WORKING TOGETHER TO ENHANCE AIRPORT OPERATIONAL SAFETY

Ermenando Silva
APEX, in Safety Manager
ACI, World

ICAO-SRVSOP-ACI LAC Workshop on the Implementation of Operational and Compatibility Procedures in the Airport Certification Process (PANS Aerodromes)
June 12-16, 2017. Lima, Perú

Safety Management System

(SMS)

Safety management system (SMS)

An SMS is a system to **assure the safe operation of aircraft** through **effective management of safety risk.**

This system is designed to **continuously improve safety by identifying hazards, collecting and analysing data and continuously assessing safety risks**.

The SMS seeks to proactively **contain or mitigate risks before they result in aviation accidents and incidents**.

It is a system that is commensurate with the organization's regulatory obligations and **safety goals**.

SMS is necessary for an aviation organization to **identify hazards and manage safety risks** encountered during the delivery of its products or services.

Safety Management System (SMS)

An SMS includes key elements that are essential for hazard identification and safety risk management by ensuring that:

a) the necessary **information** is **available**;

b) the **appropriate tools are** available for the organization's use;

c) the **tools are appropriate to the task**;

d) the tools are commensurate with the **needs and constraints of the organization**; and

e) **decisions are made based on full consideration of the safety risk**.

SMS framework

Sms framework

Safety policies and objectives **create the frame of reference** for the SMS.

The objective of the safety risk management component is to **identify hazards, assess the related risks and develop appropriate mitigations** in the context of the delivery of the organization's products or services.

Safety assurance is accomplished **through ongoing processes that monitor compliance with international standards and national regulations**.

Furthermore, the safety assurance process provides **confidence that the SMS is operating as designed and is effective**.

Safety promotion provides the **necessary awareness and training**.

Safety risk management

Service providers should ensure that the safety risks encountered in **aviation activities are controlled in order to achieve their safety performance targets**.

This process is known as **safety risk management** and includes **hazard identification, safety risk assessment and the implementation of appropriate remediation measures**.

The safety risk management component systematically **identifies hazards that exist within the context of the delivery of its products or services**.

Hazards may be the result of **systems that are deficient in their design, technical function, human interface or interactions with other processes and systems**.

Safety risk management

Safety risk management encompasses the assessment and mitigation of safety risks.

The objective of safety risk management **is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations**.

Safety risk management is therefore a **key component of the safety management process at both the State and product/service provider level**.

Safety risks are conceptually assessed as acceptable, tolerable or intolerable.

Risks assessed as initially falling in the intolerable region are unacceptable under any circumstances.

The probability and/or severity of the consequences of the hazards are of such a magnitude, and the damaging potential of the hazard poses such a threat to safety, that **immediate mitigation action is required.**

Safety risk management

They may also result from a **failure of existing processes or systems to adapt to changes in the service provider's operating environment**.

Careful analysis of these factors during the planning, design and implementation phases can often identify potential hazards before the system becomes operational.

Understanding the system and its operating environment is also essential for achievement of high safety performance.

Hazards may be discovered during the operational life cycle, through employee reports or incident investigations. Analysis of these hazards should be conducted in the context of the system.

This context is key to avoiding attribution of events to —**human error where defects in the system may be neglected, remaining latent for future and potentially more serious events to occur.**

Hazard identification

The service provider shall **develop and maintain a formal process that ensures that hazards associated with its aviation products or services are identified**.

Hazard identification shall be based on a combination of **reactive, proactive and predictive methods** of safety data collection.

Hazards

Hazard identification is a **prerequisite to the safety risk management** process.

Any **incorrect differentiation between hazards and safety risks can be a source of confusion**.

A clear understanding of hazards and their related consequences is essential to the implementation of sound safety risk management.

Understanding hazards and consequences

A hazard is generically defined by safety practitioners as **a condition or an object with the potential to cause death, injuries to personnel, damage to equipment or structures, loss of material, or reduction of the ability to perform a prescribed function**.

For the purpose of aviation safety risk management, the term hazard should be focused on those **conditions which could cause or contribute to unsafe operation of aircraft or aviation safety-related equipment, products and services**.

Understanding hazards and consequences

Hazards are an inevitable part of aviation activities.

However, their manifestation and possible consequences can be addressed through **various mitigation strategies to contain the potential for a hazard to result in unsafe aircraft or aviation equipment operations**.

Hazard identification methodologies

The three methodologies for identifying hazards are:

a) Reactive.

