Background and Fundamentals of the Safety Management System (SMS) for Aviation Operations

Prepared by

The SMS Project Team

of

The Air Line Pilots Association, International

Second Edition
February, 2006
# Table of Contents

Introduction 1

Objective
SMS Benefits

Chapter 1 - Background 3

The Eras of Aviation Safety
- The Machine Period
- The Human Period
- The Organizational Period

Westrum’s View of Organizations 4
- The Pathological Organization
- The Bureaucratic Organization
- The Generative Organization

The Reason Model of Accident Origins 6
- Types of Organizational Failure

Traditional Safety Management 8
- Safety Managers

Safety Innovation 9
- The Safety Culture

Chapter 2 - Fundamentals of SMS 10

Origins
- System Safety Steps
- SMS / System Safety Definitions

SMS Arrives
- What SMS Means to the Operator...and the Industry
- The SMS Relationship
- SMS Activities

Chapter 3 - SMS Details 18

Organization
- Culture and Safety Culture
- A Management Framework
  - The Accountable Executive
  - Policy
  - A Plan
Chapter 4 - Risk Management

Risk Assessment
  Problems in Risk Assessment
  Inputs
  Motivation
  Compensating

Managing Risk
  The Risk Assessment Matrix
  Risk Value Judgments
  Risk Acceptance

Hazard Control or Mitigation
  Hazard Controls
  System Safety Order of Precedence
  Verification

Chapter 5 - Hazard Information Systems

Requirements
Resources

Chapter 6 - Conclusion

Top-Down Change
Bottom-Up Change
Safety Case – Business Case

References

Commercial Sources
Regulator Sources
Where to Find SMS Information

Appendix 1 – The SMS Grid

Appendix 2 – The Safety Risk Assessment Process (SRA)
  Overview
  Five Steps to a Safety Risk Assessment

Appendix 3 – Guidelines for Developing a Safety Management System (SMS)

SMS Components
  Organization
  Risk Management
  Hazard Information
Appendix 4 – SMS in Canada
Canadian SMS Requirements
Critique
General
Transport Canada and Enforcement
Problems
Introduction

This text provides an introductory view of the Safety Management System (SMS). SMS is a proactive approach to ensuring the health of air carriers through effective management of the hazards that are a natural part of aviation operations. Plainly stated:

- SMS is an **Operator** based safety approach
- SMS integrates Employee and Management experience and information
- SMS interfaces with the Regulator’s oversight systems

Objective

Our objectives are to explain the background and theory of SMS and to outline the actions an airline would use to develop and implement an effective company SMS program. We will examine Management and Employee roles and actions, and we will provide exposure to Safety Risk Assessment (SRA) methods that lie at the heart of SMS.

SMS Benefits

In aviation safety, one of the biggest challenges is to make positive change at your company to improve safety. In this, you must guard your credibility and objectivity if you’re going to be effective. Armed with proper knowledge and skills, you can make lasting improvements in your company’s safety achievement.

This manual provides a means to assess the safety performance of your airline and effectively bring about change, when and where change is needed. This perspective will also help you work more effectively with government agencies as they begin to introduce the same concepts and methods into their operations.

SMS programs have begun in the United Kingdom and Australia; the Joint Aviation Administration also recommends SMS. Further, in North America, Transport Canada is in the process of a phased application of SMS in all aviation operations through regulatory requirement and the U. S. Federal Aviation Administration is moving toward internal use of SMS.

In this manual we aim to provide knowledge and skills that yield improved risk management decision-making and increase your ability to target resources to those issues having the greatest threat to your company’s operations. Using SMS methods helps you effectively assess risk and develop solutions. SMS moves debates beyond emotional appeals and provides a method of communicating safety issues that will be compelling and convincing to the company’s decision makers.
SMS focuses on the entire organization. It incorporates line management, safety expertise, and employee involvement to produce a “safety culture.” That safety culture is vital to a company’s survival and prosperity. The SMS shift from traditional safety approaches to that of the organization is key to safety achievement.

Early in the 20-century, a famous British jurist observed that,

“Every accident is a failure of organization.”

Here, in the 21st century, that observation still holds true. The Safety Management System provides a way of changing organizations in a positive way. But, it requires the full participation of all the company to make it effective.

Notes:
Chapter 1 - Background

The Eras of Aviation Safety

Change is the mother of twins: Progress and Worry

The Machine Period

The machine period began with the Wright brothers’ first flight. In these early days, safety management was characterized by the phrase, “fly-fix-fly.” As aircraft broke down and builders identified the failure, changes were made to try to prevent a recurrence. Aviation companies were small scale so safety fixes were developed quickly. Significant improvements were made to aircraft engines, airframes and systems. The preventive actions mostly were improvements in design and airworthiness in response to the high incidence of mechanical-based accidents.

The Human Period

The human period flowered in the mid-1970s as safety practitioners began to emphasize the man / machine interface. Following a number of serious accidents, programs such as Crew Resource Management and Pilot Decision Making training were developed. There was emphasis on improved personnel selection and training. Flight deck interaction of crewmembers and of the crew with the aircraft got new emphasis. The human period was a response to the then current perception of 70-80% of mishaps being “human factor” accidents.

The Organizational Period

The organizational period began in the late 1980s and focused our attention on organization and management influences in accident causation. As accidents continued to occur, notwithstanding the attention paid to the individual, safety specialists and accident investigation agencies looked deeper into accident causation. Accident investigators began looking at underlying factors which “set up” accident potential.

Two “models” of organizations and safety implications became most important to safety efforts. The two are:

---

1 The concept of safety eras is from Mr. Mike Doiron, President of the Moncton Flight College in Moncton, New Brunswick, Canada.
2 The greatest safety advance in the last 50 years must be the introduction and perfection of the jet engine. The failure rate of modern engines is such that a major accident as a result of engine failure is an extremely rare event.
3 The Moshansky Inquiry into an Air Ontario F-28 accident at Dryden, Ontario, Canada is considered the most thorough accident investigation, ever. Mr. Justice Virgil Moshansky identified a wide range of related factors, which set the stage for the accident. These factors included actions by the pilots, the company, the regulator and the government.
1. Professor Ron Westrum’s classification of organizational types and their behavior, and
2. Professor James Reason’s model of organizational failure.

The Westrum and Reason models give us practical views of how accidents are generated and prevented and they account for the influence of organizational issues on accident causation in a way that makes sense to managers.

After a basic review of Westrum’s organization types we’ll show how useful the Reason model is for identifying safety hazards and deficiencies. The Reason model is effective because it translates so well to corporate managers and to employees.

Notes:

Westrum’s View of Organizations

Professor Ron Westrum of Eastern Michigan University has identified three basic types of organizations. The three aptly cover the organizations we work in and with in the aviation industry. No matter whether you look at airlines, government bodies or aviation interest groups, the Westrum models fit.

   The Pathological Organization

The pathological organization is best described as dysfunctional. If it functions, it functions in spite of itself. In any event, it is not a good place to work.

In the pathological organization Information is blocked or controlled and is used to promote or punish. The idea that “knowledge is power” probably came from a pathological organization. It this sort of organization, it’s difficult to achieve positive

---

4 “Complex Organizations: Growth, Struggle and Change” by Professor Ron Westrum, (out of print)
change since the motivation is to blame the messenger and crush new ideas. Failure is covered up and those within the organization have developed a culture to shirk responsibility. Additionally, there is no or little employee/employer bridging or bonding. Management, employees, and their agents, are extremely separate.

The Bureaucratic Organization

A bureaucratic organization is one that is run “by the book.” Here the emphasis is on process and well-established information flow channels. Change is top down, and the organization is inflexible. Most regulatory authorities by their nature are bureaucratic. Bureaucratic organizations aren’t all bad, though, as they are functional in a stable environment. However, they are dysfunctional in a dynamic environment. Paperwork and lots of meetings characterize bureaucratic organizations. Unfortunately, for us, aviation is a fairly dynamic environment and that may explain why many of us see the regulator as a bit of a dinosaur at times. It also explains why change is so hard to achieve in or with a bureaucratic organization.

The Generative Organization

The generative organization is a healthy organization. It is flexible. Information flows freely and effectively. The emphasis is on achievement, not process, and the organization responds well to problems. Positive change may come from all levels as the organization actively seeks information and willingly shares responsibility. New ideas are welcomed. There is continuous evaluation of product. Performance and employee/employer bridging is encouraged and rewarded.

As we move further into this text and introduce you to the concepts of SMS, you will see that the objective is to move corporations towards becoming generative.

Notes:
The Reason Model of Accident Origins

Professor Reason’s work can be summed up as the “Swiss cheese” model of accident causation.

![Diagram of the "Swiss Cheese" Model]

Reason identifies five factors which he characterizes as either “elements of production” or “those who participate” in the various elements.

- First are the decision makers - system architects, senior managers;
- Second is line management - specialists who interpret and implement the strategies of the decision makers;
- Thirdly, there are organizational preconditions which impact outcomes (the organization’s “culture” – e.g., skill, knowledge, motivation, alertness of the workforce;
- Fourth, there are productive activities - actual performance of people and machines; and,
- Fifth are the system defenses or safeguards against foreseeable injury, damage and outages.

February, 2006
We can see the slices of “cheese” that really are parts of our organizations and that all are part of enabling an accident or loss. As an accident process begins it must move through each of Reason’s five factors much like moving through filters. Two things stand out when you look at accidents in this way:

1. You can see that each of the five has a role in enabling an accident to occur, but …
2. … you also can see that action in these parts of organization function can block or prevent an accident.

This is a full view of the accident process, but if you think about the bottom or last filter, “Defenses,” you’ll see something important. This is the area that most of our safety actions have been aimed, up until the present. An important distinction to realize is that SMS programs view and act upon the entire process, not just a single part.

Types of Organizational Failure

The Reason model includes two types of “failures” that happen in an organization. Recognizing them is an important part of managing a safety program:

**Active Failures** - errors and violations having an immediate, adverse effect.

**Latent Conditions** – existing or sometimes hidden situations in an organization. These are placed in the system by decisions or actions of those at some distance from the operation. Latent conditions may be compared to medical pathogens, which invade the body and lie dormant until a triggering condition (active failures), such as fatigue or stress, brings on illness or disease.

You could consider the Latent Condition in an organization as a compressed spring and the Active Failure as the trigger, which releases the spring. The important thing to realize about these two failure types is how an organization can get best value for its money when addressing them. SMS is all about saving our companies the expense of losses and making the companies more effective.

Up to the present, aviation safety programs only saw and went after Active Failures. That has meant going after only one thing – commonly viewed as the “cause” of the accident. Most of our safety history has been oriented to investigating accidents and then solving one thing, in one place ------- which keeps repeating at other times and in other places.
The problem of Latent Conditions is critical to organizations’ efficiency and safety record. Latent Conditions, such as policies or common practices, are embedded in an organization’s normal functions and can enable many accidents – not just one. For controlling loss, here’s where the most gain can be made. Safety efforts aimed at Latent Conditions have a broader effect than those aimed at Active Failures.

Notes:

“Traditional” Safety Management

Safety managers – This is the common form for safety programs that you see today. It’s based on the limited view of Machine and Human models (Active Failures) of safety. Its great weakness is that, in effect, it makes the appointed Safety Manager “responsible for safety.” Here, the Safety Manager may be called a Director of Safety, or even a Vice President, but this person still is the one who’s responsible………..and vulnerable.

The Safety Manager usually conducts safety meetings, puts up safety posters, reacts to incident reports, and investigates accidents. A big part of the job seems to be taking his or her lumps from the rest of management, from the employees and from the regulator. Safety is compartmentalized into a relatively isolated branch of management, leaving line management to deal with “real” concerns such as operating the airline.

This approach permanently restricts the scope and activity of safety efforts. So long as safety programs and safety managers are “outside” the normal management flow and function, they are vulnerable to arbitrary reduction in scope, staff, and budget. As this occurs, their effectiveness dwindles and so does the safety margin inherent in the operation.
Safety Innovation

The Safety Culture - An organization’s culture is a set of beliefs, norms, attitudes, roles, social practices and technical practices. In simple terms, a culture is, “The way we do things here!”

The aim of a CEO and his/her managers needs to be establishing a culture within which constructive criticism and safety observations are encouraged and acted upon in a positive way. The term for this is a “Safety Culture.”

A Safety Culture is a set of beliefs, norms, attitudes, roles, social practices and technical practices concerned with minimizing exposure of employees, managers, customers and members of the general public to conditions considered dangerous or hazardous.

