SAFETY MANAGEMENT
INTERNATIONAL COLLABORATION GROUP

Risk Based Decision Making Principles

30 January 2013

This paper was prepared by the Standardization Workgroup of the Safety Management International Collaboration Group (SM ICG). The purpose of the SM ICG is to promote a common understanding of Safety Management System (SMS)/State Safety Program (SSP) principles and requirements, facilitating their application across the international aviation community.

The current core membership of the SM ICG includes the Aviation Safety and Security Agency (AESA) of Spain, the National Civil Aviation Agency (ANAC) of Brazil, the Civil Aviation Authority of the Netherlands (CAA NL), the Civil Aviation Authority of New Zealand, the Civil Aviation Safety Authority (CASA) of Australia, the Direction Générale de l'Aviation Civile (DGAC) in France, the European Aviation Safety Agency (EASA), the Federal Office of Civil Aviation (FOCA) of Switzerland, Japan Civil Aviation Bureau (JCAB), the United States Federal Aviation Administration (FAA) Aviation Safety Organization, Transport Canada Civil Aviation (TCCA) and the Civil Aviation Authority of United Kingdom (UK CAA). Additionally, the International Civil Aviation Organization (ICAO) is an observer to this group.

Members of the SM ICG:

- Collaborate on common SMS/SSP topics of interest
- Share lessons learned
- Encourage the progression of a harmonized SMS
- Share products with the aviation community
- Collaborate with international organizations such as ICAO and civil aviation authorities that have implemented or are implementing SMS

For further information regarding the SM ICG please contact:

Regine Hamelijnck
EASA
+49 221 8999 1000
regine.hamelijnck@easa.europa.eu

Jacqueline Booth
TCCA
(613) 952-7974
jacqueline.booth@tc.gc.ca

Amer M. Younossi
FAA, Aviation Safety
(202) 267-5164
Amer.M.Younossi@faa.gov

Carlos Eduardo Pellegrino
ANAC
+55 213 5015 147
carlos.pellegrino@anac.gov.br

Peter Boyd
CASA
+61 2 6217 1534
peter.boyd@casa.gov.au

EXECUTIVE SUMMARY

This document introduces the principles necessary for effective risk based decision making. It also identifies the pertinent data attributes necessary to enable data utilization to make risk based decisions, and presents considerations for data management.

Safety management is becoming the standard for aviation safety worldwide. Risk management is one of the main components of safety management and the key elements for an effective risk management process are the identification of hazards, assessment of the risks associated with the consequences of these hazards, and the mitigation of the risks considered unacceptable. Service providers and regulatory authorities both have roles in aviation risk management. They both need to manage risk, although the nature and scope of the hazards and processes may be different. For example, while a service provider may identify hazards specific to their unique organization, an authority may be identifying hazards from emerging trends across an entire aviation system based on aggregate data from multiple sectors.

Well-functioning safety management processes, whether established under a Safety Management System (SMS) or a State Safety Programme (SSP), require data to support analyses and assessments, as well as strategies to guarantee that these data possess certain attributes, such as data validity, completeness, timeliness, availability, and accuracy. Additionally, since safety management is a data-driven system, it is dependent on an effective data management process. Data management is the continuous development and maintenance of processes and procedures to assure that an organization has the data it needs and that data is organized, reliable and appropriate. Establishing data attribute requirements and a data management plan will enable effective hazard identification and risk mitigation.

Hazard identification should be used during system design and system change processes; and hazards should continue to be identified via continuous monitoring during system operation. During hazard identification, all possible sources of hazards should be considered. The risk associated with the potential outcomes for each particular hazard should be assessed or analyzed, in which each risk is the product of severity and probability. Thereafter, the risks that are considered unacceptable by the organization should be mitigated.