This methodology involves analysis of **past outcomes or events**.

Hazards are identified through **investigation of safety occurrences**.

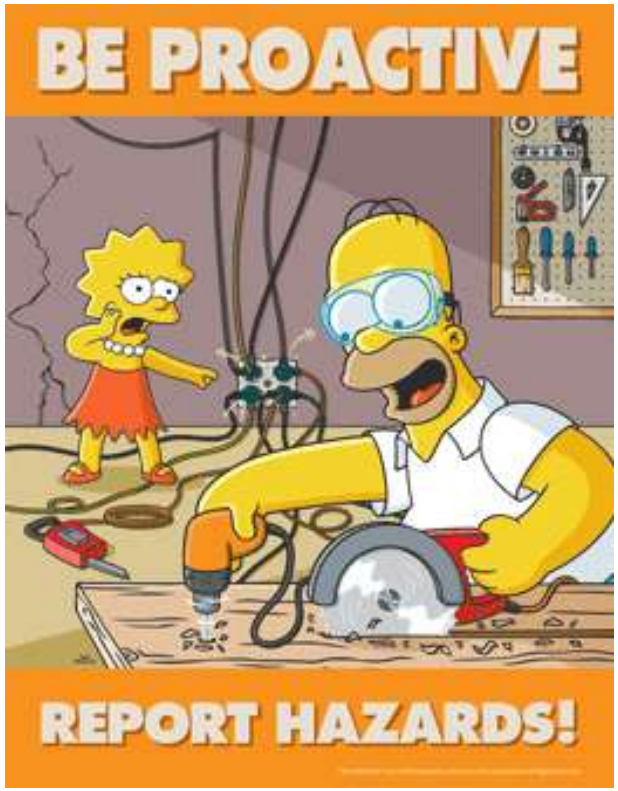
Incidents and accidents are clear indicators of system deficiencies and therefore can be used to determine the hazards that either contributed to the event or are latent.

Hazard identification methodologies

b) *Proactive*

This methodology involves analysis of existing or real-time situations, which is the primary job of the safety assurance function with its audits, evaluations, employee reporting, and associated analysis and assessment processes.

(This involves actively seeking hazards in the existing processes).



c) *Predictive*

This methodology involves **data gathering in order to identify possible negative future outcomes or events**, analysing system processes and the environment to **identify potential future hazards and initiating mitigating actions.**

Safety risk

Safety risk management is another key component of a safety management system.

The term **safety risk management is meant to differentiate this function from the management of financial risk, legal risk, economic risk** and so forth.

The fundamentals of safety risk and includes the following topics:

a) a definition of safety risk;

b) safety risk probability;

c) safety risk severity;

d) safety risk tolerability; and

e) safety risk management.

Safety risk

Definition of safety risk

Safety risk is the ***projected likelihood and severity of the consequence or outcome from an existing hazard or situation****.*

*While the outcome may be an accident, a intermediate unsafe event/consequence may be identified as —****the most credible outcome****.*

Provision for identification of such layered consequences is usually associated with more sophisticated risk mitigation software*.*

Safety risk probability

The process of controlling safety risks starts by **assessing the probability that the consequences of hazards will materialize during aviation activities** performed by the organization.

Safety risk probability is defined as **the likelihood or frequency that a safety consequence or outcome might occur**.

Likelihood	*Meaning*	*Value*
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

Figure 2-11. Safety risk probability table

Safety risk probability

The determination of likelihood can be aided by questions such as:

a) Is there a **history of occurrences** similar to the one under consideration, or is this an isolated occurrence?

b) What **other equipment or components** of the same type might have similar defects?

c) How many personnel are following, or are subject to, the **procedures in question**?

d) What **percentage of the time** is the suspect equipment or the questionable procedure in use?

e) To what extent are there **organizational, managerial or regulatory implications** that might reflect larger threats to public safety?

Safety risk severity

Once the probability assessment has been completed, the **next step is to assess the safety risk severity, taking into account the potential consequences related to the hazard**.

Safety risk severity is defined as **the extent of harm that might reasonably occur as a consequence or outcome of the identified hazard**.

Safety risk severity

The severity assessment can be based upon:

a) ***Fatalities/injury***. How many lives may be lost (employees, passengers, bystanders and the general public)?

b) ***Damage.*** What is the likely extent of aircraft, property or equipment damage?

The severity assessment **should consider all possible consequences** related to an unsafe condition or object, taking into account the worst foreseeable situation.