What characterizes a Safety Culture? Here are its hallmarks:

An informed culture
- Management and Employees understand “hazards” and “risk”
- The workforce knows and agrees on what Risk is acceptable and what Risk is unacceptable
- The company seeks to learn what lies behind “errors” so they can be prevented, but it does not tolerate “willful violations”

A reporting culture
- Employees and Management are encouraged to voice safety concerns. No one “shoots the messenger”
- When safety concerns are reported they are analyzed and appropriate action is taken

A learning culture
- People are encouraged to develop and apply their own skills and knowledge to enhance organizational safety
- Staff are updated on safety issues by management
- Safety reports are fed back to staff so that everyone learns

A proactive culture
- Employees and management work continuously to identify and overcome hazards

Notes:
Chapter 2 - Fundamentals of SMS

Origins

SMS has grown out of the aerospace discipline called “System Safety.” System Safety originated in the 1960s when spectacular losses made it obvious that the aerospace industry needed an organized approach to loss control (or safety) – an approach that included Man, Machine and Environment. These three are the hallmarks and credo of System Safety.

From that realization grew the organized and integrated view of safety that has been responsible for much success in aerospace activities. Other industries saw the advantages offered by System Safety and likewise adopted its practice.

In System Safety, the idea of “Safety” has a definition:

“Safety in a system may be defined as a quality of a system that allows the system to function under predetermined conditions with an acceptable minimum of accidental loss.”

Roland and Moriarty

In simpler terms, think of System Safety as:

“Organizing to put your hindsight where your foresight should be in the identification and management of risks.”

Jerome F. Lederer

When safety professionals applied System Safety, they did it in steps that were documented and repeatable. Safety efforts before this had lacked this organized approach. One of System Safety’s strengths is that it is a “life cycle” oriented process. System Safety is active throughout the entire life cycle of a “system.” Here, safety analyses and hazard control actions begin during the conceptual phase of a system and continue through the design, production, testing, use and disposal phases until the system is retired.

System Safety Steps

There are clear steps to follow when you use System Safety:

1. Identify Hazards
2. Determine possible consequences of each Hazard
3. Assess Hazards for associated Risk based on severity & probability
4. Review current or planned mitigation or controls for hazards (system defences)
5. Make recommendations for positive change
6. Perform continual, real-time, system evaluation (howgozit)
7. Do loss investigation
8. Monitor, get feedback, evaluate previous assessments
9. Modify the system as “monitoring” shows necessary

This is a commonsense process and includes a lot when you consider the many aspects of “Man, Machine, and Environment.” Note item number seven! Up until recent times, loss or accident investigations were the foundation of safety programs and often were the entire safety program. In System Safety, investigations were put in proper perspective and used in a productive manner. In System Safety and SMS, investigations are not done purely for the sake of doing investigations.

**SMS / System Safety Definitions**

There are some specific safety terms that we use in SMS and System Safety. They are concepts with fairly simple definitions, and they’re important to know:

- **Accident** – Any unplanned event or series of events that results in death, injury, or illness to personnel or damage to or loss of equipment or property, or damage to the environment, i.e., mishap.

- **System** - A group of interacting, interrelated, or interdependent elements working together within a given environment to achieve a given purpose within a given time period.

- **Hazard** - An event, condition or circumstance, which can lead to a loss when combined with certain conditions in the environment.

- **Risk** - The consequence of a hazard, measured in terms of probability (frequency) and severity. How often does it happen? How bad can it be?

- **System Deficiency** - The circumstances which permit hazards of a like nature to exist within a system.

- **Mitigation** (System Defenses) – A technique, device or method taken, or proposed, to control the hazard or to reduce the probability or the severity of its associated risk. Mitigations often are also called “Hazard Controls” or “Countermeasures.”

**Notes:**
**SMS Arrives**

In the 1990s safety professionals and managers evolved their views based on System Safety and on new corporate management oriented safety models such as Reason’s. While System Safety processes are perfect for the life cycles of aircraft, ships, and buildings and such, they have limits when applied to the operators of the systems.

For an airline, we’d like to think that there’s no “life cycle” involved. We want our airlines to be ongoing, which means healthy and profitable. Safety is an important part of ensuring that airlines do “go on.” To this end, the effective techniques of System Safety required adaptation to meet the needs of operators, our airlines.

The result is the Safety Management System (**SMS**). SMS focuses corporate management activity on loss control as part of the normal line management functions in running a company. In a sense, corporate SMS programs can be called “organic.” They are part of the corporate fabric instead of a vulnerable “extra” tacked onto the corporate structure and functions.

**What SMS Means to the Operator… and the Industry**

In SMS, the idea of Safety is expanded to include and integrate several ideas:

- **Safety** – managing risk to agreed and acceptable levels
- **Management** - allocation of resources
- **System** - interacting, interrelated, or interdependent elements forming, or regarded as forming, a collective unity

You can see that SMS strongly emphasizes the idea of management. Management is, in turn, something that Operators are highly conscious of. In using SMS, Operators develop, use and update:

- **Safety Strategies** – aimed at compliance with safety rules and at prevention/reduction of harm arising from decisions/operations
- **Business Strategies** – aimed at creating and fostering shareholder value
- **A Management Framework** - aimed at enhancing organizational performance through integrating line and safety management.

For Operators, one of the most attractive parts of SMS is that each Operator “owns” its own SMS program. While each program will have basic similarities, each will be tailored to meet the specific environment and needs of its “owner.”
The SMS Relationship

For airlines, SMS programs are a three-way relationship of the Operator, Employees, and the Regulator. Each of the three has actions to perform, and those actions relate to similar actions between the other two. Consider this something like a three-legged stool. It works well with all three legs, but is unstable with two and worthless with only one.

Figure 2 – The Relationship of SMS “ Actors”

SMS Activities

SMS programs require three sorts or types of activity. These form the basic framework within which the three SMS “actors,” Operator/Employee/Regulator, work. SMS activities fall into one of the three types of action:

1. Organization – actions that set up the program and guide its administration. This would include policies and procedures, and, most importantly, a specific person accountable for the safety of the operation. This is the “accountable executive” and is the person who sets the goals and direction for the company, the person who directs where and how the money is spent, the person in charge.
2. Risk Management – these actions include detecting, analyzing and acting to mitigate or control hazards. In aviation, Risk Management actions are common because this is the classification of most “traditional” safety actions, on a piecemeal instead of coordinated basis.

3. Information – No safety system can be effective without good information. You need it to manage risk. You need it to detect new problems. You need it to verify your “fixes” are working. While you may need to develop new types of information, you’ll find that a lot already exists and is merely waiting to be coordinated and viewed by the right people.

The table, below, shows the high level view of how SMS is organized.

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>SMS Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
<td>• A designated “accountable executive”</td>
</tr>
<tr>
<td></td>
<td>• A documented program, policies and procedures</td>
</tr>
<tr>
<td></td>
<td>• Employee inclusion</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>• Hazard detection and analysis systems</td>
</tr>
<tr>
<td></td>
<td>• Hazard control systems and practices</td>
</tr>
<tr>
<td></td>
<td>• Management/Employee inclusion and involvement</td>
</tr>
<tr>
<td><strong>Information on hazards and controls</strong></td>
<td>• Means of gathering safety related information</td>
</tr>
<tr>
<td></td>
<td>• Detect new hazards</td>
</tr>
<tr>
<td></td>
<td>• Verify that hazard controls are working</td>
</tr>
<tr>
<td></td>
<td>• Employee input of safety information via non-punitive reporting systems.</td>
</tr>
</tbody>
</table>

Figure 3 – The Overall SMS Framework

You also can view SMS activity as a pyramid. Here, clearly, the quality of everything depends on the foundation of good safety information. It’s also just as clear that everything in SMS flows downward from the way the program is organized.
These are the three activities that the three actor groups carry out, but they are done in relation to each other – *not in isolation*. The table, below, shows a basic grid style view of the complete relationship:

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>SMS Actor Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operator (airline, airport, etc.)</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>ORG</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>RM</td>
</tr>
<tr>
<td><strong>Information system on Hazards</strong></td>
<td>INFO</td>
</tr>
</tbody>
</table>

This Grid orients you to the types of activities in SMS and the three-way relationship of the program. Appendix 1 provides an expanded view of the Grid that is more specific concerning what activities each Actor performs in relation to and cooperation with the others. The main point of this “basic” Grid is that each actor in an SMS...
program has actions and responsibilities in each type of Activity – these all knit together and support each other.

The SMS program on the airline’s property includes both SMS activity by the Airline/Operator and by the Employees. Operator and Employees each have actions in Organization, Risk Management and Information activities.

The focus of this Manual is that of the Operator or airline, so we need to take a closer look at the part of the Grid that applies. Like zooming in from a large chart to a smaller one, we see more detail, but still not as much as in Appendix 1. In the view, below, the emphasis is that the Employer and the Employees each have activities to perform that mate with those of the other. However, there are essential differences, especially at the Organizational level of the program. We will discuss these in more detail, later.

At this point the concept to grasp is that Employer and Employee are linked by formal involvement. Success of the airline depends on both working together. Few things are more frustrating to observe than a boat with two rowers, each pulling in opposite directions. At the best, that describes a static and non-productive relationship going nowhere and achieving nothing. If you place the boat and the rowers in the context of a river moving toward a waterfall, then you see “counter productivity” taken to the ultimate level…self-destruction.

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Operator SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operator (airline, etc.)</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>• “Accountable Executive”&lt;br&gt;• Policies/ Procedures</td>
</tr>
<tr>
<td><strong>Risk Management Activities</strong></td>
<td>• Hazard Detection&lt;br&gt;• Risk Management</td>
</tr>
<tr>
<td><strong>Hazard Information Systems</strong></td>
<td>• Hazard Control/Detection systems&lt;br&gt;• Non-punitive reporting system</td>
</tr>
</tbody>
</table>

Figure 6 – The Basics of SMS at an Airline
The Operator’s SMS program is self-contained, but it mates with the SMS activities of the Regulator. Viewed from the other side, the Regulator must be able to react positively and supportively with the SMS activities of the Operator. The Regulator, in SMS, interacts with the self-contained Operator’s SMS program.

The Regulator’s Role

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Regulator (FAA, TC, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>• Internal SMS</td>
</tr>
<tr>
<td></td>
<td>• Operator oversight (ATOS)</td>
</tr>
<tr>
<td>Risk Management Activities</td>
<td>• Hazard Detection, Control, Tracking programs</td>
</tr>
<tr>
<td>Hazard Information Systems</td>
<td>• Safety info: FOQA, ASAP, ASRS, SDR, etc.</td>
</tr>
<tr>
<td></td>
<td>• Non-punitive safety reporting</td>
</tr>
</tbody>
</table>

Figure 7 – The Regulator’s Roles in SMS

Notes:
Chapter 3 - SMS Details

Now that we have the “big picture” of SMS in mind, it's time to get into some of the details of SMS Activities. We'll look, first, at Organization, then Risk Management, and finally at Information.

Organization

The SMS program belongs to the Operator, so it involves action by the Chief Executive or Operating Officer to make SMS take place. This is the Accountable Executive – the person at the top who has the final say and who is responsible for the success of the business. The Accountable Executive is the person that the public and the Regulator see as “in charge.” If the airline does well, the Accountable Executive gets the credit. If the airline flounders, the Accountable Executive gets the “credit” for this, too.

For the Accountable Executive, SMS is the “loss control” part of the Business Plan. To make SMS work, the Accountable Executive develops and publishes policies and procedures that incorporate SMS into the normal management of the company. When safety efforts flow from the “top,” they are an integral part of corporate planning and decision-making at all levels.

Culture and Safety Culture

Each organization or corporation has its own, unique culture. In simple terms, this culture is what the people in the organization do and how they do it. It is the common body of perceptions and modes of action that characterize one organization vs. another.

A common mistake among organization managers is their perception of safety in an operating organization. Commonly they believe that they can force their organization to be an “operational culture” where everything is oriented to the mechanics of operating the airline. Also, commonly, managers perceive that safety is the opposite of the operational orientation. In other words, the perception in some organizations is that “being safe” takes away from the operational reality of airline operations.

This misses the point. The goal is not merely to be safe. The goal is for an organization to operate safely. This requires that the airline foster a “safety culture.” If the airline doesn't operate safely, it incurs losses of people, equipment, money, and reputation. These losses drag an organization down and can even bring it to an end. Factors such as personnel and passenger casualties, equipment damage and loss, and financial outlays for unplanned repairs all have dollar values. Even the spin-masters of the Marketing department probably would admit that their
airline’s reputation could have a dollar value put on it in terms of lost business. Losses of any sort are costly.