This document provides an overview of risk based decision making, data attributes, data management, and elements of safety risk management. The final Chapter of this document contains examples of existing data collection, hazard identification, and analysis processes from Safety Management International Collaboration Group (SM ICG) member authorities.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to introduce principles that are necessary for an effective risk based decision making process. This includes pertinent data attributes necessary to enable data utilization to make risk-based decisions, and the overall management of this data. This document is intended to be used by authorities and service providers that are in the initial stages of safety management development/implementation processes. This document only introduces basic principles; therefore, use of additional sources in conjunction is recommended.

2. INTRODUCTION

Safety management is becoming the standard for aviation safety worldwide. It is a tool that assists managers to make decisions based on the risks that exist in their organizations or in their environments. Risk management is one of the main components of safety management as it encompasses the assessment and mitigation of safety risks, to which organizations are exposed.

Service providers and authorities have roles in aviation risk management; they both need to manage risk, although the nature and scope of the hazards and processes may be different. For example, while a service provider may identify hazards specific to its unique organization, an authority may be identifying hazards from emerging trends across an entire aviation system based on aggregate data from multiple sectors.

The key elements for a risk management process are: identification of hazards, assessment of the risks associated with the consequences of these hazards, and the mitigation of the risks considered unacceptable. All these elements require data to support effective risk management. Consequently, proper management of data throughout the risk management lifecycle is essential to support a robust safety management process.

This document begins with a discussion of general data utilization concepts. Then it provides further details regarding data attributes, data management, hazard identification, risk analysis, and risk mitigation processes. Finally, it offers examples of existing authorities' data collection, hazard identification and analysis methods.

The level of complexity and sophistication of an organization's safety management process and/or safety management tool will vary based on the size, maturity, and complexity of a given aviation sector within a particular State or industry organization. As such, the principles contained in this document are intended to be achieved with a safety management implementation that is scaled to a particular aviation sector or service provider's size, maturity, and complexity. For example, for relatively small and/or simple aviation sectors, it may be acceptable to perform risk management using manual data collection, analysis, and storage, rather than complex Information Technology (IT) tools.

3. RISK BASED DECISION MAKING OVERVIEW

The primary goal of risk management is to leverage safety-related data to identify and control the potential consequences of hazards in the aviation system before an accident or serious incident occurs. Risk management becomes much more effective with classification of safety data using common taxonomies that allow the data to be viewed in more dimensions to detect hazards more efficiently. Data analysis may include inputs from any aviation safety related data from one or more aviation sectors, so it is important to use common taxonomies. The outputs of the data analysis process are risk management options. Figure 1 depicts examples of the types of inputs and outputs.

