ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)
2.2: Safety certification of ATM systems

FAA SAFETY RISK MANAGEMENT IN THE DEVELOPMENT OF NEW SYSTEMS

(Presented by the United States)

SUMMARY

This paper outlines the background and current status of safety risk management (SRM) conducted by the United States Federal Aviation Administration (FAA) for new air traffic control equipment/systems. SRM is based on the same safety risk management principles reflected in the International Civil Aviation Organization (ICAO) Annex 11. The paper describes how SRM is conducted and managed as part of the FAA's Acquisition Management System.

REFERENCES

Annex 11
Doc 4444, PANS-ATM
FAA Order 8040.4, Safety Risk Management, June 1998.
System Safety Management Program, Revision 4, April 2003. FAA, Acquisition Management System, available online at http://fast.faa.gov/toolsets/SafMgmt/index.htm.

1. INTRODUCTION

1.1 The Federal Aviation Administration (FAA) is developing a safety management system (SMS) for the provision of air traffic services in accordance with the requirements in the International Civil Aviation Organization (ICAO) Annex 11 — *Air Traffic Services*. One foundation of the FAA's future SMS is the current acquisition and research (ARA) safety risk management (SRM) process being implemented for the development and acquisition of new air traffic control equipment/systems for use in the U.S. National Airspace System (NAS). The future SMS will extend formal safety risk management into all areas of the

provision of air traffic services, including operations and maintenance. The purpose of this paper is to describe the SRM process currently utilized for new systems.

2. DISCUSSION

2.1 Background

2.1.1 The FAA's NAS Modernization System Safety Working Group (SSWG) was established in 1999. The first priority of the group was to develop a system safety handbook to provide guidance to FAA employees and contractors on how to conduct system safety engineering. The *System Safety Handbook* (SSH) was completed and published in 2000. It can be accessed at http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm.

2.1.2 Once the *System Safety Handbook* was complete, the group developed an operating plan for conducting system safety on new air traffic control equipment/systems in the NAS. The operating plan detailed the what, who, when, and why of SRM. It also describes the standards for conducting safety risk assessments for new systems. In 2001, this operating plan became the *System Safety Management Program* (SSMP) and was incorporated into the FAA's Acquisition Management System (see Figure 1).

