.

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
18	Procedures requiring aircraft identification for clearance (7110.65, 2-4-20) <ul style="list-style-type: none"> • 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 to the proposed air/ground communication system hazards.
19	Procedures requiring Facility Identification (7110.65, 2-4-8) for the ATC facility giving the clearances.	Existing control applies to the proposed air/ground communication system hazards.
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.” <ul style="list-style-type: none"> • The aircraft shall accept clearances/instructions only from the current control authority. 	Existing control applies to the proposed air/ground communication system hazards.
21	The intended recipient is also listening so he/she may query or chime in (party line).	Existing control applies to the proposed air/ground communication system hazards.
22	Voice procedures: <ul style="list-style-type: none"> • Procedures for giving aircraft ID in granting clearances • Procedures for communication when aircraft have same or similar call signs 	Existing control applies to the proposed air/ground communication system hazards.
23	Voice and data communications shall have the following response capabilities: <ul style="list-style-type: none"> • Initiation of one-way air-ground voice transmissions shall be possible within 250 milliseconds of keying the specialist’s microphone. • The ground-air transmission time for data messages shall not exceed 6 seconds (NAS-SR-1000 3.6.1.A.5). 	The NAS shall assure ground-air 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 to the proposed air/ground communication system hazards.
25	ADS report (surveillance) can provide aircraft position (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 5 Radar).	Existing control applies to the proposed air/ground communication system hazards.
26	CPDLC pilot position reports can provide aircraft position.	Existing control applies to the proposed air/ground communication system hazards.
27	Oceanic separation standards (FAA Order 7110.65P Effective Data August 4, 2005 Chapter 8 Offshore/Oceanic Procedures).	Existing control applies to the proposed air/ground communication system hazards.
28	Clearly intelligible air-ground 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 to the proposed air/air communication system hazards.
30	Only one Pre-Departure Clearance (PDC) is sent (thus cannot get out of order).	Existing control applies to the proposed air/ground communication system hazards.
31	Airport design minimizes runway and taxiway crossing by vehicles.	N/A
32	Standard no com procedures.	Covered by Control 6

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
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 a ground 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)	N/A
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 C 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.	N/A
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.”	N/A
36	Mobile-to mobile communications still available	N/A
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 air-ground 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.	N/A
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.	N/A
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.”	N/A
42	FAA Order 7110.65 Paragraph 3-1-12, Visually Scanning Runways - Local controllers shall visually scan runways to the maximum extent possible.	N/A
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.	N/A
44	CFR Part 139.205(b)(19) requires that these procedures be included in the Airport Certification Manual (ACM).	N/A

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
45	Controller use of full call sign/runway ID (not shortened) (FAA Order 7110.65P 3-7-1 Ground Traffic Movement Phraseology)	N/A
46	Controllers must establish position before moving vehicle (FAA Order 7110.65 Section 1 General 3-1-7 Position Determination)	N/A
47	Procedures for identification of vehicles requesting clearances (Part 139CFR ground vehicle guidebook for training)	N/A
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)	N/A
49	Vehicle readback procedures (voice) (Part 139CFR ground vehicle guidebook for training)	N/A
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 which 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. The number of direct-access calls that are blocked because of saturation of equipment shall not exceed 1 in 1000 calls.	N/A
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: <ul style="list-style-type: none"> • 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

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
60	Inter-facility 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 which 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
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: <ul style="list-style-type: none"> • 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 to the proposed air/air communication system hazards
78	Standard operating procedures/pilot training	Existing control applies to the proposed air/air communication system hazards
79	Redundancy to prevent interruption - centers can talk to multiple facilities (2 or 3 facilities typical) and command center	N/A

TABLE 18.—COMMUNICATIONS SYSTEM SAFETY CONTROLS

Existing control ref. no. ^a	Existing NAS controls	Proposed controls
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 (LOA) 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 air-ground 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 to the proposed air/ground communication system hazards
85	Data Link Messages are time stamped so order can be determined	Existing control applies to the proposed air/ground communication system hazards
86	Data link response message indicate to which message they refer	Existing control applies to the proposed air/ground communication system hazards
89		The NAS shall comply with national standards to avoid the interference of new systems with existing systems. (NAS SR-1000, 19310)
90		L-DACS shall comply with the performance and infrastructure requirements.

