Chapter 1: Introduction to the System Safety Handbook

1.1 Introduction

The System Safety Handbook (SSH) was developed for the use of Federal Aviation Administration (FAA) employees, supporting contractors and any other entities that are involved in applying system safety policies and procedures throughout FAA. As the Federal agency with primary responsibility for civil aviation safety, the FAA develops and applies safety techniques and procedures in a wide range of activities from NAS modernization, to air traffic control, and aircraft certification. On June 28, 1998, the FAA Administrator issued Order 8040.4 to establish FAA safety risk management policy. This policy requires all the Lines of Business (LOB) of the FAA to establish and implement a formal risk management program consistent with the LOB's role in the FAA. The policy reads in part: "The FAA shall use a formal, disciplined, and documented decision making process to address safety risks in relation to high-consequence decisions impacting the complete life cycle."

In addition, the Order established the FAA Safety Risk Management Committee (SRMC) consisting of safety and risk management professionals representing Associate/Assistant Administrators and the offices of the Chief Counsel, Civil Rights, Government and Industry Affairs, and Public Affairs. The SRMC provides advice and guidance, upon request from the responsible program offices to help the program offices fulfill their authority and responsibility for implementing Order 8040.4.

This System Safety Handbook provides guidance to the program offices. It is intended to describe "how" to set up and implement the safety risk management process. The SSH establishes a set of consistent and standardized procedures and analytical tools that will enable each LOB or program office in the FAA to comply with Order 8040.4.

In FAA, the Acquisition Management System (AMS) provides agency-wide policy and guidance that applies to all phases of the acquisition life cycle. Consistent with Order 8040.4, AMS policy is that System Safety Management shall be conducted throughout the acquisition life cycle (section 2.9.13) of the AMS. The SSH is designed to support this AMS system safety management policy. It is included in the FAA Acquisition System Toolset (FAST), and is referenced in several of the FAST process documents. It is also designed to support safety risk management activities in FAA not covered by AMS policy and guidance.

This SSH is intended for use in support of specific system safety program plans. While the SSH provides guidance on "how" to perform safety risk management, other questions concerning "when, who, and why" should be addressed through the three types of plans discussed in this document: System Safety Management Plan (SSMP), and a System Safety Program Plan (SSPP), and an Integrated System Safety Program Plan (ISSPP). The SSH focuses on "how" to perform safety risk management, while these planning documents describe, in Chapter 5, the organization's processes and procedures for implementing system safety.

High-level SSMPs describe general organizational processes and procedures for the implementation of system safety programs, while more specific SSPPs are developed for individual programs and projects. The ISSPP is intended for large complex systems with multiple subcontractors. The SRMC is responsible for developing an overall FAA SSMP, while the System Engineering Council develops the SSMP for AMS processes, such as Mission Analysis, Investment Analysis, and Solution Implementation. Integrated Product Team (IPT) leaders, program managers, project managers and other team leaders develop SSPPs appropriate to their activities. Chapter 4 of the SSH provides guidance for the development of a SSPP.

1.2 Purpose

The purpose of this handbook is to provide instructions on how to perform system safety engineering and management for FAA personnel involved in system safety activities, including FAA contractor management, engineering, safety specialists, team members on Integrated Product Development System (IPDS) teams, analysts and personnel throughout FAA regions, centers, facilities, and any other entities involved in aviation operations.

1.3 Scope

This handbook is intended to support system safety and safety risk management throughout the FAA. It does not supercede regulations, or other procedures or policies; however, this handbook provides best practices in system safety engineering and management. When these regulations or procedures exist, this handbook will indicate the reference and direct the reader to that document. If a conflict exists between the SSH and FAA policies and regulations, the policies and regulations supercede this document. However, if results of analysis using the tools and techniques in this SSH identify policy or regulatory issues that conflict with existing FAA policies and regulations, the issues should be brought to the attention of the Office of System Safety (ASY), and consideration should be given to changing the policy or regulation. This handbook is also intended to provide guidance to FAA contractors who support the FAA by providing systems and/or analyses. This handbook does not supercede the specific contract, but can be referenced in the statement of work or other documents as a guide.