An airline using SMS aims at involving the entire resources of the company in loss control. Here the idea is to be proactive in avoiding or minimizing losses to the company. It requires:

- An awareness of the ways that the company is confronted with potential losses.
- A willingness to coordinate all the company’s resources in avoiding losses.
- Tying management and employees together in the loss control process. With this slant, the company increases its efficiency.

A company that takes this approach has a “safety culture.” This is the company that recognizes Hazards and assesses Risk associated with each Hazard. This sort of company goes on from the Assessment stage to managing the Risk. You can see that this works best when the airline ties all its resources together:

- Organization - management and employees all are proactive on detecting hazards and organizing the response.
- Risk Management – all the parts of the company combine information to accurately assess Risk and develop realistic controls or mitigations for the hazards. At the best this eliminates “silos” common in corporations; at the least it opens up means of “cross-silo” communication.
- Information - Existing and new sources of information are applied to the problem of detecting hazards, verifying hazard controls are in place and confirming how effective hazard controls turn out to be.

**A Management Framework**

A great deal of SMS depends on management from the top. It requires Policies and Procedures. It requires Planning. Fortunately, these all are normal functions of management.

While a newly organizing company has to create everything from “scratch,” existing companies already have management structure and practices. For the existing company this is both an advantage and a disadvantage. It permits an existing company to pull together existing practices and resources into an SMS system. It also saddles a company with existing misperceptions and dysfunctions.

For the new or old corporation, the first parts of setting up SMS are the same:

**Designate the Accountable Executive** - The SMS program flows from the direction of the Accountable Executive, so the company must first decide what officer is the Accountable Executive. This selection and designation is something that must be
practical in terms of the flow of policy in the company. Designating the Accountable Executive also must agree with the Regulator’s practical understanding of what makes the company tick. There is no advantage to selecting a “figurehead.” Since an Accountable Executive is concerned about revenue, asset utilization, productivity, and company financial health, SMS needs to originate from that same person.

**Establish Policy** – A company must have a policy setting out the goal of the SMS program and directing that it be implemented throughout the company. The policy needs to establish the idea that safety achievement must be planned and measured. The management structure will be responsible for safety achievement and accountable for it, too. The policy motivates and involves all company management and employees. The Policy is a statement of organizational and individual responsibility

To implement effective SMS you must define:

1. The organization’s safety objectives,
2. What form SMS will take and
3. Who has what responsibility?

The policy makes it clear that the company will be *proactive* in safety, not *reactive*, e.g.:

<table>
<thead>
<tr>
<th>Proactive</th>
<th>Reactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Safety reporting can be proactive</td>
<td>• Accident investigations are reactive</td>
</tr>
<tr>
<td>• System surveys are proactive</td>
<td>• Incident investigations are reactive</td>
</tr>
<tr>
<td>• Risk assessments of <em>proposed</em> operations are proactive</td>
<td>• Error management is reactive</td>
</tr>
<tr>
<td>• Risk assessments of <em>current</em> operations (not triggered by an incident or concern) are proactive</td>
<td>• Deviation analysis is reactive</td>
</tr>
</tbody>
</table>

**Figure 8** – Proactive and Reactive organization actions

**Establish a Plan** – SMS does not happen overnight. The company needs a plan for moving from the current mode of operation to SMS. The Plan must reflect the time required to change current practice and to develop new company practices and procedures where and when needed. While a small company operating a few aircraft in a limited geographic area probably could move into SMS in only a few months, a large airline with many aircraft operating in a variety of environments could need a few years to complete the changeover. Appendix 2 outlines one possible approach to organizing SMS at an airline.
The time period involved in establishing the Plan depends on two important things:

1. The “push” applied by the Accountable Executive and
2. How many of the elements of SMS already exist in the company.

The company’s SMS Plan, like any other company plan, will require Goals, Milestones and defined Steps to mark out the way. Here, the various parts of the company need to be realistic in determining what needs to be done and how quickly it can be done, in coordination with the rest of the company.

Plan for whatever specialized training might be required, however, recognize that the need for such training is limited. SMS takes advantage of existing management and employee expertise, so general training is not needed. The personnel who are doing the overall planning and coordination may need training, but not the general group. As the SMS program develops, training needs may become apparent, but plan to accomplish these as normal training would be accomplished. Plan to “grow” the SMS program, not “mint” it.

**Organize Procedures and Practices** – Procedures and practices of a company are both the road to follow and the drumbeat that the company marches to. In setting up procedures and practices, SMS designers need to:

- Define roles, resources, responsibilities, “top down” accountabilities with a reporting structure, and cross silo coordination. Define who makes up safety committees and what they are to accomplish.

- Seek compatibility and integration with other management systems to avoid “reinventing the wheel.” This goes to the issue of credibility for the designers of an SMS program. Incorporate as much of what exists as is possible to allay the natural suspicion of “empire building” that arises.

**Set Up Controls** - An airline needs Controls as part of its SMS program. This means that when safety results are assessed, there are standard means for initiating corrective action when needed. Off-target safety performance needs to be recognized and dealt with in the management structure. Internal audits and inspections are a valuable means of getting at safety achievement and shortfalls. In all cases it’s preferable that companies find and fix their own problems before outside parties get involved.

**Define the Role of the Safety Manager** – While the title may vary, the airline will need a designated person and staff to advise the "accountable executive" on safety issues and problems. The safety manager aids the "accountable executive" by
monitoring SMS processes. The safety officer aids company managers by providing expertise in loss prevention methodology and techniques.

In defining the Safety Manager’s job, SMS designers must keep in mind that the Safety Manager and/or the Safety Department do not implement the SMS program. The airline’s management implements SMS. The Safety Department may gather and analyze hazard and risk information, but developing and implementing hazard mitigations is a line management function.

One of the most important services a Safety Department can provide is that of the “feedback loop.” An essential part of SMS and System Safety is the information loop that looks at how well hazard mitigations work. It’s not realistic for managers to command fixes and assume that they do what was intended. Good ideas may not work. Situations may change. Fixes may be misapplied. Etc. For whatever reason, it is normal that companies adjust the ways it reacts to hazards. Making good adjustments requires information that accurately reflects the way the company operates.

Define the Role of the Employee – One of the innovations of SMS is that employees are actively and continuously involved in company safety achievement. Depending on your experience and bias, it may seem natural to involve employees or it may seem highly irregular. The important thing to realize is that employees have the best knowledge of what’s going on in the field. They are the part of the company “where the rubber meets the road.” Understanding that is part of establishing and maintaining a “safety culture.”

With that in mind, SMS Policy and Procedures need to aim at the following:

- Employees need to know and understand the requirements of SMS, particularly, to access non-punitive safety information and reporting provisions
- Employees are knowledgeable in operations and a good source of reports on operating deviations
- Employee involvement depends on feedback and an explanation for action or inaction when an employee reports safety information
- Key employees will need SMS training
- A company needs to develop and implement employee/employer agreements to support SMS and ensure protections are in place. It’s not realistic to expect employee involvement if there’s no protection from company and regulator when they provide a report. Reports are “data points.” The company needs data to keep its operation efficient.

A company needs to be able to distinguish between employee actions that are part of the normal job process and employee actions that purposefully bring about harm. Purposeful harmful acts merit direct action regarding the employee. This is very different from an employee making a safety report that involves normal actions and
brings hazards to the attention of the company. In the first case, safety is not the issue so much as a willful act that needs to be dealt with. In the second case, the act of safety reporting needs to be encouraged by impunity from company or regulator disciplinary actions.

Notes:
Chapter 4 - Risk Management

“We do not know how to predict what will happen in a given circumstance. The only thing that can be predicted is the probability of different events. We can only predict the odds.”

Richard P. Feynman
Nobel Laureate - Physics

Definition: Risk Management is the process where management decisions are made concerning control and minimization of hazards and acceptance of residual risks.

If one wants to “manage” risk, one needs to recognize that “management” entails the idea that some level of risk is acceptable. To follow up that idea, “safety” means drawing a line between the acceptable and the unacceptable – then working to make that distinction work in the real world.

Airlines, Employees and Regulators all proceed with different concepts of Risk, based on the perceptions of their people, their experience, public pressure and any number of other “environmental” factors. If differing Risk strategies and views exist, then there are inevitable disagreements, any of which drag the operating process down. If the three Actors can come to agreement on the ideas of Risk, then the operating process can go smoothly and efficiently.

Risk Assessment

Risk needs to be used as a term attached to a specific hazard...and hazards can become known in many ways. We can learn of hazards from accidents, we can learn of hazards from peoples’ innate ability to forecast or infer, and we can learn of hazards from collecting information from the operating environment. Appendix 3 expands the approach to Risk Assessment used in the Safety Risk Assessment (SRA) process.

In an SMS program, when we have a specific hazard to work with, then we need to assess or analyze it before we run off in some direction meant to “fix” the problem. A lot of traditional safety activity, over the years, has been devoted to promoting “fixes” in search of hazards. That’s a poor investment of energy, time and money.

In SMS, the Operator and Employees cooperate in hazard detection and then in Risk Management. Together, they assess the risk that goes with a hazard and agree on the acceptable level of risk. Assessing each hazard for Probability and for Severity does this. In other words, the Employer and Employees pull together quantitative and qualitative information to figure out “How bad could it be?” and “How likely is it to Happen?”
Quantitative information makes the Assessment easier to do and to defend, but often there isn’t enough such information. In that case we must fall back on experience and expert opinion – Qualitative information. Certainly, that makes the Assessment harder to arrive at, but it still is valid if arrived at by discussion between informed Assessors. When a Risk Assessment rests on the opinion of one “expert” or a single instance, it is not as valid as when arrived at by consideration of a group of experts with experience in the matter.

Problems in Risk Assessment

When a company starts a Risk Assessment process it needs to understand where the problems in the process lie. That understanding will lead to a better “product” for the airline – useful insights regarding a hazard.

Inputs

Information deficiency – one of the obvious problems in Risk Assessment is lack of information. Hazard data can be scarce, and sometimes the first step in assessing the probability and severity of a hazard may be to do concentrated research to fill a void in information.

Measurement error – obvious, but possible, is making errors in measuring probability and severity of a hazard. As in anything else, be careful, and use correct measurements.

Uncertainty – Several types of uncertainty plague risk assessments.

- Uncertainty in cause and effect – this is offset by bringing in expertise of knowledgeable persons
- Uncertainty in human and management factors – often risk is viewed from the context of hardware. Human factors are a less clear quality to analyze
- Uncertainty in predicting the future – again, expert opinion is valuable, as assessors need to have a valid perspective on the way things will be.

These uncertainties aren’t abnormal. In fact, they’re typical of any management activity involving assessment. They can’t be eliminated, but they can be accounted for to the best ability of the assessing group.

Motivations

The motivation and driving force behind risk assessment can contain pitfalls for a company. At a minimum, Risk Assessors need to follow an organized, “systems” approach that is well thought out – not “quick and dirty.”
To go further, the process has to be based on correct assumptions where they are required. One can assume normal wear and tear that degrades equipment, but is that assumption valid if the equipment is operating in a high, hot and sandy desert climate?

One of the most basic Motivation problems that can face Risk Assessors is that of resources. It is too easy to base a risk assessment on the resources available (or perceived to be available) rather than on the risk associated with a given hazard. This could be summarized by the expression, “No matter what the question is, the answer is………”

Compensating

In Risk Assessment, it’s important to offset the problems in the assessment that we’ve described. In most cases, the best things to do are clearly document the risk assessment process and then explain where the uncertainties lie. This includes describing the thought process behind Risk Conclusions. If you have only one “data point” then it’s valid to explain how the Risk was inferred from that minimal data set. It is not valid to demand actions, in dramatic prose, and not “mention” that the actions are based on inference rather than analysis. You’ll only get just so far by declaring that “the sky is falling.” That’s no way to gain and maintain credibility with managers or employees.

Managing Risk

Once the Risk of a Hazard has been understood to the best degree possible, then it’s time to figure out what that means. That in turn leads to conclusions on what to do about the risk.

The Risk Assessment Matrix is a basic tool for Risk Management. The matrix ties hazards to the risk qualities of Severity and Probability. The matrix can be in as much detail as is useful, and doesn’t need to offer more detail than is realistic. Where lots of data exists, there may be five or six levels of probability and severity that could be looked at. With scanty data, or in qualitative analysis, it may be more appropriate to use a less complex matrix on the order of “small, medium, and large.” Don’t lock into a 5x5 matrix or a 2x2 matrix. Set up a matrix according to need and information available.