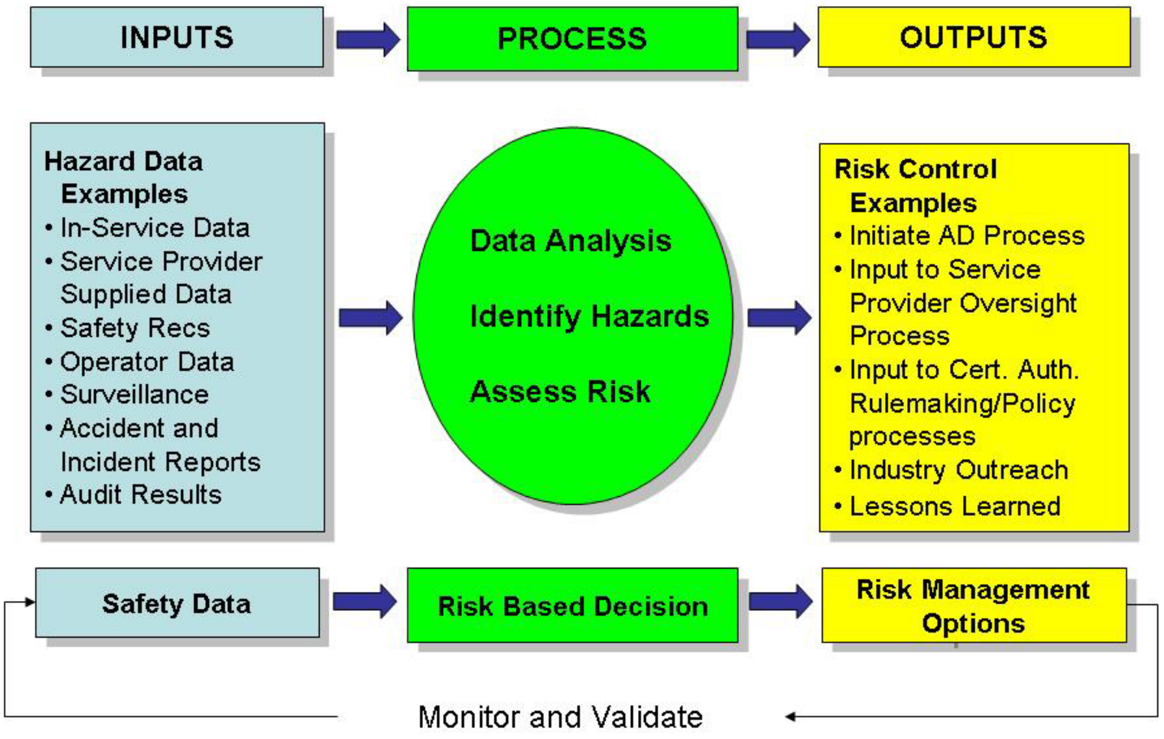

Figure 1: Data Analysis Process Inputs and Outputs

As mentioned earlier, inputs can come from any part of the aviation system, including hazard analysis of new processes or products, surveillance of existing aviation systems, in-service events, accident/incident investigations, voluntary reporting systems, etc. When necessary, outputs or risk controls are applied to eliminate the hazard or reduce the level of risk.

Effective hazard identification is dependent on the availability of data. Even if hazard analysis is performed on new processes or products not yet in operation, data describing the process or product is required. Also, data should be managed and the necessary data attributes should be addressed. In addition, it may be appropriate to combine or aggregate data from multiple aviation sectors to ensure a comprehensive understanding of each identified hazard. Chapters 4 and 5 of this document provide additional information regarding data attributes and data management.

Furthermore, the process depicted in Figure 1 should utilize reactive, proactive, and predictive methodologies to identify hazards. Analyzing the hazards identified as a result of incident or accident investigations is an example of a reactive methodology. A proactive one might include evaluating risks after audits, inspections, or mandatory reports, while a predictive methodology could involve considering the results of system vulnerability analysis of operation on a day-by-day basis. Chapters 6, 7, and 8 of this document provide additional information regarding the identification of hazards, risk analysis, and risk mitigation.

4. DATA ATTRIBUTES

Well-functioning safety management processes, whether established under an SMS or SSP, require data. This chapter briefly examines data attributes that should be considered during system design, data collection, analysis, and dissemination processes.

Before discussing data attributes, one should consider that safety data can be broadly classified into several categories: reportable occurrence data, voluntary occurrence data, observation data, and surveillance data. Reportable data are required to be submitted by regulations. This includes data acquired from investigation of accidents and serious incidents as well as certain technical occurrences. While not required by regulations, voluntary data are reported in order to assist in identifying hazards and includes reports on incidents and errors. Observation can be used to identify hazards by observing outliers[1] from normal operations. It includes programs such as Flight Data Monitoring and Flight Operational Quality Assurance. Surveillance data come from audits, surveys or inspections that check conformance with specific requirements. All categories of data are important elements of a well-functioning safety management process.

Regardless of the type of data, quality is one of the most important elements in ensuring that the data can be integrated and used properly for analysis purposes. It is important that data quality principles and practices are applied throughout the processes from data capture and integration to analysis. Some of the most important data attributes are: validity, completeness, timeliness, availability, and accuracy.