^aControl numbers 1 to 83 correspond to the existing controls, Table 2-3 p. 14 of Ref. 10. 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.

Appendix F.—SP 800–53 Security Controls Applicable to L–DACS

The SP 800–53 security controls catalog contains 17 families of controls⁷¹ that belong to three control classes: management, operational, and technical.

Table 19 summarizes the classes and families in the security control catalog and the associated family identifiers. Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. Families of controls found relevant to the proposed L–DACS are highlighted in yellow.

TABLE 19.—SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

Identifier	Control family	Control class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Evaluation of the controls resulted in identification of 46 of the 171 individual controls relevant to this assessment. They are listed in Table 20.

TABLE 20.—SECURITY CONTROLS RELEVANT TO THE PROPOSED L–DACS^a

Control families	Control	Control ID
Access control (AC)	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	AC–3
	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	AC–4
	The information system enforces separation of duties through assigned access authorizations.	AC–5
	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	AC–6

⁷¹As noted in NAS SR–1000, the seventeen security control families in NIST Special Publication 800–53 are closely aligned with the 17 security-related areas in FIPS 200 specifying the minimum security requirements for protecting federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class.

TABLE 20.—SECURITY CONTROLS RELEVANT TO THE PROPOSED L-DACS^a

Control families	Control	Control ID
	The information system enforces a limit of [<i>Assignment: organization-defined number</i>] consecutive invalid access attempts by a user during a [<i>Assignment: organization-defined time period</i>] time period. The information system automatically [<i>Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]</i>] when the maximum number of unsuccessful attempts is exceeded.	AC-7
	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	AC-8
	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	AC-9
	The information system limits the number of concurrent sessions for any user to [<i>Assignment: organization-defined number of sessions</i>].	AC-10
	The information system prevents further access to the system by initiating a session lock after [<i>Assignment: organization-defined time period</i>] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures	AC-11
	The information system automatically terminates a remote session after [<i>Assignment: organization-defined time period</i>] of inactivity.	AC-12
	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.	AC-15
	The information system appropriately labels information in storage, in process, and in transmission.	AC-16
Audit and accountability (AU)	The information system generates audit records for the following events: [<i>Assignment: organization-defined auditable events</i>].	AU-2
	The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events	AU-3
	The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [<i>Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)</i>].	AU-5
	The information system provides an audit reduction and report generation capability.	AU-7
	The information system provides time stamps for use in audit record generation.	AU-8
	The information system protects audit information and audit tools from unauthorized access, modification, and deletion	AU-9
	The information system provides the capability to determine whether a given individual took a particular action.	AU-10

TABLE 20.—SECURITY CONTROLS RELEVANT TO THE PROPOSED L-DACS^a

Control families	Control	Control ID
Identification and authentication (IA)	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	IA-2
	The information system identifies and authenticates specific devices before establishing a connection.	IA-3
	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals	IA-6
	The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	IA-7
Systems communications protection (SC)	The information system separates user functionality (including user interface services) from information system management functionality.	SC-2
	The information system isolates security functions from nonsecurity functions.	SC-3
	The information system prevents unauthorized and unintended information transfer via shared system resources	SC-4
	The information system protects against or limits the effects of the following types of denial of service attacks: [<i>Assignment: organization-defined list of types of denial of service attacks or reference to source for current list</i>].	SC-5
	The information system limits the use of resources by priority.	SC-6
	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	SC-7
	The information system protects the integrity of transmitted information.	SC-8
	The information system protects the confidentiality of transmitted information	SC-9
	The information system terminates a network connection at the end of a session or after [<i>Assignment: organization-defined time period</i>] of inactivity.	SC-10
	The information system establishes a trusted communications path between the user and the following security functions of the system: [<i>Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication</i>].	SC-11
	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	SC-13
	The information system protects the integrity and availability of publicly available information and applications.	SC-14
	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	SC-15
	The information system reliably associates security parameters with information exchanged between information systems	SC-16
	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.	SC-20
	The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.	SC-21
	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.	SC-22
	The information system provides mechanisms to protect the authenticity of communications sessions.	SC-23

TABLE 20.—SECURITY CONTROLS RELEVANT TO THE PROPOSED L-DACS^a

Control families	Control	Control ID
System information integrity (SI)	The information system verifies the correct operation of security functions [<i>Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]</i>] and [<i>Selection (one or more): notifies system administrator, shuts the system down, restarts the system</i>] when anomalies are discovered.	SI-6
	The information system detects and protects against unauthorized changes to software and information.	SI-7
	The information system implements spam protection	SI-8
	The information system checks information for accuracy, completeness, validity, and authenticity.	SI-10
	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	SI-11

^aOnly the controls that impose limitations/requirements on the information system are listed here. Additional controls may apply noting organizational responsibilities. Refer to Ref. 20 for complete list of controls.