The Risk Assessment Matrix

Following are two example Risk matrices. One commonly is seen in Canada and the other in the U. S. One ranks left to right; the other ranks right to left. The format does not matter, since they both display the same information. Again, use the format that’s useful to you and to the people who will be reviewing it.
Example Risk Assessment Matrix No. 1:

![Risk Assessment Matrix](image)

Typically, we describe Severity and Probability measurements in “most to least” terms such as:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Probability/Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 – Catastrophic</td>
<td>5 - Certain / Imminent</td>
</tr>
<tr>
<td>4 – Severe</td>
<td>4 - Probable</td>
</tr>
<tr>
<td>3 – Major</td>
<td>3 - Likely</td>
</tr>
<tr>
<td>2 – Minor</td>
<td>2 - Occasional</td>
</tr>
<tr>
<td>1 – Negligible</td>
<td>1 - Remote / Unlikely</td>
</tr>
</tbody>
</table>

With Severity and Probability assessed, the range of response typically is as follows:

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Unacceptable</td>
</tr>
<tr>
<td>Magenta</td>
<td>Undesirable</td>
</tr>
<tr>
<td>Yellow</td>
<td>Acceptable – with action</td>
</tr>
<tr>
<td>Dark Green</td>
<td>Acceptable with monitoring</td>
</tr>
<tr>
<td>Light Green</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>
One of the tasks of a Risk Assessment exercise is to arrive at a common scale for each of these qualities of Risk. In some cases, numeric values can be set, but often the descriptions will be purely verbal. Agreement must exist on the definitions of the scale.

Example Risk Assessment Matrix No. 2:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Frequent</td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td></td>
</tr>
</tbody>
</table>

Figure 10 – “Four by Five” Risk Assessment Matrix

Severity is viewed in four grades, which users can define by dollars, damage or any other useful concept.

Likelihood is broken down into five groups. While these can be qualitative judgments, some users assign numeric values to the Likelihood / Severity scale. An example of this is:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>1.0</td>
</tr>
<tr>
<td>Probable</td>
<td>(10^{-3}) (one in a thousand)</td>
</tr>
<tr>
<td>Occasional</td>
<td>(10^{-5}) (one in 100,000)</td>
</tr>
<tr>
<td>Remote</td>
<td>(10^{-7}) (one in 10,000,000)</td>
</tr>
<tr>
<td>Improbable</td>
<td>(10^{-9}) (one in 1,000,000,000)</td>
</tr>
</tbody>
</table>

In this example, the ranking of Assessed Risk is fourfold:

- High: Red
- Serious: Yellow
- Medium: Blue
- Low: Green

In either version of the Risk Assessment Matrix, you see the same ranking and rating idea adapted to the needs of the organization that uses it. The theory and use are the same – only the display is different.

It’s relatively easy to determine that a hazard that is both Catastrophic and Imminent is something that deserves action. Likewise a hazard gauged as Negligible and Unlikely will go to the bottom of the list for action. Such a hazard may even be discarded for further consideration – with appropriate documentation of the decision. However, there’s a broad area of risk assessment between the two extremes that is
the area of value judgment and decisions regarding risk acceptance. Risk Assessment matrices are a tool in deciding what deserves action. They’re a means of relating the risk of one hazard to that of another.

As a practical matter, when a Risk Assessment team identifies hazard control actions that are easy and inexpensive, these actions should be done without a lot of debate. Always do the easy stuff quickly, while you’re still debating the more complicated stuff.

**Risk Value Judgments**

At some stage, organizational values and subjective judgments enter the decision-making process and you have to consider:

- The importance of the estimated risk
- Associated social, environmental and economic considerations
- The potential cost of acting vs. not acting

Part of these judgments is having a good knowledge of your environment. Certainly you need to view Risk in terms of the physical environment, but you also need to have an accurate view of other situations in which the organization functions. For instance, what are the policies, practices and prejudices of the Regulator that apply to the hazard you’re looking at? What parts of the organization will have to be involved in hazard mitigation? What public perceptions bear on the hazard and associated risk? Sometimes, matters such as these alter the purely objective view of a Risk Management group.

**Risk Acceptance**

A risk assessment team develops and documents an understanding of a hazard and its risk. From that understanding, the team needs to go on to developing mitigations for the hazard, and from that the team heads into the touchiest part of Risk Management – the level of risk acceptance that will bear on the hazard.

Of course we want to eliminate all risks and their hazards, but experience teaches us that complete mitigation or control is not feasible or realistic. That means that there always will be some level of acceptance that applies to risk.

This is the point when technical experts bring decision makers into the effort. Sometimes decision makers are left out or they choose not to participate until the time comes to make a decision. However, it’s always better that decision makers participate in the Risk Assessment process so that they have a good basis of knowledge.

This is why it’s so important for the Risk Assessment group to thoroughly document its research and conclusions. All of this needs to be explained to the decision
makers. Sometimes Risk Assessment conclusions must be explained to the regulator, and sometimes even explained to the public.

For the Decision Maker(s) there are two questions that bear on their Risk Management:

1. What risk will I accept?
2. What risk will those I represent accept?

They aren’t easily answered questions and they shouldn’t be. This is not “shoot from the hip” decision making. This is decision making based on the Risk Assessment that’s been furnished and based on the decision maker’s knowledge of the organization’s environment. It’s possible that the decision maker may send the Assessment Team back to do more work. Decision makers get to do that. However, this may not be a good idea if the hazard is rated as Imminent and Catastrophic. The Risk Assessment group needs to clearly describe the importance of its recommendations.

Once the decision on Risk Acceptance and actions is made then Documentation needs to take place. Documentation serves two important purposes for the company:

1. Documentation lays out the rationale for Risk Acceptance based on Risk Acceptance. This is the material that Decision Makers will need for reference when questions arise.
2. Documentation preserves the Risk Assessment and Acceptance work for those that come along later. It can spare later Assessors from having to start from a zero knowledge point, and it shows what the situation was at the time of the original work.

Notes:
One operator responded its Decision Making problems by developing the structured approach shown in the table, below:

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Follow Up</th>
<th>Level of Communication</th>
<th>Advice to Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unacceptable</td>
<td>• Stop operation</td>
<td>Regulator, Manufacturer, Other operators, Management &amp; Employees</td>
<td>Warn all</td>
</tr>
<tr>
<td></td>
<td>• Do detailed Quantitative Engineering and Operational Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undesirable</td>
<td>• Restrict operation</td>
<td>Regulator, Manufacturer, Other operators, Management &amp; Employees</td>
<td>Warn all</td>
</tr>
<tr>
<td></td>
<td>• Do detailed quantitative and/or qualitative engineering and operational risk assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable – with action</td>
<td>• Restrict operation as required</td>
<td>Management &amp; Employees</td>
<td>Alert Management &amp; Employees</td>
</tr>
<tr>
<td></td>
<td>• Detailed action plan to resolve problem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable – with monitoring</td>
<td>• Establish monitoring parameters</td>
<td>Management &amp; Employees</td>
<td>Alert Management &amp; Employees</td>
</tr>
<tr>
<td></td>
<td>• Set timelines for assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable</td>
<td>• Risk profile monitoring</td>
<td>Management &amp; Employees</td>
<td>Advise Management &amp; Employees</td>
</tr>
</tbody>
</table>

Figure 11 – Example Decision Making Matrix
The matrix, above, is an example of how one organization gauged its hazard control actions in relation to the risk of the hazard. The format is the main point in presenting this model; the content can be varied by the organization to meet its own needs.

**Hazard Control or Mitigation**

Once the Risk Assessment process is complete, SMS activities move into Mitigation or Control of the Hazard. Now the Operator systematically allocates resources to minimize losses by applying controls to the hazard. Hazard controls are something we have a lot of experience with as aviation has grown hundreds on hundreds of controls in the guise of Flight Manuals, Aircraft Handbooks, Incident Response Teams, Command/Leadership/Resource programs and all the gizmos that populate our aircraft.

**Hazard Mitigations / Controls**

When a company develops and applies hazard controls there are some things to consider. One concern is whether or not the control(s) have anything to do with the hazard. Another is whether or not the mitigating action(s) create other problems. For instance, announcing a new reporting system probably doesn’t do much to mitigate a hazard even though it may project a good “image.” An example of Controls creating problems is the multiple warning devices that were placed in transport aircraft cockpits in the 1970s – there were so many bells, whoops, chimes, chirps, voices, lights, etc. that they began to interfere with pilots getting the information they needed. That had to be fixed, so Human Factors improvements in information transfer were put into cockpit designs of the 80s and 90s.

**System Safety Order of Precedence**

When companies take action to control hazards, they need to follow a standard order of precedence for the controls used. In simplest terms the most desirable way to control a hazard is to design it out. The least effective way to control a hazard is to post a warning placard or put up a safety poster. Below, we list the full order of precedence that controls are measured against.

- **Level 1** – design the hazard out - modify the system
- **Level 2** - physical guards or barriers - prevent the risk from occurring
- **Level 3** - a warning or alert signal when the hazard will occur
- **Level 4** - procedural and/or training changes
- **Level 5** - advise people (placards, notices, etc.)

The idea is to build safety in and minimize relying on human input or intervention. Realize that putting in warnings or alerts adds complexity and maybe even
generates other hazards. In corrections 3 – 5, human performance is the basis for the hazard control, and human performance is the least reliable sort of “solution” to depend upon.

**Verification**

There are two parts to “closing the loop” in Risk Management. One is Hazard Information Systems, discussed below. The other is management verifying that hazard controls actually are put in place as intended. Especially in a large company, you can’t assume that directing a hazard control / mediation to be put into effect means that it actually is put into effect, that it is implemented when intended, or that it is implemented in the way that was intended. The simple principle is to, “Verify. Verify.”

Once controls are put in place, a company needs to “close the loop” by setting up tracking systems for the hazard and its controls. This serves several purposes, all aimed at keeping the company efficient and preserving resources. All this is not for simple “make work.” You may find you have to modify the operation or process as time passes and the effects of mitigations change or the operating environment changes.

![The Risk Management "Loop"](image)

**Figure 12 – Risk Management is a “Closed Loop”**
Chapter 5 - Hazard Information Systems

There are several reasons that an SMS program must include hazard information systems:

- Foremost, information systems bring undetected hazards to the attention of the company
- Information systems serve as the means to see whether hazard controls have the desired effect, an opposite effect, or any effect at all. This is a “tracking system”
- Information systems give the company a way to actively involve employees in the safety program – assuming that employees who submit reports get positive feedback for their participation
- Information systems can provide analytic data that aid in assessing Risk for severity and frequency

Requirements

This will depend on the size and organization of the company as well as whether or not there are reporting systems outside the company that serve the purpose. While outside reporting systems, such as the NASA administered Aviation Safety Reporting System (ASRS) may meet some company needs, it’s likely that companies will want to tailor internal reports to internal circumstances.

In any case, when reports involve employee input and/or self-disclosure, it’s vital that employees be given impunity for submitting reports. Without that key feature, reporting inputs are inhibited and the company will not get the information it needs to keep itself operating efficiently and safely. Also, as a practical matter, if a company fails to extend impunity for employee reports it sends a message that employee participation is not valued. It’s a choice between motivating positive behavior that enhances the company versus aggravating the people that have all the field information and who operate all the company’s equipment.

Resources

For the people who are organizing an SMS program, Information Systems are a natural starting point. Due to the nature of aviation operations and the history of safety efforts in aviation, many reporting systems already exist. The immediate task for planners is to identify what is in place. Once that’s done, planners can address the means of getting the information rerouted to places it needs to be and to analyzing the information.
Certainly, new information systems may need to be developed, but first take advantage of what you already have. Programs such as FOQA, ASAP, and SDRs come immediately to mind because many air carriers already are using the information from these programs. They do an excellent job of showing what the “real world” of a company’s operations looks like.

Remember that gaining information on incidents or occurrences that are sub-accident level is important because any of them could have been an accident if circumstances were a little different. There may be an iceberg beneath what your reports indicate.

Also, SMS planners need to be certain there is a good quality mishap investigation and reporting system in place. The point of mishap investigation is not merely to produce a report, but to learn what’s needed to prevent the mishap recurring. Mishap reports need to lead to Risk Management. Mishap reports are part of “closing the loop.”

**Notes:**
Chapter 6 - Conclusion

Now that you’ve seen the basics of what makes up SMS, you can see that two things are all important:

- Management commitment to involvement and support
- How well the SMS Plan is put together

“Top – Down” Change

SMS at an airline is a “top down” process when it’s in use. From the top downward, the Accountable Executive puts the Plan and its growth into motion. Before that happens, a lot of preparatory work needs to be done.

