Safety Management Systems – New Wine, Old Skins

Steven D. Smith, Federal Aviation Administration

Key Words: Safety, Risk, and Safety Culture

SUMMARY & CONCLUSIONS

The Federal Aviation Administration (FAA) has embraced the use of a Safety Management System (SMS) to maintain and improve its National Airspace System. Beginning in the year 2000, the FAA Administrator directed that research into the feasibility of an SMS within the Air Traffic Service be conducted. An FAA team quickly concluded that the SMS was an important step in maintaining our high level of safety. In 2001, the International Civil Aviation Organization (ICAO) mandated the use of SMS in all of its member states. The FAA has aggressively pursued implementation of its version of the SMS since that date.

The FAA implementation is built on a four part interlocked system consisting of Policy, Architecture, Assurance and Safety Promotion.

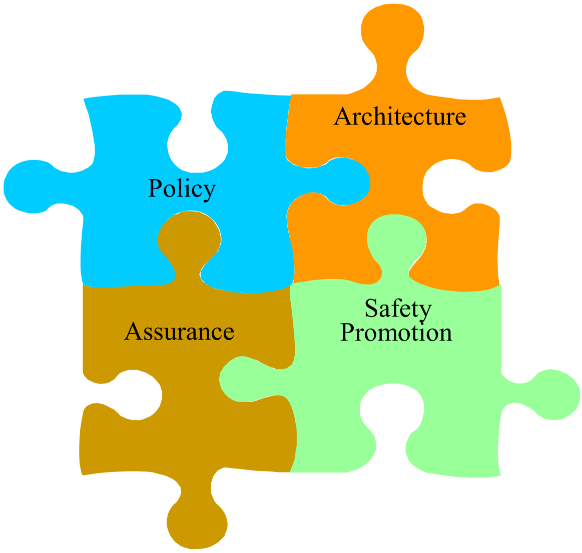
While safety is always a primary concern at the FAA, SMS formalizes the safety risk management policies currently employed at the Administration and introduces a plan to strengthen the safety culture and safety training of its employees.

Changes in the current system, either new introductions of technology or enhancements of current operations, will be subject to a strict safety risk assessment methodology. Risks will be identified, prioritized, and then mitigated. Data will be collected and monitored to ensure the system maintains or improves the level of safety before the change.

The six part safety risk management system coupled with continuous monitoring will strengthen the existing new system development process and bring a formalized process to the operations and maintenance procedures. It will truly bring new wine into old skins.

INTRODUCTION

What is a "Safety Management System" and how does it differ from existing safety programs? A safety management system (SMS) is defined as "…a proactive, integrated collection of processes, procedures, policies and programs used to formally assess, define, and manage safety risk."[1] To be successful, a safety management system must be an integrated collection of Policy, Architecture, Assurance and Safety Promotion. Each of these pieces can be further parsed into subsections: Policy – requirements, responsibilities and secondary quality assurance; Architecture – filters, guidance and documentation; Assurance – data tracking and analysis as well as primary quality assurance; and finally Safety Promotion – training, safety culture and lessons learned. The Federal Aviation Administration has embraced this philosophy within the Air Traffic Organization (ATO) and will use it to maintain and improve one of the safest air traffic management systems in the world.



Components of the Safety Management System

RATIONALE AND MOTIVATION

In the year 2000, The Administrator of the Federal Aviation Administration formed a team to research the possible use of a safety management system within the FAA. The team quickly concluded that the design, development and deployment of an SMS within the FAA were important steps to ensure the high level of safety within the air traffic management system. In 2001, the International Civil Aviation Organization (ICAO) amended Annex 11, Air Traffic Services (ATS), to require its member states to establish an SMS for the provision of air traffic services. Since this date, the FAA has aggressively reviewed previous implementations of SMS's throughout the world and combined the best ideas from each of these models with its own unique perception to form a world class SMS for use within the National Airspace System (NAS).

[1] FAA SMS Manual, Version 1, April 30, 2004

Safety has always been a primary component within the air traffic control and navigation services system whether it related to equipment purchase and/or design, air traffic procedures, or employment and training of its personnel.

The SMS integrates existing FAA operational policies, processes, and procedures, as well as introduces new elements necessary for a systems approach to managing the safety risk within the ATO. The SMS is expected to evolve as a result of lessons learned through the application of safety related tools and concepts, changing technologies, advances in aviation operations, and improved techniques for managing risk.