Safety risk tolerability

The safety risk probability and severity assessment process can be used to derive a **safety risk index**.

The index created through the methodology consists of an **alphanumeric designator, indicating the combined results of the probability and severity assessments**.

The third step in the process is to **determine safety risk tolerability**.

First, it is necessary to **obtain the indices in the safety risk assessment matrix**.

Severity	*Meaning*	*Value*
Catastrophic	— Equipment destroyed — Multiple deaths	A
Hazardous	— A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely — Serious injury — Major equipment damage	B
Major	— A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency — Serious incident — Injury to persons	C
Minor	— Nuisance — Operating limitations — Use of emergency procedures — Minor incident	D
Negligible	— Few consequences	E

Figure 2-12. Safety risk severity table

Safety risk probability X safety risk severity

For example, consider a situation where a safety risk probability has been assessed as occasional (4), and safety risk severity has been assessed as hazardous (B).

The composite of probability and severity (4B) is the safety risk index of the consequence.

Risk probability		Risk severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Figure 2-13. Safety risk assessment matrix

Safety risk matrix

The index obtained from the safety risk assessment matrix must then be exported to a **safety risk tolerability matrix that describes the tolerability criteria for the particular organization**.

Using the previous example, the criterion for safety risk assessed as 4B falls in the —**unacceptable under the existing circumstances category**. In this case, the **safety risk index of the consequence is unacceptable**.

The organization must therefore:

a) **take measures to reduce the organization's exposure to the particular risk**, i.e. reduce the likelihood component of the risk index;

b) **take measures to reduce the severity of consequences related to the hazard**, i.e. reduce the severity component of the risk index; or

c) **cancel the operation if mitigation is not possible**.

Safety Risk Tolerability

Safety risks assessed in the tolerable region are acceptable provided that appropriate mitigation strategies are implemented by the organization.

A safety risk initially assessed as intolerable **may be mitigated and subsequently moved into the tolerable region provided that such risks remain controlled by appropriate mitigation strategies**.

In both cases, a **supplementary cost-benefit analysis may be performed if deemed appropriate**.

Safety risks assessed as initially falling in the acceptable region **are acceptable as they currently stand and require no action to bring or keep the probability and/or severity of the consequences of hazards under organizational control**.

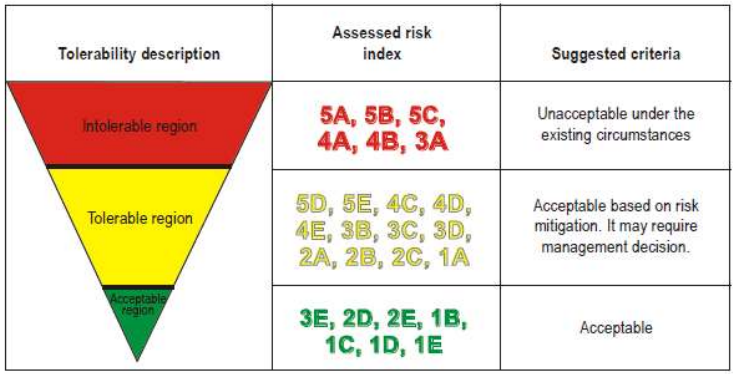


Figure 2-14. Safety risk tolerability matrix

Risk management documentation

Each risk mitigation exercise will **need to be documented as necessary.**

This may be done on a basic spreadsheet or table for risk mitigation involving non-complex operations, processes or systems.