A company’s SMS Policy needs to fit its organization and the goals it wants to achieve, so someone needs to think out what sort of Policy the company needs and what the roles of the various parts of the company are. Identifying the roles depends on communicating within the entire company structure. All this must accurately fit within an accurate understanding of the company’s environment. Geography, climate, personnel and education, the regulator, the customer base, and more need to be considered when understanding the environment. Each aspect of the environment represents needs or requirements for the company. All of the aspects effect the company’s safe operation.

“Bottom – Up” Change

Some of the first work in putting an SMS program into place is fairly easy. This “bottom – up” effort is to see what already exists at the airline which can and should be pulled into the SMS Plan.

Today, most airlines have some internal safety reporting systems and information systems devoted to quality assurance, maintenance recording, and equipment failures. Likewise information exists outside the company with industry parties and the regulator. In some cases there may already be non-punitive safety reporting systems in place. The thing to remember is that SMS doesn’t mean re-inventing the wheel; SMS is all about tying the company’s parts together efficiently.

1. First learn what you have.
2. Second, learn what you need.
3. Third, fill in the gaps between “have” and “need.”

In this manual, we’ve described what SMS is and how it has evolved. SMS is the natural development of all the safety efforts before it.
SMS represents the best way to boost the efficiency and effectiveness of airlines. It promotes internal coordination of resources. Its comprehensive nature improves the airline’s interface with regulators. SMS enhances the company’s business plan. The safety case is the business case.

When an SMS program is put into place, line management becomes the principle actor in safety achievement, and that’s where safety efforts are most effective. In this way, safety becomes an integral part of a company’s processes instead of something pasted on for observation but not use. SMS moves safety from the periphery into the core of the business – keeping the company efficient through loss control and best use of resources. Safety is part of the business plan. SMS is good business.

SMS effectively works in the mode of ALPA’s safety philosophy:

- Identify hazards - actions, conditions, system failures or procedural failures that may result in an accident, incident or hazardous event;
- Analyze risk of the identified hazards; and
- Implement Human Centered Design of systems, systems components and procedures to establish and maintain an acceptable level of risk.

For airlines, SMS fulfills the ALPA motto:

“Schedule with Safety.”
References

Commercial Sources

Managing the Risks of Organizational Accidents - James Reason
System Safety Engineering and Management – Roland and Moriarty
Managing Risk - Vernon Grose
Down to Earth - Forest L. Reinhardt
Managing Risk - Alan Waring and A. Ian Glendon
Modern Management - Pierre G. Bergeron
Systematic Safety Management in the Air Traffic Services - Richard Profit
Aviation Safety Programs - Richard H. Wood
Modern Safety Management - Det Norske Veritas
Normal Accidents - Charles Perrow
Sustainable Forestry Initiative Standard - American Forest & Paper Association
Responsible Care - American Chemistry Council

Regulator Sources

Introduction to Safety Management Systems – Transport Canada
Risk Management and Decision-Making in Civil Aviation – Transport Canada
Aviation Safety Management - Civil Aviation Authority, Australia

Where to Find SMS Information

<table>
<thead>
<tr>
<th>Source</th>
<th>Contact</th>
<th>Resources</th>
</tr>
</thead>
</table>
| Air Line Pilots Association   | SMS Group Engineering & Air Safety Department 535 Herndon Parkway Herndon, VA 20171 USA 703-689-4369/4198 Steve Corrie / Bill Edmunds | • SMS Information packet,  
  • Executive and Basic SMS Introduction presentations,  
  • Two-day SMS training session,  
  • Half-day Safety Risk Assessment training session,  
  • Combined two and a half day SMS / SRA training |

February, 2006
SMS texts:
- *Introduction to Safety Management Systems* – TP 13739 E (04/2001)
- *Risk Management and Decision Making in Civil Aviation* – TP 13095 (03/2001)

Products and Services:
- *System Safety Analysis Handbook*,
- *Proceedings of the International System Safety Conferences*,
- *Journal of System Safety*
- List of “links” to System Safety sources

Useful Texts
Appendix 1 – The SMS Grid

This Grid or Matrix presents the various elements of an SMS Program inclusive of all three players in the program – the Operator, Employees and the Regulator.

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Client Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operators (airline, airport, etc.)</td>
</tr>
<tr>
<td>I. Organization</td>
<td>Employees (ALPA, etc.)</td>
</tr>
<tr>
<td>II. Risk Management Activities</td>
<td>Regulatory groups (FAA, Transport Canada, etc.)</td>
</tr>
<tr>
<td>III. Information Systems on Hazards</td>
<td></td>
</tr>
</tbody>
</table>

* The vertical columns are devoted to each player or actor in the SMS relationship. Read down the columns to progress from Organizational activities, through Risk Management, to Information activities.

** Follow across the Grid, horizontally. See that each player has similar and related activities in each part of the SMS relationship. Each player’s actions reinforce and relate to the other players’ actions.

Figure 13 – The Basic SMS Grid
## Specific SMS Elements Grid

<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Client Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operator (airline)</strong></td>
<td><strong>Employee (ALPA)</strong></td>
</tr>
<tr>
<td><strong>I. Organization</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Documented SMS Program</strong></td>
<td>- <strong>Documented SMS Program</strong></td>
</tr>
<tr>
<td>Specific, documented program organization</td>
<td>Formal involvement in the operator’s SMS program</td>
</tr>
<tr>
<td>SMS integration with Business Plan</td>
<td></td>
</tr>
<tr>
<td>Systematic and continuous activities for managing safety risks</td>
<td></td>
</tr>
<tr>
<td>- <strong>Management Role</strong></td>
<td></td>
</tr>
<tr>
<td>Accountable Executive – designated and documented</td>
<td></td>
</tr>
<tr>
<td>Formal responsibility for “loss control” at each level of management</td>
<td></td>
</tr>
<tr>
<td>Formal and regular management oversight of hazard / loss control activity assisted by safety trained personnel</td>
<td></td>
</tr>
<tr>
<td>Cadre of safety trained personnel</td>
<td></td>
</tr>
<tr>
<td>(Cont’d)</td>
<td>(Cont’d)</td>
</tr>
</tbody>
</table>
| - **Documented Policies** (Cover entire company) | - **Documented Policies**  
 Contract/LOA/MOU documentation of SMS participation actions/responsibilities | - **Documented Policies**  
 Recommended standards for Operator SMS programs |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Acceptance policies</td>
<td></td>
<td>Framework for review of Operator SMS activities: ATOS, CSET, etc.</td>
</tr>
</tbody>
</table>
| - **Employee Role**  
 Develop full participation of employees | - **Employee Role**  
 Develop and provide topic experts specialists to participate in company hazard analysis and control activities | - **Employee Role**  
 Prepare line level personnel to live in and foster an SMS environment |
<p>| Effectively use employee expertise based on line level experience of hazard occurrences and with hazard controls | | |</p>
<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Client Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>II. Risk Management Activities</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator (airline)</td>
</tr>
<tr>
<td></td>
<td>Intra company study groups (cross silos) to take advantage of varied expertise and skills</td>
</tr>
<tr>
<td>- Hazard Analysis Systems</td>
<td>- Hazard Analysis systems</td>
</tr>
<tr>
<td></td>
<td>Participate in Hazard Analysis activities</td>
</tr>
<tr>
<td>- Risk Assessment Systems</td>
<td>- Risk Assessment Systems</td>
</tr>
<tr>
<td>- Hazard Control Systems</td>
<td>- Hazard Control Systems</td>
</tr>
<tr>
<td></td>
<td>Participate in control development</td>
</tr>
<tr>
<td></td>
<td>Modify controls as field experience indicates</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Cont’d)
| - **Hazard control tracking systems**  
  Verify that hazard controls are in place  
  Verify the effects of hazard controls | - **Hazard control tracking systems**  
  Participate in feedback on hazards and hazard controls  
  Provide reports on hazard status | - **Hazard control tracking systems**  
  Verify Regulator, Industry, and Operator hazard controls are in place, e.g. oversight and required reporting programs  
  Evaluate the effect of the controls |
<table>
<thead>
<tr>
<th>SMS Activity</th>
<th>Client Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>III. Information Systems on Hazards</strong></td>
<td><strong>Operator (airline)</strong></td>
</tr>
<tr>
<td>- Internal hazard information systems</td>
<td>- Hazard reporting systems</td>
</tr>
<tr>
<td>For detection, analysis and program improvement</td>
<td>For detection, analysis and program improvement</td>
</tr>
<tr>
<td>Non-punitive reporting systems for employees</td>
<td>Participate in employer non-punitive operator safety reporting systems</td>
</tr>
<tr>
<td>Feedback and sharing of information</td>
<td>Participate in industry non-punitive safety reporting systems</td>
</tr>
<tr>
<td>Integrate full range of operator information (cross silo)</td>
<td>Internal safety reporting systems</td>
</tr>
<tr>
<td>- Use of external hazard information systems</td>
<td>- Use of external hazard information systems</td>
</tr>
<tr>
<td>e.g., regulator, manufacturer, industry group, international, etc.</td>
<td>e.g., regulator, manufacturer, industry group, international, etc.</td>
</tr>
</tbody>
</table>
Appendix 2 – The Safety Risk Assessment (SRA) Process

Overview

Safety Risk Assessment (SRA) is a core part of the Safety Management System (SMS). SRA is aimed at eliminating hazards or reducing them to acceptable levels. SRA is a “closed loop” process that consists of learning, acting and adapting. This recognizes that situations change, we learn new things, our plans don’t work as designed, etc. In other words, SRA is a “real world” process rather than an “ivory tower” exercise. SRA is integral with Risk Management, so the table, below, ties SRA to Risk Management in the “closed loop.” In an overall view, the SRA process consists of Organizing, Assessing and Managing Risk.

<table>
<thead>
<tr>
<th>Process Stage</th>
<th>Process Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organize</strong></td>
<td>• <strong>Identify</strong> the problem/program and appropriate Risk decision maker(s)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Form</strong> a Working Group, Steering Committee, ExCom</td>
</tr>
<tr>
<td></td>
<td>• <strong>Define</strong> the problem/program</td>
</tr>
<tr>
<td></td>
<td>o People</td>
</tr>
<tr>
<td></td>
<td>o Equipment</td>
</tr>
<tr>
<td></td>
<td>o Environment</td>
</tr>
<tr>
<td></td>
<td>o Interfaces</td>
</tr>
<tr>
<td></td>
<td>• <strong>Define</strong> terminology</td>
</tr>
<tr>
<td></td>
<td>o the hazard(s)</td>
</tr>
<tr>
<td></td>
<td>o terms of severity</td>
</tr>
<tr>
<td></td>
<td>o terms of probability</td>
</tr>
</tbody>
</table>

Notes:
<table>
<thead>
<tr>
<th>Process Stage</th>
<th>Process Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess Risk</td>
<td>• First Look</td>
</tr>
<tr>
<td></td>
<td>o Preliminary Hazard List</td>
</tr>
<tr>
<td></td>
<td>o Preliminary Hazard Assessment</td>
</tr>
<tr>
<td></td>
<td>• Agree on Hazards for SRA focus</td>
</tr>
<tr>
<td></td>
<td>• Assess Risk of “focus hazards”</td>
</tr>
<tr>
<td></td>
<td>o FTA, FMEA, OSA, STEP, etc.</td>
</tr>
<tr>
<td></td>
<td>• Identify Unknowns</td>
</tr>
<tr>
<td></td>
<td>• Provide analysis to Risk Decision Maker(s)</td>
</tr>
</tbody>
</table>

Notes:
<table>
<thead>
<tr>
<th>Process Stage</th>
<th>Process Actions</th>
</tr>
</thead>
</table>
| **Manage Risk** | - **Evaluate** Risk Assessment and identified Unknowns  
| |   - Does this require further analysis?  
| |   - Are the Unknowns acceptable?  
| |     - Is Action required?  
| |       - If “No” then document why.  
| |       - If “Yes” then Implement Hazard Controls/Mitigations  
| | - **Monitor/Measure** Performance  
| |   - Employee/industry safety reports  
| |   - Incident and accident reports  
| |   - Testing  
| |   - Violations  
| |   - Audits  
| |   - Etc.  
| | - **Refer** “lessons learned” back to Risk Assessment Working Group  
| | - **Modify** Hazard Control Actions as indicated by performance measuring |

**Notes:**
Five Steps to a Safety Risk Assessment

*SRA* is an activity that you can use both for EASC Projects and E&AS Activities. It is based on System Safety techniques (U.S. MIL STD 882 and Canada’s CSA Q-850). *SRA* is a well-defined and structured process that gives you the advantage of an accurate look at your problem. When you use *SRA*, you may even have a better look at the problem than other interested parties might have.