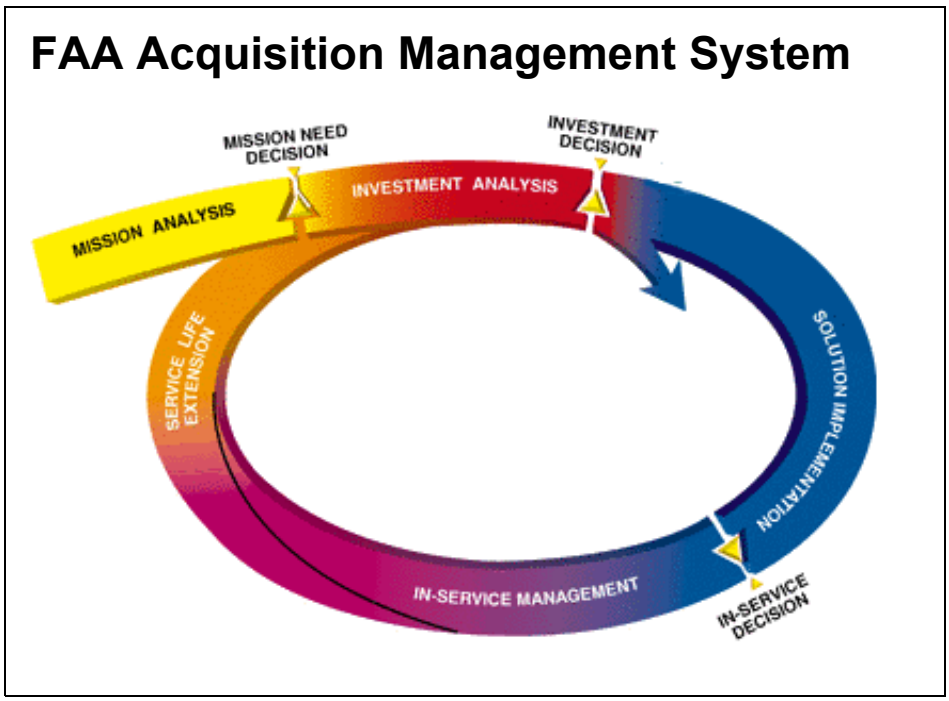

Figure 1

2.1.3 The *System Safety Management Program* is integrated with the FAA's system engineering process as part of the Specialty Engineering discipline. Other segments of specialty engineering include: Quality, Human Factors, Reliability and Maintainability, Electromagnetic Environmental Effects, and Hazardous Materials. All of the elements of system engineering are tightly woven together, with information passing between the engineering elements in an integrated manner. In addition to finding problems, another major benefit of safety risk management is that it identifies problems early in the development process.

Experience has shown that the later a problem is discovered the more it will cost to fix (see Figure 2). Safety risk management identifies problems early when the cost to mitigate is the least.

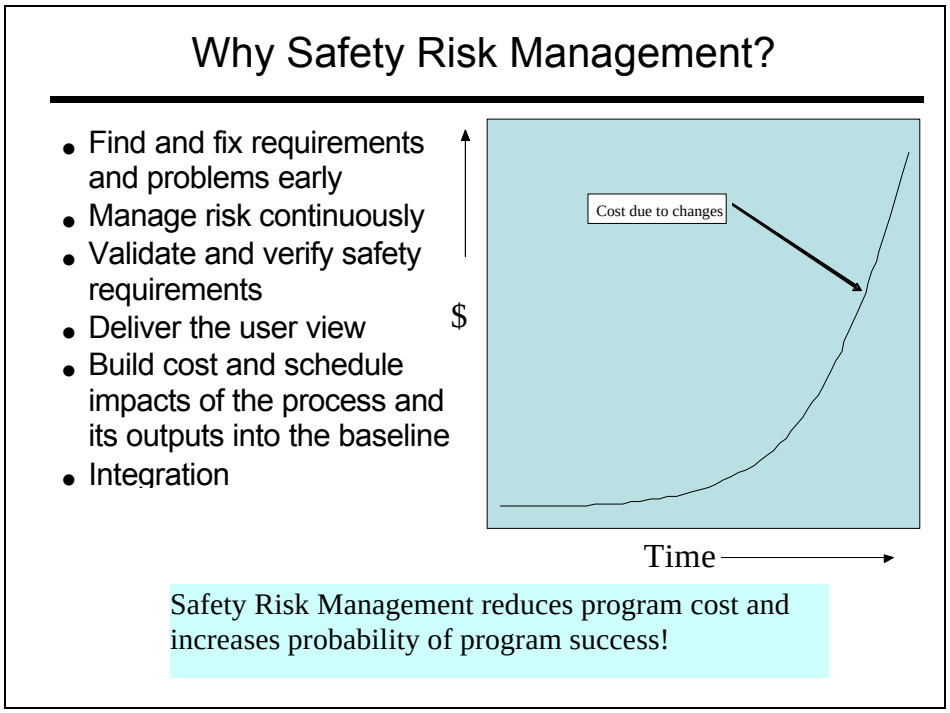

Figure 2

2.2 **Features of the existing SRM**

2.2.1 Safety risk management is the core of the FAA's current and future safety management system. SRM is a disciplined method of describing a system and the changes to the system that are being considered. Once the system is described, hazards are identified and then each hazard is assessed to determine its risk. The risk is plotted on a risk matrix where the hazards are prioritized according to their risk. Strategies are then developed to control each hazard's risk. These controls are written in requirements language and converted into safety requirements. Once validated, each safety requirement is then run through a rigorous verification process. After verification is complete, each hazard is re-evaluated for its residual risk and the process is repeated until all the risk is acceptable (see Figure 3).