1.4 Organization of the Handbook

The SSH is organized from general to specific instructions. The first three chapters provide a brief overview of system safety policy, system safety processes, definition of what system safety is as practiced in FAA, and some common principles of the safety discipline. Chapters 4-6 explain how to establish a system safety program, how to prepare the required system safety plans, and how to perform system safety integration and safety Comparative Safety Assessment. Chapter 7 describes how to perform integrated system hazard analysis. Chapters 8 and 9 discuss hazard analysis tasks and some of the analytical techniques used in system safety analysis. Chapter 10 discusses how to perform system software safety. Chapter 11 explains test and evaluation safety guidance. Chapter 12 is focused on facilities and is directed to Occupational Health and Safety aspects of FAA

facilities and equipment operation. Chapter 13 is a special discussion of the commercial launch vehicle safety and certification process. Chapter 14 addresses training, Chapter 15 discusses operational risk management, Chapter 16 treats Organizational Systems in Aviation, and Chapter 17 concludes with Human Factors Safety Principles.

1.5 Relationship of the SSH to the AMS

The AMS contains guidance to the acquisition engineers in the FAA Acquisition System Toolset (FAST). The SSH is a tool within the FAST toolset. AMS Section 2 refers to the following process documents that contain further detailed guidance on implementation of the system safety management process.

Mission Analysis Process (MAP)
Investment Analysis Process (IAP)
Integrated Program Plan (IPP)
Acquisition Strategy Paper (ASP)

In addition, the following eight appendices to the Investment Analysis Plan (IAP) contain guidance related to system safety:

Appendix A Investment Analysis Plan
Appendix B Requirements Document
Appendix C Investment Analysis Process Flow Discussion
Appendix D Candidate Solution Identification & Analysis Discussion
Appendix F Acquisition Program Baseline
Appendix G Investment Analysis Report
Appendix H Investment Analysis Briefing
Appendix J Definitions and Acronyms

Where these FAST documents indicate a requirement for including system safety activities, or results of safety analyses in documentation or briefings, they generally reference the appropriate chapter in the SSH for a discussion of how to comply with the requirement. Figure 1-1 shows the flowdown of system safety relationships from the AMS Section 2 the other FAST documents listed above Section 2.9.13 System Safety Management is the primary policy statement in Section 2. It states as a requirement that each line of business shall implement a system safety program in

accordance with FAA Order 8040.4. The second tier of documents provide further guidance on how to implement the order, and the Appendices to the Investment Analysis Process document provide templates and formats for documentation that will be taken to the JRC.
Table 1-1 shows the applicability of each chapter in this handbook to the applicable AMS segment.

Table 1-1: System Safety Handbook vs. AMS Segment

AMS Segment	All	Mission Analysis	Investment Analysis	Solution Implementation	In Service Management	Service Life Extension
Applicable Handbook Chapters	2,3,6,7, 8,12,13,17	4	5	9,10,11	9,10,11,15,16	9,10,11,15, 16
Applicable Appendices	A, C, D, E, G, H		B	J	F, J	J
Launch Unique	13					