**Step One – Plan**

*It’s about organizing ALPA’s effort in the project.*

**Questions:**

1. What is the scope of the project and its objectives?
2. Is the system and/or subsystems on which the project is based clearly defined?
3. Are the system/subsystem requirements clearly documented?
4. Will the system/subsystem interact with other systems and how?
5. What safety issues are readily apparent in the new project?
6. What other ALPA projects could be affected by this new project?
7. Is it a project that is narrowly focused area does it have broad, system-wide impact?
8. Who are the customers of the project’s benefits?
9. What ALPA resources will be required?
10. Does the project require an ALPA multidisciplinary team?
11. Who are the stakeholders involved in the project?
12. How effective do the government/industry chairmen appear to be in handling the project and team?
13. Is the chair/co-chairs easily influenced by stakeholders?
14. What methods are being proposed to address the safety issues involved?
15. What tools will be used in the methodology to assist in analyzing the safety issues?
16. How much confidence can be placed in the methodology and the tools that will be used?
17. What mechanism(s) will be put in place to verify implementation, to monitor, and to measure the effectiveness of the project results once they are implemented?
18. Will the project team accept a safety risk assessment approach to addressing the safety issues?
19. Who else might be affected or be the target of the SRA outside the project team?
Actions:

1. Attempt to answer these and other related questions important to the project.
2. Ensure that the system(s) involved in the project are clearly defined.
3. Define the goals that ALPA wants to achieve through the project.
4. Define the products that are expected to result.
5. Ensure that the needed resources are available for the project.
6. Identify any potential shortcomings in resources.
7. Identify the expected costs involved and the expected length of time to complete the project.
8. If a SRA will be performed:
   a. Ensure that the scope of the SRA is consistent with the system(s) involved.
   b. Determine the best method of performing the SRA.
   c. Determine what data sources and information will be needed to accomplish the SRA.
   d. Review the adequacy of the plan.
   e. Develop the terms of reference for the team:
      i. Include the list and definition of terms used in the SRA
      ii. Obtain a consensus in defining the risk limitations, i.e. what is and is not acceptable risk (Ref. Risk Matrix development).
      iii. Identify the subject matter experts (domain experts) that will be required in the SRA process.
      iv. Decide how the SRA will be documented and included in the team report.
9. If the project team is not in favor of performing a SRA, find out what can be done to change their minds – who can be influenced?
10. If a SRA will not be performed, apply the method as best you can through your individual participation to identify the shortcomings in the other method(s) chosen and make these known to the team and ensure that it is documented in the written work of the project.
11. Ensure these shortcomings are reported to ALPA management.
Step Two – Hazard Identification and Analysis

*It’s about “Murphy’s Law” - What can go wrong will go wrong!*

**Definition**

*A “hazard” is an event, condition or circumstance that can lead to a loss.*

**Identification**

1. Hazards may be *actual* or they may be *potential*.
2. Hazards can be identified by observation, using data and the knowledge of others that can help describe how a particular activity, process or system functions or is supposed to function. This information can indicate where and what problems could or are occurring so that effective corrective actions can be formulated and implemented.
3. Effective hazard identification depends on:
   - the experience and knowledge of the analysis group,
   - the proper choice of analytical methods, and
   - the availability of accurate safety data resources.

**Historical Data**

Historical data can provide insights into the hazards associated with a previous or current activity or system, which can be used to direct attention to identifying new hazards in the identification process. Historical data can also provide guidance for formulating future corrective actions. Previous “Lessons Learned” can define “past mistakes” with the hope that these same mistakes will not be repeated in future activities and systems. “Lessons Learned” can also highlight the things that were done right for future reference.

“Safety data” essentially has four primary uses by the safety practitioner in the course of safety activities:

1. In the design process;
2. In hazard analyses;
3. In safety risk assessment activities; and
4. In validating and monitoring execution of SRA results and its effectiveness

**Some Means for identifying hazards**

1. Review available data and program/system requirements
2. Conduct observations, audits, safety surveys, investigations, research
3. Conduct factual briefings from subject matter (domain) experts, project team members, frontline personnel
4. Apply relevant analysis tools - flow charts, event trees, fault trees, failure mode and effects (and criticality) analyses, software programs, mathematical & statistical modeling, simulations

5. Brainstorm within the team

**Hazard Identification and Analysis**

**Identification - Preliminary Hazard List (PHL)**

This is the first step in the *Hazard Identification and Analysis* process. It’s the first document prepared in the SRA. A hazard is the potential for harm. It could be a physical condition called an unsafe condition, i.e. inappropriate function, failure, or it could be an inappropriate human act, i.e. an unsafe act, human error in a design, or procedure. The objective is to develop a list of these initial hazards. It can be based largely on anecdotal and historical information, but includes data and information from the previously mentioned sources. For example:

**Inputs:** Safety data from similar systems, hazard logs, incident or accident reports, safety lessons learned, program safety requirements, expert opinion, etc.

**Outputs:** A list of actual or potential hazards for follow-on hazard analysis and identification of additional safety design requirements.

Normally, the PHL is started in the conceptual phase of a program or project. It provides management with initial information on inherent hazards that may be associated with the concept in a design. The idea is to develop a list of all possibilities, without regard to the likelihood of the event actually occurring. Again, the typical way of developing the PHL is by brainstorming within a group. It can also be developed from checklist (the least effective), generic requirements reviews, informal conferencing, and research.

**PHL Process**

The first objective is to acquire as much information about the concept design as possible. It is very appropriate to invite the subject matter (domain) experts to participate in the PHL development. The process steps are:

1. Establish a team to develop the PHL. Team members should be from appropriate areas involved in the concept/system design.
2. Provide training to the team in system safety concepts and how to develop a PHL.
3. Identify the method of conducting the PHL.
4. Identify the document format.
5. Team members will need to enhance or acquire concept/system knowledge.
6. Review prior system safety related data, if available
7. Acquire knowledge of previous related occurrences.
8. Consider all life cycle phases of the design.
9. Consider all system and activity elements; human, hardware, software and environment interactions
10. Identify energy sources (where’s the thrust of the harm?)
11. Consider generic hazards as a start (see table, below)
12. Start to develop the PHL.

**Analysis – Preliminary Hazard Analysis (PHA)**

Once initial hazards are listed, it is possible for changes to be made early in the concept design stage so that these hazards can either be eliminated early or controlled later in the process. The PHL also provides the bases for a more detailed analysis called Preliminary Hazard Analysis (PHA).

The primary intent of a PHA is to ensure that all relevant hazards are identified. It also is intended to identify the cause(s) and effect(s) of the hazard(s), to define its characteristics, and to prioritize it or to ignore it if it is not worthy of further analysis. *Cause(s)* is the underlying reason why a hazard exists. The *effect(s)* is the possible consequence(s) resulting from allowing the hazard to exist. Each hazard can have a number of potential causes and consequences.

**Primary Hazard** - A hazard that leads to or is responsible for other hazards existing in the system. It’s the driver behind other hazards.

**System Deficiency** – A condition or circumstance that permits hazards of a like nature to exist within a system. Similar hazards may be present in a similar activity or system and attempts should be made to identify them as well.

From a generic hazard classification, hazard(s) characteristics can be further defined by formulating a **Hazard Statement**. Some examples are:

- The IFR separation is 1 mile
- The airport’s painted signs are weathered
- Pilots receive no simulator training
- Taxiway “E” meets runway 32 at 140°

A useful method to help analyze the hazard potential is to develop scenarios that explore the various ways that harm can be manifested or revealed. These are called hazard **scenarios** and can be thought of as the, “**What ifs?**” Take the time to identify any Primary Hazards and System Deficiencies.
Input:
- Using the results from the PHL, analyze the hazards by determining the cause(s) and consequence(s) of the hazard(s)
- Rank these hazards in the order of importance as determined by the team.

Output: The PHA documents and organizes information on the potential hazard areas and on the ranking of hazards by consequences or severity.

The PHA is the basic system safety analysis for a program. It is a living document that requires periodic updating from feedback. From the identification process, the safety practitioner can then begin to identify the risks associated with the hazards.
Step Three – Risk Assessment

It’s about the likelihood of the harm happening – what’s your comfort level?

Definition

“Risk” is the consequence of a hazard. Risk is measured in terms of severity and probability.

In this step, further classify the consequences in terms of severity and add to it the probability (exposure) of the hazard(s) or potential for harm occurring. Ask the question, “If a particular hazard potential does occur, how often and how severe will it be?”

The kind of assessment method, whether qualitative or quantitative, will depend on availability of exposure data. Usually, the data you would like to have is not readily available. Generally, some combination of the two methods will be used.

Levels of Risk

Levels may be assigned quantitatively, qualitatively or both. Develop or use an existing Risk Matrix for documenting the assessment. (See attachment __). If there is an existing matrix, it may help facilitate the acceptance of your work and provide the decision-maker(s) with a result that is understood and compatible with what is already in use. Ensure that there is consensus on the classifications. If there are any changes to be made, make them before you begin the process.

From this exercise, risk statements can be formulated that combine in narrative form the product of the severity and likelihood of the hazard(s) potential for harm.

Acceptable Levels of Risk

Another important function is to determine what risks are acceptable. From a single organization standpoint, it may be fairly easy based on the organizations, goals, objectives, culture, etc. However, when several stakeholders are involved, the exercise could be difficult. Part of this exercise determines the scope and parameters of the Risk Matrix. What is the potential loss or degree of loss that the program/project is trying to avoid? These potential losses can be considered individually or in tandem and severity and probability estimates assigned accordingly.

Finally, compare and rank the risks.
Hazard Control - Risk Mitigation

As a part of the Risk Assessment, you'll next turn your attention to how the loss can be prevented. This includes assessing existing hazard control or risk mitigation actions or developing new prevention actions, strategies, or “controls.” These controls or mitigation actions are designed to either eliminate or lessen the potential for the hazard(s) to create harm. In this particular assessment exercise, it is possible to identify areas where further safety analyses are required.

Thoroughly review existing and corresponding regulatory standards, policies, procedures, best practices, equipment capabilities and reliabilities, human performance capabilities and limitations, and training. From this review, make a determination of the ability of these types of controls to either eliminate or control the hazard(s) to “acceptable” levels of risk. If they cannot adequately reduce risk to acceptable levels, then you must formulate new controls and mitigation actions. Use the following approach to mitigating Risk. In it you'll see the natural ranking from the most to least desirable ways to control Risk.

System Safety Order of Precedence – A defined order of hazard control actions.

1. Modify the system to design out the hazard
2. Add physical guards or barriers to prevent the risk from occurring
3. Add warning or alert signals
4. Develop procedural limits and training
5. Brief all pilots!

More Important Definitions

Consequential Risk – Additional risk that may be created while attempting to address the original hazard(s).

You should ask, "Will we create more problems if we try fixing the hazards, than if we leave things alone?" In other words, what impact will corrective actions have on producing additional hazards and therefore risks?

Residual Risk – The risk that may remain after the process has been completed.

Since all risk may not be mitigated, the residual risk must be identified so that it can be made known and further work can be accomplished.

The decision-making matrix discussed in Step Four, below, provides a guide for how to react to the risk you identify. Develop the decision-making matrix with agreement of the Risk Assessment group before doing the assessment. If there is an existing decision matrix within a program, project or organization, then try to use or adapt it.
In the example Decision-Making matrix of Step Four, below, there are five action levels based on the risk assessed. For example, from the matrix one could decide that risk values over 20 are unacceptable and they will require action as detailed under that category. Undesirable risk could represent 15-19, while acceptable could be 10-14 with some action. Acceptable with monitoring could be 5-9 and acceptable, 0-4. These are not hard and fast rules for assigning action, but are meant only to be illustrative. The risk factors that will be assigned to the various levels are based on the goals, objectives, and values of the program, project and/or organization.
Step Four – Decide and Report

It’s about revealing the hazards and associated risks involved in the program or project to decision-makers so that their conscience can be exercised.

Report Documentation

Once the team or group makes decisions relative to each risk, document the rationale for acceptance and confirmation of the corrective actions to be taken. Using the Decision Matrix will help in formulating follow-on actions.

Take program/project requirements, organizational values and subjective judgments into account. They are part of the decision-making process. Consider the importance of the assessed risk against shared values, the associated social, environmental and economic considerations and the potential cost of acting vs. not acting.