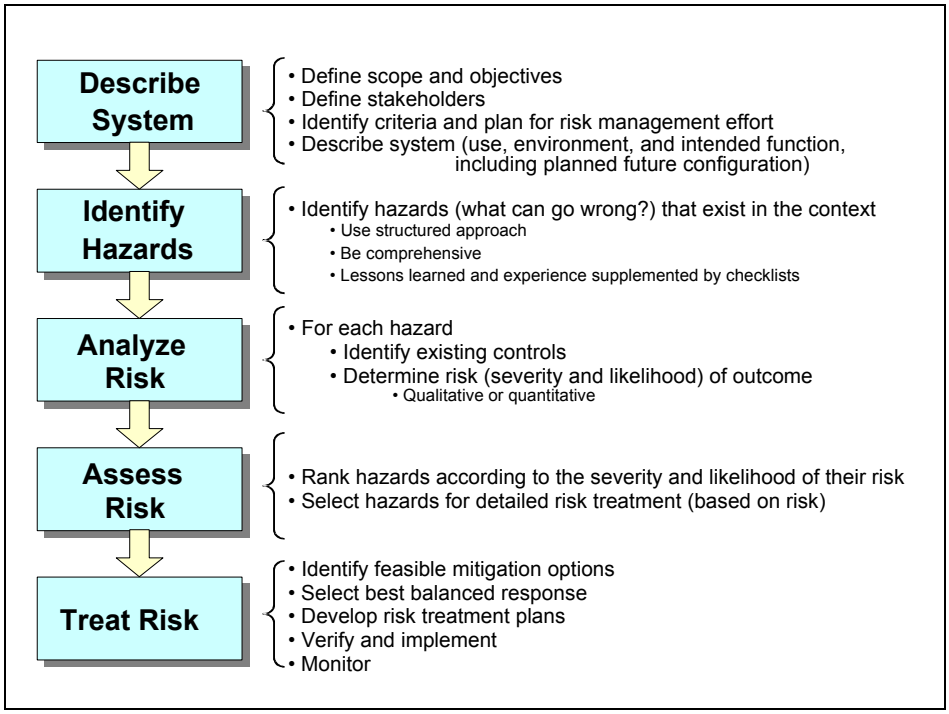

Figure 3

2.2.2 The focus of the safety risk management is to reduce the risk of each hazard and the sum total of all the risk inherent in the system. This is achieved through a closed loop process that focuses resources on the highest risk elements of the system.

2.2.3 Figure 4 depicts the fundamental products of SRM for new system acquisitions.

a) **Operational Safety Assessment (OSA)** looks at the functional hazards in a service or operation and develops safety requirements based on the hazard severity. OSA is completed to support the Mission Need Statement.

b) **Comparative Safety Assessment (CSA)** looks at the preliminary functional hazards involved in a change or decision. Each alternative is then evaluated for its risk. CSA is used to support decisions involving different alternatives or in trade studies.

c) **Preliminary Hazard Analysis (PHA)** is the initial analysis of the proposed top-level system architecture (functional and physical). PHA includes risk assessment of each hazard with controls that are developed to a greater level of detail than the OSA or CSA (usually at the requirement or specification level). PHA supports investment decisions.

d) **Integrated Safety Program (ISP)** is a statement of the required safety products, standards, and organization relationships on the program. ISP is documented in the *Integrated Program Plan* (IPP). ISP supports Investment decisions.

e) **Sub System Hazard Analysis (SSHA)** is a detailed hazard analysis focusing on the anomalous behavior of components of individual subsystems (i.e., flight controls). SSHA will usually include fault or event trees for the higher severity hazards.

f) **System Hazard Analysis (SHA)** is a detailed hazard analysis that focuses on hazards generated by the interaction between elements within a system or interactions between the system and other systems.

g) **Operating and Support Hazard Analysis (O&SHA)** is a detailed hazard analysis focusing on the hazards generated by the operation and maintenance of the system in normal and abnormal environments.

h) **System Safety Assessment Report (SSAR)** summarizes the safety work, findings, and verification of safety requirements.

i) **Hazard Tracking System (HTS)** *Hazard Tracking and Risk Resolution* (HTRR) is a closed-loop method of ensuring that the requirements and mitigations associated with each medium and high-risk hazard are implemented.