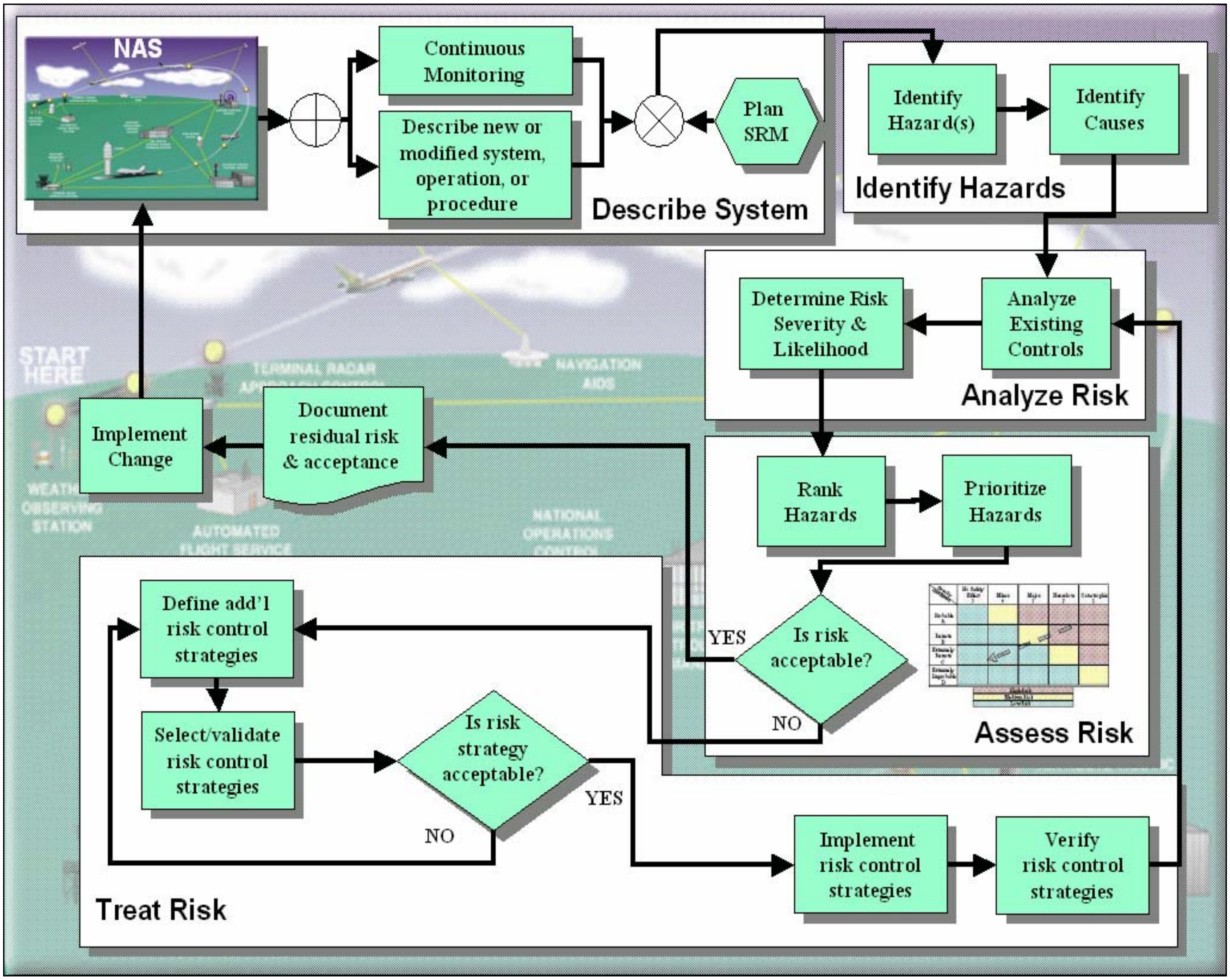
The SMS provides a common framework to assess safety risks to the current and future NAS. It addresses new equipment and changes to equipment (hardware/software), ATC procedures, instrument flight procedures, separation standards, airspace (en route and terminal), airports (ground/taxi), and maintenance activities. In addition, the SMS includes processes to collect and analyze safety data, conduct safety reviews and evaluations to assure safety, and continuously monitor the NAS to assess the safety risk.