References

1. Safety Risk Management Guidance for System Acquisitions (SRMGSA), U.S. Department of Transportation Federal Aviation Administration Air Traffic Organization, Safety Services 02/08/2007
2. Communications Operating Concept and Requirements for the Future Radio System (COCR), Eurocontrol/FAA, Version 2.0, May 2007.
3. Next Generation Air Transportation System (NextGen) Integrated Work Plan, Joint Planning and Development Office, Version 1.0, September 2008. http://www.jpdo.gov/iwp/IWP_V1.0_No_Appendices.pdf
4. Zelkin, N. and Henriksen, S., L-Band Digital Aeronautical Communications System Engineering— Concepts of Use, Systems Performance Requirements, and Architecture, NASA/CR—2001-216326.
5. FCI Aeronautical Data Services Definition Task Report, ITT AES, March 31, 2009.
6. National Airspace System (NAS) System Engineering Manual (SEM), Version 3.1, Federal Aviation Administration ATO Operations Planning, 06/06/06, p. 4.10–4.
7. FAA Air Traffic Organization Safety Management System Manual , Version 2.1, 05/08
8. FAA System Safety Handbook, http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/.
9. Future Aeronautical Communications Infrastructure Technology Investigation, ITT Corporation, 04/08, p. xv.
10. National Airspace System Communication System Safety Hazard Analysis and Security Threat Analysis, Federal Aviation Administration, 02/21/06, p. 7.
11. RTCA DO-290, Safety and Performance Requirements Standard for Air Traffic Data Link Services in Continental Airspace (Continental SPR Standard), April 29, 2004.
12. RTCA SC-203 Operational Services and Environmental Definition (OSED), Draft, October 23, 2009.
13. 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, 4 August 2009.
14. System Wide Information Sharing (SWIM), FAA, Presented to: SWIM TIM on Infrastructure and Technology by Mike Hritz FAA SWIM Planning and Prototyping Lead, 14 May 2008.
15. FAA Order 1370.82, Information Systems Security Program, 6/9/00.
16. NIST, Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems. Computer Security Division, National Institute of Standards and Technology. Gaithersburg, MD, 2004. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.
17. Stoneburner, G., Goguen, A., and Feringa, A., NIST, Special Publication 30, Risk Management Guide for Information Technology Systems. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
18. Security of Aircraft in the Future European Environment (SAFE) project, <http://www.safee.reading.ac.uk/home.htm>
19. SBSS PDR Part IIID. Security, ITT Corporation, November 15, 2007.
20. Recommended Security Controls for Federal Information Systems, NIST SP800-53, December 2007.
21. NAS SR-1000, National Airspace System, System Requirements Specification (13 Jan 2005).

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 01-01-2011		2. REPORT TYPE Final Contractor Report		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE L-Band Digital Aeronautical Communications System Engineering--Preliminary Safety and Security Risk Assessment and Mitigation			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Zelkin, Natalie; Henriksen, Stephen			5d. PROJECT NUMBER NNC05CA85C		
			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-17261		
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-2011-216327		
12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified-Unlimited Subject Category: 04 Available electronically at http://www.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 NNC05CA85C, Task 7: "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 L-band (960 to 1164 MHz) terrestrial en route communications 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 a preliminary 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 L-band communication system after the technology is chosen and system rollout timing is determined. The security risk analysis resulted in identifying main security threats to the proposed system as well as noting additional threats recommended for a future security analysis conducted at a later stage in the system development process. The document discusses various security controls, including those suggested in the COCR Version 2.0.					
15. SUBJECT TERMS Aircraft communication; Wireless communications; Air traffic control					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 95	19a. NAME OF RESPONSIBLE PERSON STI Help Desk (email: help@sti.nasa.gov)
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (include area code) 443-757-5802