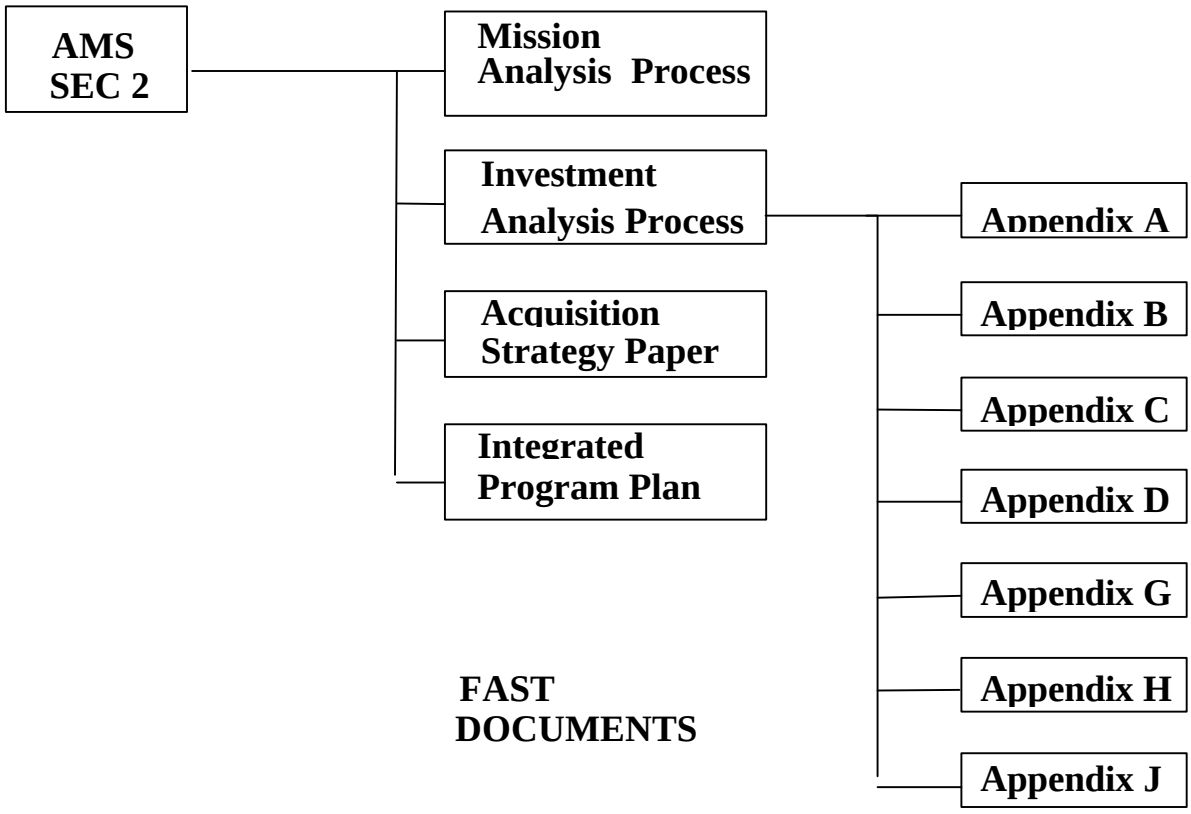

Figure 1-1: Documents Affected by the System Safety Policy Changes to the Acquisition Management System (AMS)

1.6 System Safety Objectives

This handbook supports the achievement of the following system safety objectives:

- Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- Hazards associated with the system (and its component subsystems) are identified, tracked, evaluated, and eliminated, or the associated risk is reduced to a level acceptable to FAA management throughout the entire life cycle of a system. Risk is described in Comparative Safety Assessment terms. See Chapter 3.
- The safety design order of precedence is applied and FAA management accepts the residual risk.
- Safety analyses and assessments are performed in support of the FAA safety risk management efforts and are in accordance with the best safety engineering practices.
- Historical safety data, including lessons learned from other systems, are considered and used in safety assessments and analyses.
- Minimum risk is sought in accepting and using new technology, materials, or designs: and new production, test and operational techniques in the NAS.
- Retrofit actions required to improve safety are minimized though the timely inclusion of safety features during research, technology development, and acquisition of a system.
- Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to FAA management.
- Consideration is given early in the life cycle to system safety through the end of the life cycle which includes system decommissioning.
- Significant safety data are documented as “lessons learned” and are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

1.7 Glossary

Appendix A contains a glossary of terms that are used throughout the handbook. It is important to understand the difference between a hazard and a risk, for example, and how these terms relate to the system safety methods. The glossary also provides discussion on different definitions associated with specific system safety terminology. It is important to understand the different definitions. The glossary can be used as a reference, i.e., as a dictionary. Many terms and definitions associated with system safety are included. The glossary can be used for training and

educational purposes. Depending on the need, these terms and definitions can be used when discussing methodology or when conducting presentations. There are terms referenced that are not specifically addressed in the handbook. These additional terms are important, however, as reference material.