Recommendations

When the Risk Assessment Group has formulated the rationale and corrective actions to address the risks, the Group will have to make a decision on whether or not to make recommendations. Safety practitioners are accustomed to making safety recommendations, particularly after an assessment, as a part of a report. However, the SRA report could probably suffice without recommendations and be used effectively by decision-makers.

Some decision-makers may like and expect recommendations because those recommendations may provide a fresh solution and complete the work. Conversely, a decision-maker(s) could be put on the defensive and spend more time fighting the recommendations than they will spend fixing the problem. Recommendations may appear confrontational because the decision-maker(s) were not part of the solution and, as has happened numerous times, they may allow the responsible decision-maker(s) to avoid action.

It may be wise for the team or group to consider including recommendations within the SRA report. If recommendations are made, they should be formulated to allow the decision-maker(s) to determine the best way to implement the action. Even better would be the approach of working with the decision-makers to develop recommendations for change.
Step Five - Evaluation

*It’s about executing the plan and how things are going – “closing the loop”*

**Validation, Monitoring and Feedback**

In this step we want to ensure that the actions and results of the Risk Assessment Group’s work are put to use. Somehow the Group needs to verify that the controls and mitigations have been put in place. Some effective means of alerting “line” personnel to the Risk control and acceptance decisions that have been made.

A tracking or monitoring system must be implemented as a part of the SRA process. This permits evaluating the performance of the corrective actions to ensure the activity or system is meeting expectations. Are the mitigations effective? Theoretically, monitoring is an activity that should be done in real time, but this may not be possible.

In addition to the performance of the activity or system, the values and beliefs used to develop and maintain the system need to be evaluated and understood. The SRA should be updated periodically to ensure it remains valid. These updates or follow-on actions are good for detecting any change from the original risk profile. Changes in the Risk situation may mean that new hazard controls or mitigation strategies need to be established. The “Feedback” of the Evaluation Step is vital and allows for measuring and maintaining the “safety” of the system.
The Overall System Safety Process – including the Risk Management Process

Define Objectives

Describe “System”

Identify Hazard(s)

ANALYZE HAZARD(S)

Hazard Controls

Verification of Controls

Risk Acceptance?

No

Modify System

Yes

Document Risk Acceptance and Rationale

Periodic System Review

The Risk Management Process

Yes
# Generic Hazards and Categories

To get you started, you might consider these generic hazards or hazard categories:

| Collision | Hazardous materials |
| CFIT | Radiation |
| Weather | Electrical |
| Loss of systems | Contamination |
| Loss of capability | Parts |
| Human error | Boundary handoff |
| Emergency conditions | Commercial software |
| Software malfunction | Commercial equipment |
| Inappropriate communication | Atmospheric conditions |
| Demand | Physiological |
| Traffic flow | Error in design |
| Inadvertent operation | Temperature |
| Inappropriate data | Explosion |
| Inaccuracy | Fixation |
| Inappropriate calculation | Fire |
| Automation lockup | Egress |
| Situation awareness | Acceleration |
| Inadequate contingency | Corrosion |
| Open networks | Impact |
| Contractual systems | Shock |
| Inappropriate warning | Pressure |
| Lack of, or loss of warning | Structural damage |
| Jamming | Toxicity |
| Spoofing | Vibration |
| Taxi accident | Noise |
| Ground control | Oversight and Omission |
| Landing accident | Takeoff accident |
**Design Considerations**

Hazards can be hypothesized by considering design difficulties or deviations, consider the following:

<table>
<thead>
<tr>
<th>Adequacy of redundancy</th>
<th>Status checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility for repair</td>
<td>Human response</td>
</tr>
<tr>
<td>Automation and human control considerations</td>
<td>Reliability measurement</td>
</tr>
<tr>
<td>Availability and Availability</td>
<td>Logistics</td>
</tr>
<tr>
<td>System tolerances</td>
<td>Sneak paths</td>
</tr>
<tr>
<td>Resource availability</td>
<td>Test access</td>
</tr>
<tr>
<td>System compatibility</td>
<td>Analog designs</td>
</tr>
<tr>
<td>System alignment</td>
<td>New technology</td>
</tr>
<tr>
<td>Response to environmental interaction</td>
<td>Technology transfer</td>
</tr>
<tr>
<td>System replacement</td>
<td>Disposal considerations</td>
</tr>
<tr>
<td>Human Factors</td>
<td>Technological growth</td>
</tr>
<tr>
<td>Ergonomics</td>
<td>Weak links</td>
</tr>
<tr>
<td>Assembly</td>
<td>Bottlenecks</td>
</tr>
<tr>
<td>Segregation of safety critical systems</td>
<td>System refinements</td>
</tr>
<tr>
<td>Verification and Validation</td>
<td>Inappropriate functions</td>
</tr>
<tr>
<td>Calibration</td>
<td>Remote transfer of information</td>
</tr>
<tr>
<td>Monitoring of safety systems</td>
<td>System deadlock</td>
</tr>
<tr>
<td>Open system designs</td>
<td></td>
</tr>
<tr>
<td>Command and Control access</td>
<td></td>
</tr>
<tr>
<td>Bypass of systems</td>
<td></td>
</tr>
<tr>
<td>Shutdown</td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
</tr>
<tr>
<td>Unique coding</td>
<td></td>
</tr>
<tr>
<td>Reasonableness checks</td>
<td></td>
</tr>
</tbody>
</table>
Simple Preliminary Hazard Analysis Worksheet

Hazard Analysis # ____  Date: __________

Location: _______________________________________________________________________________

ORGANIZATION/DEPARTMENT: __________________________________________________________________________

System/Activity/Task: __________________________________________________________________________________

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Potential Cause(s)</th>
<th>Potential Effect(s)</th>
<th>Hazard Category</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Detailed Hazard Analysis Worksheet**

General Hazard Analysis No. ________________________________  
Location/Dept. ____________________________________________________________________________  
Description (Task/Activity) ____________________________________________________________________  
Prepared by ________________________________  
Date ______________

Countermeasures ____________________________________________________________________________

Cost/Impact ____________________________________________________________________________

<table>
<thead>
<tr>
<th>Task/Activity Elements</th>
<th>Hazard Elements</th>
<th>#1</th>
<th>#2</th>
<th>#3</th>
<th>#4</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazard Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note:* First define and determine the Task/Activity elements to be examined and assign a number to each. Also identify the Hazard Elements and record in order of criticality, the #1 being the most critical. (See attached instructions)
Detailed Hazard Analysis Worksheet (cont.)

**Instructions**

1. The Hazard Analysis Worksheet is used to examine those hazards identified in the Preliminary Hazard List (PHL).

2. Pick a logical starting point in the sequence of events and observe the task(s) and activity (ies) in their entirety several times before doing the analysis.

3. Begin with the first task/activity and define the element(s) being performed.

   **Note:**
   - Do not select too large a task/activity element(s). This would block your ability to isolate each part of an element that may contain hazard(s)
   - Do not select a task/activity element(s) so small that one hazard element may be involved in many other tasks/activities elements. This would unnecessarily complicate the analysis.

4. Repeat step 2 for subsequent task/activity elements, ensuring that no task/activity is excluded or repeated (overlap).

5. Where options or simultaneous activities are required, analyze each separately and then combine them in a final listing.

6. List the task/activity elements on the form in the order in which they occur in the sequence. Ensure that the starting and ending points of each element are clearly defined.

7. Prepare a Detailed Hazard Analysis Worksheet for each countermeasure as well.
## Sample Risk Assessment Matrix

<table>
<thead>
<tr>
<th>Severity**</th>
<th>Probability*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Catastrophic</strong></td>
<td></td>
</tr>
<tr>
<td>Loss of life</td>
<td>5</td>
</tr>
<tr>
<td>Loss of aircraft</td>
<td>5</td>
</tr>
<tr>
<td><strong>Critical</strong></td>
<td></td>
</tr>
<tr>
<td>Serious injury</td>
<td>4</td>
</tr>
<tr>
<td>Substantial damage</td>
<td>4</td>
</tr>
<tr>
<td><strong>Serious</strong></td>
<td></td>
</tr>
<tr>
<td>Aircraft damage</td>
<td>3</td>
</tr>
<tr>
<td>Minor injury</td>
<td>3</td>
</tr>
<tr>
<td><strong>Marginal</strong></td>
<td></td>
</tr>
<tr>
<td>Operational effect</td>
<td>2</td>
</tr>
<tr>
<td>Loss of employee time</td>
<td>2</td>
</tr>
<tr>
<td><strong>Negligible</strong></td>
<td></td>
</tr>
<tr>
<td>System disruption</td>
<td>1</td>
</tr>
</tbody>
</table>

See Severity and Probability Categories (below):

- Improbable \((10^{-9})\): Not likely to ever occur
- Remote \((10^{-7})\): Likely to occur once every twenty years
- Occasional \((10^{-5})\): Likely to occur once a year
- Probable \((10^{-3})\): Likely to occur twice a month
- Frequent \((1.0)\): Likely to occur once a week
** Severity Categories **

** Catastrophic **
This would equate to loss of life or the loss of an aircraft hull. In other areas of loss it could represent the loss of your job, a complete loss of customer confidence in the airline or financial failure.

** Critical **
Critical could represent serious injury or substantial aircraft damage in an accident or incident scenario. In other areas of potential loss you are trying to avoid, it could represent the loss of someone else's job, reduced customer confidence or loss of market share or significant negative financial impact on the company.

** Serious **
This could equate aircraft damage or minor injury. But, in other areas of potential loss it could represent some job losses, some loss of market share or financial impact.

** Marginal **
Marginal could be used for effects that may be undesirable but not earth shattering. It could suggest a need to make operational changes or result in reducing the productivity of staff.

** Negligible **
This is a minor severity loss and, probably one that you will decide to live with.

** Probability Categories **

** Frequent **
For frequent you would want to establish the worst-case scenario. If the loss potentially could occur once a week, that is probably a good starting point. However, here may be other losses, such as loss of customer confidence that you may choose to assume will happen every day. That, then, would be the worst-case scenario. The matrix above shows a qualitative assessment (Frequent) along with a quantitative assessment (1.0)

** Probable **
The next category should reflect a linear progression from frequent, which you are going to use throughout the matrix. That is, the steps between each category should be linear one to the other. In our example we have shown the quantitative assessment for the subjective probable as $10^{-3}$ or the loss may occur once every 1,000 times for the operation. If I have 1,000 movements a month and I have experience one accident per month then my probability of having an accident is once every 1,000 movements or once a month.

** Occasional **
For occasional, we have shown a progression of the probability of loss to $10^{-5}$ or once in every 100,000 times for the particular operation.

** Remote **
Remote means, in our example, that you anticipate the risk of a loss you are trying to avoid once every 10,000,000 times for a particular operation.

** Improbable **
Quantitatively, this means a loss every 1,000,000,000 times for the operation

Once you have established categories, the organization should establish specific actions to be taken in light of different risk levels. These decisions should reflect shared values within the organization and should remain consistent. There should be no opportunity to modify the action on a particular risk assessment and this should only be done when the complete assessment process and performance of the process is reviewed in depth.
## DECISION MAKING MATRIX

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Follow up</th>
<th>Level of Communication</th>
<th>Advice to Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unacceptable</td>
<td>Stop operation</td>
<td>Regulator</td>
<td>Warn all</td>
</tr>
<tr>
<td></td>
<td>Detailed Quantitative Engineering &amp; Operational Risk Assessment</td>
<td>Manufacturer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other Operators</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management &amp; Employees</td>
<td></td>
</tr>
<tr>
<td>Undesirable</td>
<td>Restrict operation</td>
<td>Regulator</td>
<td>Warn all</td>
</tr>
<tr>
<td></td>
<td>Detailed quantitative and/or qualitative engineering &amp; operational risk assessment</td>
<td>Manufacturer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other operators</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management &amp; Employees</td>
<td></td>
</tr>
<tr>
<td>Acceptable with action</td>
<td>Restrict operation as required</td>
<td>Management &amp; employees</td>
<td>Alert management and employees</td>
</tr>
<tr>
<td></td>
<td>Detailed action plan to resolve problem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable with monitoring</td>
<td>Establish monitoring parameters</td>
<td>Management &amp; employees</td>
<td>Alert management &amp; employees</td>
</tr>
<tr>
<td></td>
<td>Set timelines for assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptable</td>
<td>Risk profile monitoring</td>
<td>Management &amp; employees</td>
<td>Advise management &amp; employees</td>
</tr>
</tbody>
</table>

February, 2006
Appendix 3 - Guidelines for Developing a Safety Management System (SMS)

SMS Components

The components that make up a Safety Management System are:

<table>
<thead>
<tr>
<th>Organization</th>
<th>Risk Management</th>
<th>Hazard Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Approach</td>
<td>• Safety Oversight</td>
<td>• Safety Oversight</td>
</tr>
<tr>
<td>• Documentation</td>
<td>• Hazard Risk Assessment</td>
<td>• Hazard Information reporting</td>
</tr>
<tr>
<td>• Training</td>
<td>• Quality Assurance</td>
<td></td>
</tr>
<tr>
<td>• Emergency Response Plan</td>
<td>• Emergency Response Plan</td>
<td></td>
</tr>
</tbody>
</table>

I. ORGANIZATION

A. Approach – organizes comprehensive and systematic management of safety throughout the company under the control of the Accountable Executive.