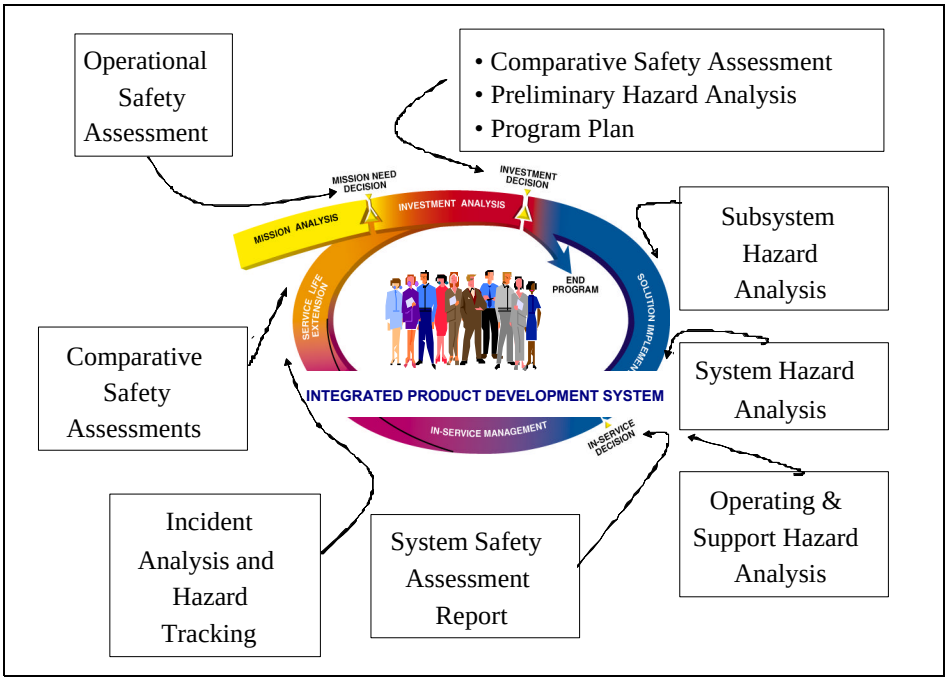

Figure 4

3. THE FUTURE OF THE FAA SMS

3.1 As described in the AN-Conf/11-IP/24 paper, *U.S. Safety Management System Development*, the FAA has started development of an SMS that will extend safety risk management into the provision of air traffic control and navigation services in the NAS. The SMS will address the safety risk management of the following:

a) introduction of safety significant new equipment, systems, or facilities used in the provision of air traffic services;

b) safety significant modifications to critical equipment, systems, or facilities used in the provision of air traffic services;

c) safety significant airspace changes;

d) safety significant changes to air traffic services procedures and standards; and

e) safety significant changes to airport procedures and standards.

3.1.1 The FAA SMS development strategy is to build on existing internal processes and procedures, which have allowed the FAA to establish an unparalleled safety history. In developing the SMS, the FAA will leverage best practices and lessons learned from other ICAO Member States, industry, and government. It is anticipated that implementation of a full SMS within FAA will be done in several phases and will be completed in a similar timeframe as other ICAO Member States. The FAA SMS will address the current U.S. structure of the provision of air traffic control and navigation services, and will adapt with the evolution of the government regulatory structure.

4. CONCLUSION

4.1 As documented in the FAA's *System Safety Handbook, System Safety Management Program* and *Acquisition Management System*, SRM is employed in the acquisition and development of new systems. Safety risk management will be the foundation of the FAA's new SMS that will extend to the provision of all air traffic control and navigation services.

— END —