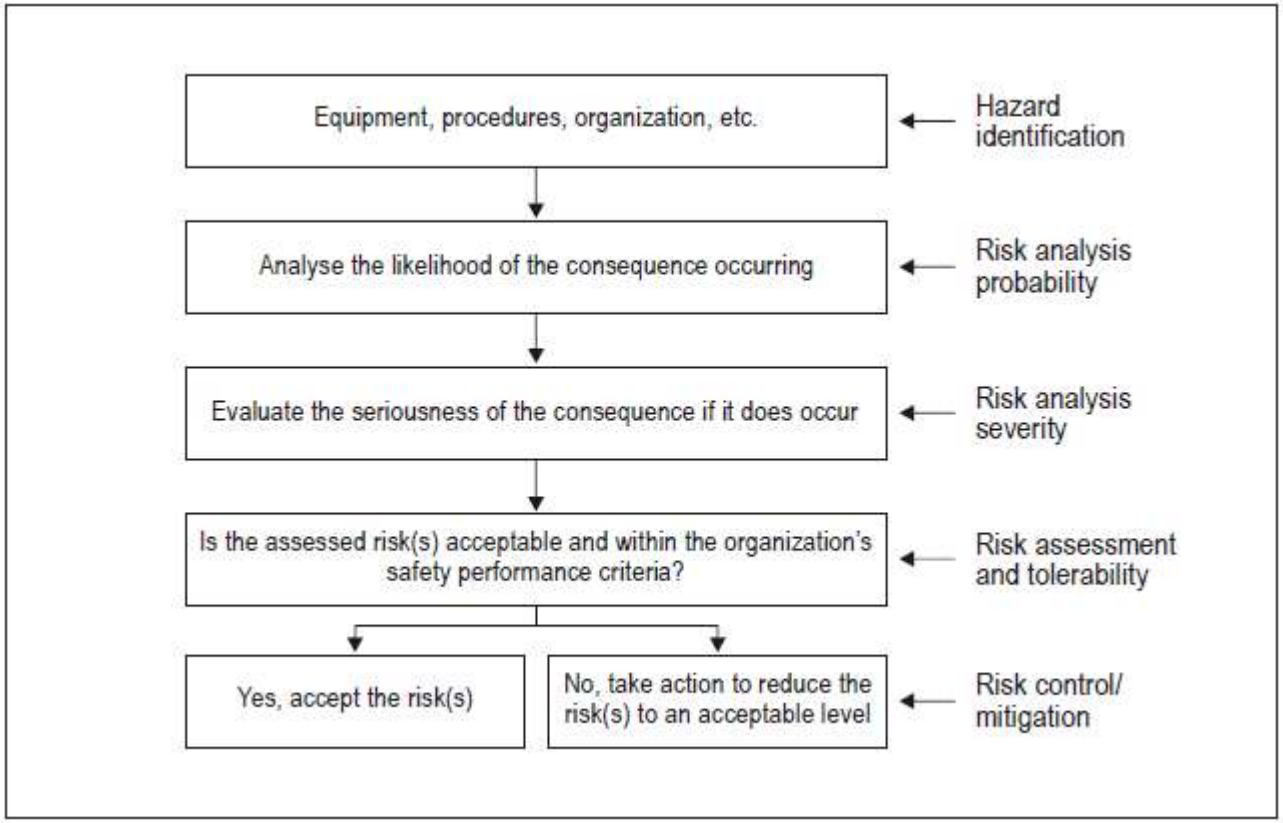
For hazard identification and risk mitigation involving complex processes systems or operations**, it may be necessary to utilize customized risk mitigation software to facilitate the documentation process**.

Completed risk mitigation documents should be approved by the appropriate level of management.

Risk index range	Description	Recommended action
5A, 5B, 5C, 4A, 4B, 3A	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Low risk	Acceptable as is. No further risk mitigation required.

Figure 2-15 An alternate safety risk tolerability matrix

Risk management process



Baseline and equivalent level of safety

The safety performance outcome from the introduction of performance-based elements within or supplementary to an SMS framework **should not be worse than that of an existing**, purely prescriptive regulatory framework.

To assess or monitor that such —equivalence is indeed the case, **there should be safety indicators to monitor the overall outcome of events** (non-conformance occurrences) of the system/process concerned for which the performance-based element will be introduced.

Baseline and equivalent level of safety

By such a comparison process, the pre-implementation —**baselinell performance can be verified against post-implementation performance, to see if an —equivalent level of performance has been maintained**.

If the post-implementation performance turns out to be better, then a —better level of performance has in fact been manifested.

Where there is a degradation of the system's performance, the service provider should work in conjunction with the regulator to verify the causal factors and take actions as appropriate, which may include modification of the performance-based requirement itself or, where necessary, restoration of basic prescriptive requirements.

Safety Risk Mitigation

If the safety risks are assessed as intolerable, the following questions become relevant:

a) **Can the hazards and related safety risk(s) be eliminated**? If the answer is yes, then action as appropriate is taken and documented. If the answer is no, the next question is:

b) ***Can the safety risk(s) be mitigated?*** If the answer is no, related activities must be cancelled. If the answer is yes, mitigation action as appropriate is taken and the next question is:

c) ***Do any residual safety risks exist?*** If the answer is yes, then the residual risks must be assessed to determine their level of tolerability as well as whether they can be eliminated or mitigated as necessary to ensure an acceptable level of safety performance.