Data Validity

Data validity is not only as important as any other data attribute; it may be more so. The results of a given analysis are only as valid as the validity of the input data feeding the analysis. Without valid data, all analysis results, trends identified, and conclusions made may be incorrect and potentially misleading. Data validity refers to the correctness and reasonableness of data, as well as ensuring that data collected is measuring what was intended. This means that the data includes all necessary digits and correct spelling. For example, dates have a valid day, month and year, and not have 32 days or 13 months.

Data validity errors are usually caused by incorrect data entry, when a large volume of data is entered into a database or when different databases with distinct data structures are merged. In order to reduce data validity errors, simple field validation techniques could be adopted. For example, if the date field in a database uses the MM/DD/YYYY format, then a program with the following two data validation rules could be used: “MM” should not exceed “12” and “DD” should not exceed “31”. This method is often referred to as a data reasonableness check.

Data Completeness

Completeness is a measure of how much data is available compared to how much data is needed for a particular analysis. Prior to developing a new analysis process that supports risk based decision making, the minimum data required should be defined. It should be noted that the larger the volume of data that is needed, the more resources (e.g.. time, manpower) will be required to obtain the data. This is something that has to be taken into serious consideration when designing data collection systems. Requirements for completeness should also be commensurate with the information available. For example, the amount of data on an accident is likely to be much greater than that for a minor incident.

[1] An outlier is an observation that lies outside the overall pattern of a distribution. It can be an indication of an area of concern or of a data error; but in any case requiring further examination.

Data Timeliness

Although timeliness is specified by user expectations, the best data is typically the most recent. Historically, technology and process limitations tended to preclude the possibility of delivering real-time data. However, with the advent of computers and network technology, barriers to real-time availability of data continue to fall. As a result, in its safety management processes an organization should strive to obtain real-time access to aviation safety data, to the greatest extent possible. For example, current systems for wireless downloading of flight data monitoring (FDM) data allow operators an almost real-time access to data.

Data Availability

Data should also continue to be available when needed. In general, data availability is achieved through redundancy involving where the data is stored and how it can be reached. Data availability can be measured in terms of how often the data is available (e.g., 99.9% availability) and how much data can flow at a time.

Data Accuracy

Data accuracy is the degree to which data correctly reflects the real world object or an event being described. There are several sources and causes of data inaccuracy. The most common of these is initial data entry, in which either the user enters the wrong value or typographical errors are committed. This can be overcome by ensuring that persons entering the data possess the skills necessary and are adequately trained. Data inaccuracy from data entry can also be overcome by having programmatic components in the application to detect typographical errors (e.g., spelling checks) or other methods to ensure data accuracy, including offering lists of possible values.

In summary, each data attribute should be addressed. In some cases, addressing each aspect may require considerable effort. An organization’s confidence in data is not something that is achieved using one attribute. Instead, data confidence is a stratified concept – achieved one layer at a time. Every time another layer is added, the data confidence factor increases. Additionally, all these attributes should be considered at the outset of designing a process or system because once the process or system is fielded it may be too late to obtain the data needed to allow management to make decisions based on data.

5. DATA MANAGEMENT

Safety management is a data-driven system, thus it depends on an effective data management process. Data Management is the continuous development and maintenance of processes and procedures to assure that an organization has the data it needs and that data is organized, reliable, and appropriate. When managing data, an organization should define what information is necessary and plan how it will be utilized within its processes.

For effective safety data management, an organization should:

- Define the data required in order to accomplish desired objectives;
- Design data architectures and database structures, based on the intended use of the data;
- Define the standards and formats for the data, including required frequency for data collection;
- Develop a process to assure collected data adheres to the defined standards and formats;
- Develop data collection tools, considering the necessity of the data to be collected and its use;
- Define data to be aggregated from multiple sources;
- Integrate safety data to other correlated data that may be relevant;
- Assure adequate data access for the users;

- Consider data protection issues;
- Consider data sharing with entities within and outside the organization; and
- Manage data during its entire life-cycle, including configuration control.