So, what exactly is different or unique about SMS and how can it be integrated into the current system?

NEW WINE – OLD SKINS

A Safety Management System is a collection of four main components: Policy, Architecture, Safety Promotion, and Assurance. Managing the "white spaces" or interfaces between these components is one of the primary differences between the previous system and the future ATO. The other primary difference is the integration or sharing of information between and among the four basic components.

Primal to the new system was the policy component. To ensure success, the new SMS was built upon a solid foundation outlined in FAA Order 8040.4, Safety Risk Management.


NAS
Continuous Monitoring
Describe new or modified system, operation, or procedure
Plan SRM
Describe System
Identify Hazard(s)
Identify Causes
Identify Hazards
Determine Risk Severity & Likelihood
Analyze Existing Controls
Analyze Risk
START HERE
Implement Change
Document residual risk & acceptance
Rank Hazards
Prioritize Hazards
YES
Is risk acceptable?
NO
Assess Risk
Define add'l risk control strategies
Select/validate risk control strategies
Is risk strategy acceptable?
YES
NO
Implement risk control strategies
Verify risk control strategies
Treat Risk
TERMINAL RADAR APPROACH CONTROL
NAVIGATION AIDS
WEATHER OBSERVING STATION
AUTOMATED FLIGHT SERVICE
NATIONAL OPERATIONS CONTROL

<u>Safety Risk Management Process</u>

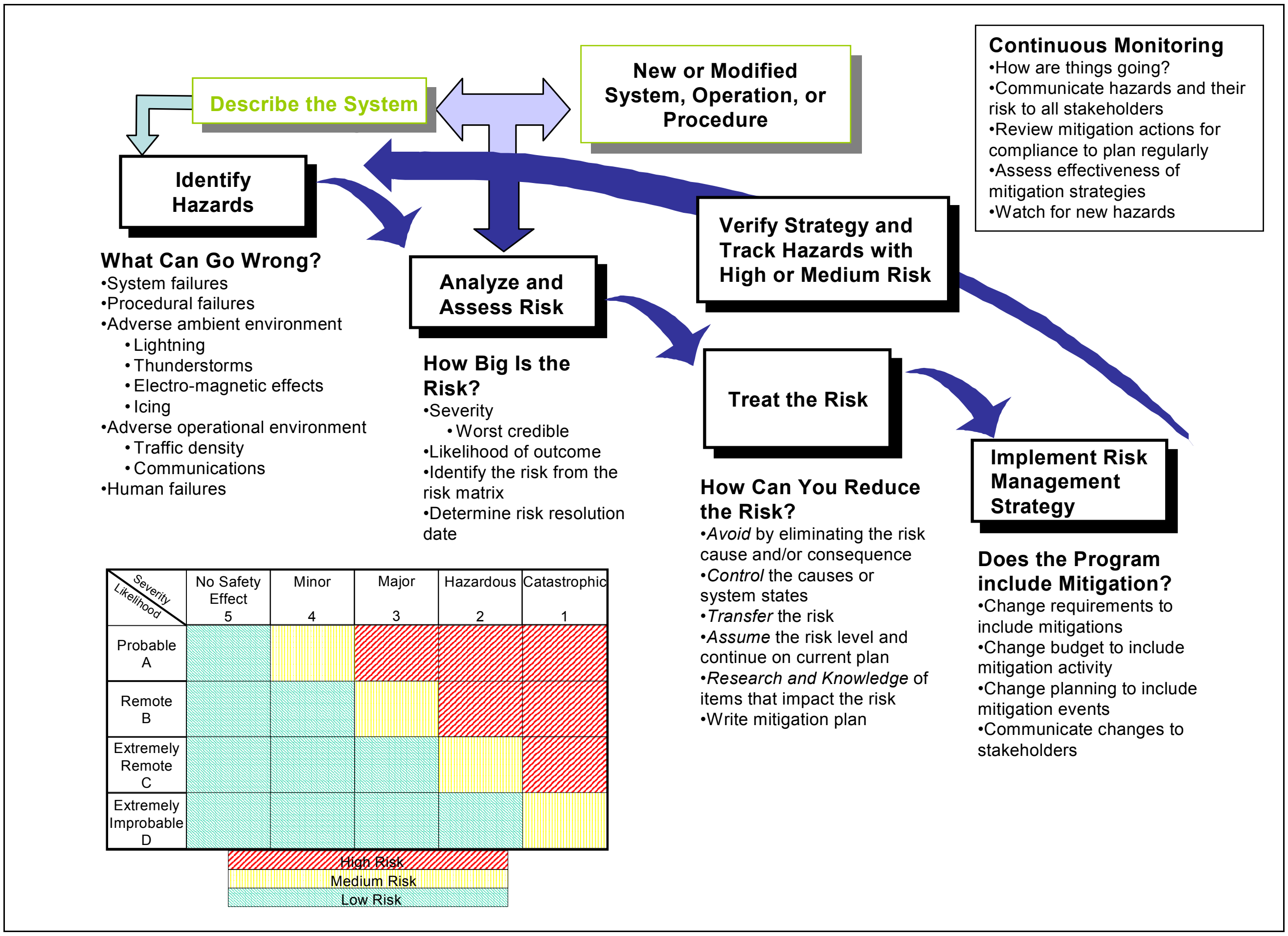
As depicted in the above graphic, the SRM process (contained in FAA Order 8040.4) is a dynamic closed-loop process that seeks constant improvement and reduction of residual risk levels present in the NAS. This lowering, or at least maintaining, of present levels in risks within the NAS as the system experiences changes is the first requirement of an SMS. Within this same puzzle piece are the definitions of who is responsible for actually performing the SRM and who the approving authority is that will ultimately set the level of acceptable risk and approve any identified residual risk within the system being examined.