Define the fundamental approach for managing safety in the company

- Mission Statement
- Philosophy
- Policy – a safety policy defining the philosophical approach to safety and performance goals.
- Non-punitive reporting policy
  - Encourage incident and hazard reporting
  - Discriminate between Errors and Willful Acts

Define roles and responsibilities

- Management accountability
  - Top management accountability for safety
  - Line management accountability for safety
- Practices
  - Proactive Leadership and Management
- Employee Involvement
  - Development of the SMS program
  - Implementation of the SMS program
  - On-going involvement in SMS administration and refinement
Designate functional area responsible for safety program oversight
Define and Document roles of all personnel
  - Delineate all lines of authority
  - Document specific safety responsibilities for each position and task
    - Accountable executive responsible for:
      - establishing and maintaining the SMS
      - Placing safety matters on meeting agendas at all levels
      - Providing resources necessary to attain strategic safety objectives
      - Allocating necessary resources, such as time and money to safety matters

Establish a requirement for a company-wide communication plan regarding the SMS program, SMS progress, and on-going SMS functions

Detail responsibility of managers for externally supplied services
Detail the line of responsibility for ensuring that staff are competent and trained for their duties

Safety office (dependent on size of the company)
  - Lines of communication to:
    - The Accountable Executive,
    - Within line management
  - Functions:
    - Safety expertise
    - Safety information systems
    - Audit functions (IEP, Quality Assurance, etc.)
    - Active involvement in safety activities and reviews at all locations
    - Receive and start action on employee safety reports
    - Promote safety topics in company publications
    - Mishap investigation and reporting – incorporating line management expertise and involvement

Document:
  - The competencies required for each position
  - Procedures
  - Safety committee(s)
    - What level of company? e.g., Board of Directors, Divisions, Departments, Shops, etc.
    - Who participates
    - Frequency of meetings
  - Required outputs:
    - Periodic reports
- Mishap and Loss reports
- Reports of progress in implementing and monitoring hazard controls

**Performance**
- Safety performance measuring
- Safety reporting
- Hazard control verification

Establish liaison with Regulator’s airline representatives / inspectors regarding company move into an SMS program for safety management.
- Ensure Regulator rep(s) understand this will make interface with oversight program easier
- Obtain Regulator support of and participation in airline’s FOQA and ASAP-like programs

**B. Documentation**

Identify applicable aviation and other safety regulations/requirements.
- Maintain documentation - current, applicable and effective

Consolidate documentation describing the components of the SMS into an SMS document

Implement changes to documents as required by:
- Changes to regulations, standards and exemptions
- Experience

**C. Training**

Document training requirements for each area of work

Provide appropriate information, skills and training to accomplish tasks for:
- Line management
- Line employees
- Safety staff
  - Accident investigation personnel

Train Line and Staff management in organizational factors and human factors.
- One time initial training
- Easily accessible training resource to be used after inevitable personnel changes

**D. Emergency Response Plan**

Policy
II. Risk Management

A. Safety Oversight

Pro-active
- Corrective action and risk reduction strategies:
  - Seek to identify potential hazards through the analysis of everyday activities or reports through the company's safety reporting system
  - Systems for reporting hazards, events or safety concerns
  - Methods for the collecting, storing and distributing data
  - Systems for analyzing data, safety reports and any other safety related information
- On-going system monitoring
- Tracking of hazard control/mitigation implementation
  - Confirmation of the effectiveness of corrective action

Reactive
- Respond to events that have occurred
  - Unexpected events (accidents, incidents, ASAP reports, etc.)
  - Indications that hazard controls are not having the desired effect.

General
- Establish means to share properly sanitized safety data with any other parties who potentially could benefit from access to the data
B. Hazard Risk Assessment

Establish a Risk Assessment methodology

Example:

<table>
<thead>
<tr>
<th>Probability of Occurrence</th>
<th>Impact</th>
<th>Negligible System disruption</th>
<th>Marginal Aircraft damage or minor injury or LOSS of Critical Aircraft System.</th>
<th>Critical Serious personal injury/substantial aircraft damage</th>
<th>Catastrophic Loss of life or aircraft hull loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Likely to occur once a week</td>
<td>5</td>
<td></td>
<td>10</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Probable</td>
<td>4</td>
<td></td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Likely to occur twice a month</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>3</td>
<td></td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Likely to occur once a year</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>2</td>
<td></td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Likely to occur once every 20 years</td>
<td>1</td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Improbable</td>
<td>1</td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Establish a Risk Management Decision scheme

Example:

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>ACTION</th>
<th>Company Follow Up</th>
<th>External Level of Communication</th>
<th>Internal Level of Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intolerable</strong></td>
<td>Immediate Measures Taken</td>
<td>Action Plan development and deployed within 48 hours &amp; Progress Monitoring</td>
<td>Advise Authorities: FAA, etc.</td>
<td>Emergency Advisory</td>
</tr>
<tr>
<td><strong>Unacceptable</strong></td>
<td>Immediate Temporary Measured Deployed within 48 hours &amp; Action Plan development and deployment within 7 days &amp; Progress Monitoring</td>
<td></td>
<td>Advise Authorities: FAA, etc.</td>
<td>Immediate Advisory</td>
</tr>
<tr>
<td><strong>Undesirable</strong></td>
<td></td>
<td>Progress Monitoring</td>
<td>As Necessary</td>
<td>Notice</td>
</tr>
<tr>
<td><strong>Acceptable</strong></td>
<td>No Action</td>
<td>Continuous Risk Profile Monitoring</td>
<td>N/A</td>
<td>Advise</td>
</tr>
</tbody>
</table>

Establish cross discipline Risk Assessment/Management groups as appropriate based upon:
- Standing problem / hazard topics
- New or unexpected operational problem / hazard topics
C. Quality Assurance

Internal and external audits:
- Make use of scheduled internal audits to build cross company cooperation and trust.
- Use external audits on a periodic basis to validate company safety efforts and detect unexpected trends or hazards

Well-designed and documented procedures for product and process control

Inspection of testing methods
- Monitoring of equipment including calibration and measurement

Monitoring of corrective and preventive actions
- Use of appropriate statistical analysis when required

Measure overall company safety performance and the effectiveness of the SMS Program via a standing audit system overseen by an SMS oversight committee

SMS Oversight Committee:
- Establish process for communicating SMS program findings and corrective actions to the Accountable Executive on a regular basis
- Establish means for tracking the effectiveness of any implemented corrective actions (mitigations for identified hazards)

D. Emergency Response Plan

Periodically train and drill all or part of the company on:
- Company mobilization and agencies notification
- Passenger and crew welfare intervention (immediate)
- Casualty and next of kin coordination
- Employee crisis reaction counseling (follow on)
- Accident investigation on behalf of the company
  - Cross discipline investigation group
  - Coordination with U. S. or foreign government investigation agencies

III. Hazard Information

A. Safety Oversight

Establish means for the Safety Department to gather and access tracking data for the whole company such that trends and profiles can be developed and monitored.
Establish standard means of distributing safety achievement and hazard tracking information to all operating groups in the company.

B. Hazard Information Reporting

Establish whole company “non-punitive” safety and hazard reporting mechanisms

Establish Event Review Committees appropriate for review of FOQA and ASAP programs or like programs for non-pilot employee groups.

Establish meaningful feedback mechanism for persons who submit ASAP or ASAP like reports.

Maintain trend analysis of hazard information systems.

Utilize level of information automation appropriate to the complexity of the company. (Avoid collecting information purely for the sake of collecting information)
Appendix 4 – SMS in Canada

Canadian SMS Requirements

In the late 1990s, Transport Canada, the Canadian regulatory authority, decided to make an SMS program mandatory for aviation companies. Since then, regulations have been passed in June 2005 requiring CAR 705 (FAR 121 equivalent) air operators and aviation maintenance organizations (AMOs) to have approved SMS programs. In addition, draft regulations have been consulted with stakeholders for airports, flight training units and the air traffic services provider (NavCanada) and are now going through legal processing and are expected to come into force by the end of 2006. The SMS requirement eventually will move to smaller air operators under CAR 704 (Commuter) and CAR 703 (Air Taxi). The planned date for these regulations’ implementation is also by the end of 2006.

The regulations make SMS mandatory. Transport Canada views this approach as a systematic, explicit and comprehensive process for managing risks to safety. The aim is to improve safety through proactive management. The regulations are aimed at:

- Increasing industry accountability by placing responsibility for “safety” with operational managers,
- Instilling a consistent and positive safety culture, and
- Improving the safety performance of aviation companies.

Transport Canada will be gradually changing its regulatory approach as SMS is implemented. Currently, Transport Canada is active at the operational level with audits and inspections of activities. The intent is to change the focus to the systems level. Inspectors will be assessing the effectiveness of safety management systems within organizations. However, Transport Canada states that their safety oversight program using risk-threat analysis will adjust priorities and resources as required to protect the travelling public.

Transport Canada’s SMS implementation plan allows for CAR 705 air operators and AMOs to implement SMS in four phases over a three year period ending on September 30, 2008 whereby these organizations will have to fully comply with all elements of the SMS regulation. Documentation and training are required for all of the phases. The requirements of each phase are as follows:

- **Phase 1**
  - Compliance document, gap analysis and project plan;
Phase 2
- Safety Management Plan to include safety policy, non-punitive reporting policy, roles, responsibilities and employee involvement, communication, safety planning, objectives and goals, performance management, and management review;
- Safety oversight through development and implementation of reactive processes, investigation and analysis, and risk management;

Phase 3
- Safety oversight through implementation of proactive processes;

Phase 4
- Operational quality assurance; and
- Emergency preparedness and response.

Critique

General

What is good about the new SMS regulations is the increased safety reporting and increased system knowledge that should result. ALPA was instrumental in having the critical elements of non-punitive reporting and employee involvement incorporated into the SMS regulations.

Heads of operating organizations will have clear responsibility and accountability for safety performance just as they now have for financial performance. We have already seen, in airlines that have started to implement SMS, improved relations between management and pilots, improved financial performance and improved relations with the regulator. Of continuing concern is that the specifics of how SMS is implemented are left to the operator as Transport Canada has adopted a performance-based, non-prescriptive approach to regulation. This is one of the reasons that ALPA has committed funds and time to training ALPA represented Canadian pilot groups on SMS so they are prepared to work effectively with company management and the regulator as each SMS program is developed on a property.

At the same time that Transport Canada is starting to apply SMS to industry, the regulatory agency is striving to establish a consistent approach to regulating under SMS by training its inspectors and producing an inspection guide for its staff. Additional guidance material is being produced to provide better information to operators on the development of an effective SMS program. The latest information on SMS in Canada can be obtained on Transport Canada’s website at:

Transport Canada and Enforcement

One benefit that already has resulted from the introduction of SMS is the new Transport Canada policy on enforcement. The policy came about as a result of work by ALPA pilot volunteers and staff. This new policy has already been used effectively for ALPA pilots and carriers in Canada and the United States. The innovative policy allows a company to conduct an internal safety investigation, when advised that a possible violation has occurred. This also is allowed if a pilot is informed of a possible violation. If the involved pilot and the company agree to the safety investigation process, Transport Canada will delay enforcement action until the safety investigation is complete and a report of follow up action received by Transport Canada. Based on the safety investigation, the company will take corrective action. If Transport Canada considers the company action satisfactory in responding to the event, then the regulatory file will be closed without punishment to the pilot or the company. The objective is to make meaningful, not cosmetic, safety improvements.

Problems

The effectiveness of inspector training to overcome the current, traditional regulatory mindset is an unknown at this point. This is a matter of concern, since the change in regulatory oversight approach and the ensuing benefits to industry are critical to the success of the overall program. Another critical component to improving safety is the sharing of safety information. As of yet, there has been no formal intent expressed by Transport Canada to require sharing of safety information between companies.