Safety Risk Mitigation

The three generic safety risk mitigation approaches include:

a) ***Avoidance.*** The activity is suspended either because the associated safety risks are intolerable or deemed unacceptable vis-à-vis the associated benefits.

b) ***Reduction***. Some safety risk exposure is accepted, although the severity or probability associated with the risks are lessened, possibly by measures that mitigate the related consequences.

c) ***Segregation of exposure***. Action is taken to isolate the potential consequences related to the hazard or to establish multiple layers of defences to protect against them.

Safety Risk Mitigation

It is important to consider the full range of possible control measures to find an optimal solution.

The effectiveness of each alternative strategy must be evaluated before a decision can be taken.

Each proposed safety risk mitigation alternative should be examined from the following perspectives:

a) Effectiveness. The extent to which the alternatives reduce or eliminate the safety risks. Effectiveness can be determined in terms of the technical, training and regulatory defences that can reduce or eliminate safety risks.

b) ***Cost/benefit.*** The extent to which the perceived benefits of the mitigation outweigh the costs.

Safety Risk Mitigation

c) ***Practicality***. The extent to which mitigation can be implemented and how appropriate it is in terms of available technology, financial and administrative resources, legislation and regulations, political will, etc.

d) ***Acceptability.*** The extent to which the alternative is consistent with stakeholder paradigms.

e) ***Enforceability***. The extent to which compliance with new rules, regulations or operating procedures can be monitored.

Safety Risk Mitigation

f) ***Durability***. The extent to which the mitigation will be sustainable and effective.

g) ***Residual safety risks***. The degree of safety risk that remains subsequent to the implementation of the initial mitigation and which may necessitate additional risk control measures.

h) ***Unintended consequences.*** The introduction of new hazards and related safety risks associated with the implementation of any mitigation alternative.

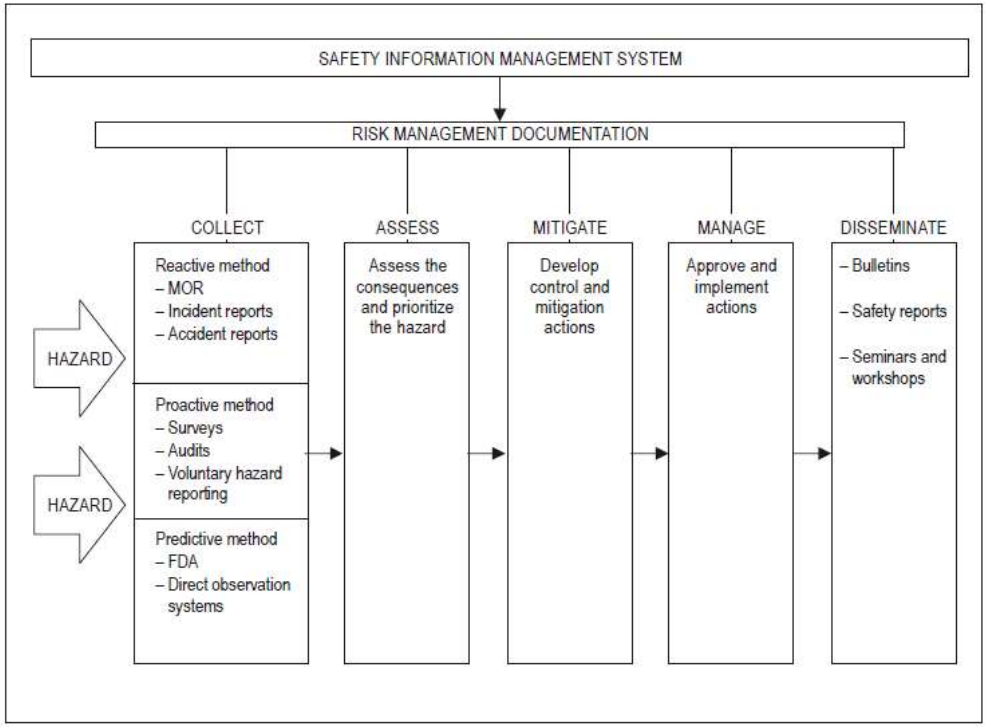
Safety Risk Mitigation

Once the mitigation has been approved and implemented, any associated impact on safety performance **provides feedback to the service provider's safety assurance process**.

This is **necessary to ensure the integrity, efficiency and effectiveness of the defences under the new operational conditions**.

Each risk mitigation exercise is to be **documented progressively.**

Completed risk mitigation documents should be approved by the appropriate level of management.



WWW.ACI.AERO/APEX

THANK YOU!