The second piece of the SMS puzzle is the architecture. The tools and processes used within the SMS were developed based on best practice safety risk management guidance and current risk management guidance within the FAA Office of System Safety, the FAA Office of System Architecture, and the FAA Air Traffic Organization. Additional tools and processes were developed specifically for the SMS that define the basic processes for deciding when to use safety risk management, when and to what depth the safety risk process must be used and finally how to document the results of a safety risk assessment.

The third piece of the puzzle is assurance. This facet focuses on safety data collection and analysis, as well as primary quality assurance, i.e., validation that what is being stated as accomplished has actually been accomplished. It's not just the collection of the same data used in a different way, it requires the identification of new data sources and the substantiation of existing data sources to ensure we are collecting the right data, the right way, for the right purpose.

The fourth and final puzzle piece is safety promotion. This is where existing and future training standards as well as the FAA safety culture are examined and defined. This is probably the most critical initial step to the success of the SMS. Without proper training and understanding, existing personnel and systems will fail to understand the "why" and "how" of the new SMS and "resistance to change" will become an insurmountable obstacle to the success of the program. The new safety culture will reinforce a positive reporting culture that: 1. is simple and easy to use, 2. is encouraged by management, 3. maintains confidentiality of the reporter, 4. provides feedback to the reporter, 5. results in corrective action to prevent reoccurrence, and 6. disseminates lessons learned to all effected parties within the Agency.

This paper will concentrate on the architecture piece, and more specifically the safety risk management process within that piece.


Describe the System
New or Modified System, Operation, or Procedure
Continuous Monitoring
•How are things going?
•Communicate hazards and their risk to all stakeholders
•Review mitigation actions for compliance to plan regularly
•Assess effectiveness of mitigation strategies
•Watch for new hazards
Identify Hazards
What Can Go Wrong?
•System failures
•Procedural failures
•Adverse ambient environment
• Lightning
• Thunderstorms
• Electro-magnetic effects
• Icing
•Adverse operational environment
• Traffic density
• Communications
•Human failures
Analyze and Assess Risk
How Big Is the Risk?
•Severity
• Worst credible
•Likelihood of outcome
•Identify the risk from the risk matrix
•Determine risk resolution date
Verify Strategy and Track Hazards with High or Medium Risk
Treat the Risk
How Can You Reduce the Risk?
•Avoid by eliminating the risk cause and/or consequence
•Control the causes or system states
•Transfer the risk
•Assume the risk level and continue on current plan
•Research and Knowledge of items that impact the risk
•Write mitigation plan
Implement Risk Management Strategy
Does the Program include Mitigation?
•Change requirements to include mitigations
•Change budget to include mitigation activity
•Change planning to include mitigation events
•Communicate changes to stakeholders

Severity / Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A	🟦	🟨	🟥	🟥	🟥
Remote B	🟦	🟦	🟨	🟥	🟥
Extremely Remote C	🟦	🟦	🟦	🟨	🟥
Extremely Improbable D	🟦	🟦	🟦	🟦	🟨

🟥 High Risk
🟨 Medium Risk
🟦 Low Risk

Safety Risk Management Summary

THE SAFETY RISK MANAGEMENT PROCESS

The first step in the safety risk management (SRM) process is the description of the system or entity being examined. It's important that the scope of the SRM be broad enough to encompass interfaces or "white spaces" between systems. This will aid in identifying often overlooked cross-boundary issues. We need to identify the environment in which the system will operate as well. It's also important that the scope not be so broad that the analysis becomes unwieldy and complex. The description should be concise yet specific enough that anyone reviewing the process would understand exactly what was being examined.

The second step is the identification of hazards. A hazard is a condition, event or circumstance which could lead to and unplanned or undesired event. You can simply ask the question: "What can go wrong?" This step identifies such things as system failures, procedural failures, environmental and operational issues, and human failures. This phase also looks at causes for those failures, the "Why does it go wrong" question. We examine common mode failures (a condition where one event or condition can cause multiple failures of more than one function within a system) and we also use "worst credible" state to identify the most unfavorable conditions expected to occur within the operational lifetime of the system or change being examined.

The next step analyzes and assesses the risk. You could ask the question: "How big is the risk?" Here we look at the potential outcome of the hazard in terms of its effect or harm and how often it is expected to occur. We use a risk matrix to determine priority and level of action required. Some risk is unacceptable (those areas in red on our sample matrix) and must be mitigated to medium or low risk before they can be accepted and the new system and/or change to an existing system be placed into operational service.

Next, we must treat the risk. Here we ask the question: "How can you reduce the risk?" We strive to eliminate the risk thru design; however, this is often not possible. Our next priority is to control either the causal factors or the system states in an effort to reduce or mitigate either the severity (how bad) or the likelihood (how often) of the risk. The two remaining options are transfer or assume the risk. Authority to assume risk is dependent on the scope (does it effect others outside the air traffic organization?) and/or risk level. It can range from local approval (by delegation) to ATO Vice President/Associate Administrator Level with concurrence from an organization outside the ATO. A mitigation plan must be written and a strategy to reduce and/or eliminate the risk must be documented.

Implementing the risk management strategy is next. In new systems development, this may be the introduction of new or changed safety requirements into the design. In existing systems, budgets must be modified to allow for proper safety enhancements to be infused into the current design. Any and all changes to the systems must be communicated to all stakeholders (users) of the system. This is where safety changes will take place and must be monitored to ensure the desired effect is being observed.

Lastly, we must verify that the safety risk strategy has been effective and we must track high (initial) and medium hazards to ensure that the desired mitigation and/or controls have the desired results. All High and Medium risks are annotated and tracked during the life of the system and/or change (even if they are reduced to low). Here we ask the question: "How are things going?" "Have we achieved the desired result?"

Continuous monitoring of the system is imperative to continued success of the SRM process. Communication to each of the effected parties of the inherent risk, the mitigation and the residual risk associated with each system examined under SRM will give each of the stakeholders a better understanding of the level of safety associated with that system. With increased knowledge comes the responsibility to report any new and/or unidentified hazards as they arise. This brings full circle the need for a strong safety culture with a viable "non-punitive" safety reporting system.

BIOGRAPHY

Steven D. Smith
Federal Aviation Administration
Air Traffic Safety Oversight Service (AOV-300)
800 Independence Ave., S.W.
Washington, D.C. 20591

e-mail: steven.d.smith@faa.gov

The Federal Aviation Administration, Air Traffic Oversight Service currently employs Steve Smith as a senior aviation technical services specialist. Steve graduated from St. Martins College in Lacey Washington and has attended Graduate courses at the University of Southern California. He has instructed courses in both system safety and risk management for both the United States and Canadian Governments. Steve has practical experience in numerous safety risk assessments concerning aircraft operations, airport movements and aviation regulatory issues. He was a member of team that created the current implementation of the Safety Management System for the FAA. He has co-chaired the FAA system safety working group, the FAA safety risk management working group and was a member of the FAA systems engineering council. He is currently the Director of Government and Intersociety Affairs for the System Safety Society, a member of the Interagency Risk Management Working Group and a board member of the National Aviation Club.