This chapter presents some of the main aspects of data management that should be considered to effectively use data for safety management.

Data Collection Planning

Prior to collecting data, an organization (authority or service provider) should identify what information is needed. For example, authorities or service providers usually possess detailed data regarding accidents and serious incidents. However, they may not possess data about all safety occurrences in their system. Consequently, to obtain this knowledge, the organization needs to develop a plan for collecting such data.

After identifying the data to be collected, the organization should determine the source of the information as well as the collection and storage processes. For example, will the system be open to the general public, crew members, service providers, etc.? In order to answer this, it is necessary to consider the data attributes discussed in Chapter 4 and determine if the source will be capable of providing that level of detail.

Data Standardization

Standardization of the content impacts directly the utilization of data. Thus, it is necessary to standardize the data in order to compare, aggregate, and combine data from different sources. To be able to link data from different sources, it is necessary to develop and maintain standards for common taxonomies or be able to convert or translate between different taxonomies. Taxonomies allow data to be identified and stored using the same nomenclature. For example an aircraft type can be recorded as “737-200” or “Boeing 737-200” or “732”. Some examples of standards are described below:

- Aircraft model: The organization can build a database with all models certified to operate.
- Airport: The organization may use International Civil Aviation Organization (ICAO) or International Air Transport Association (IATA) codes to identify the airports.
- Type of occurrence: The accident investigation organization may use taxonomies developed by ICAO and other international organizations to classify the occurrences.

Due to legacy issues as well as other factors, sometimes common taxonomies might not be in place between various databases. In such a case, data mapping should be created to allow the standardization of data based on equivalency. Using the aircraft type example above, a mapping of the data could show that a “737-200” in one database is equivalent with a “732” in another. In some cases, this may not be a straightforward process as the level of detail during data capture may differ. When the use of a common taxonomy is not feasible due to high data heterogeneity, other forms of data integration should be considered.

If a new standard is being created, the organization may have to consider both internal and external sources for developing the necessary standards.

Data Structure and Format

Once the organization has decided on the processes that will be utilized to collect data, the next step is to define the structure of the data to be collected. It will also be necessary to consider where the data will reside. If the data is being combined with existing databases, then the same structure of the data already collected will need to be used. For example, if an existing database contains detailed information on flight hours, crewmembers, aircraft, airports and others, combining it with a new database will require data fields with the same formats of the existing database, in order to effectively integrate this information. Every common field between the systems should have the same format. For example, a “date” field would be the same in each system (e.g., "MM/DD/YYYY"). Another possible strategy for allowing combination of data with different structures or formats is the use of data transformation. This strategy can be applied when data from different sources are equivalent. Once the data becomes transformed, then the data will be interchangeable and analysis encompassing different databases will be possible.

Data Collection Tools

Once the sources, content, formats and standards are defined, it is necessary to build the proper tools to collect the data. At this point, it is very important to consider the following attributes:

- **Ease of access**: The reporting system should be available in a place easy to find and to access (e.g., large link at the top of the main page of an organization’s website). The access should block unauthorized persons, but should be easy to access by the intended users. For instance, a crew member (intended user) should access through his/her pilot’s license number and a password, which would be the same password used to access other organizational systems.

- **Ease of reporting**: When filling out the report, the user should spend the minimum effort as possible to enter the information. For example, the data and hour fields should auto-populate by clicking the options on a calendar.

- **Absence of redundant information**: Ensure that information that is already available to the organization is not being collected again. For example, if the organization already has a database containing information on crew personnel, it should be adequate to query only by pilot license numbers.

- **Controlling input:** Format restrictions can be designed so that information is obtained in the desired format. For example, if a time is entered as "0954," the system would format according to the defined structure, which is the same as "09:54 am."

These are just some of the considerations that should be taken into account while designing data collection tools. Also, note that data collection tools can be paper-based or computer-based, depending on the type and the amount of data being collected.

Data Storage and Database Maintenance

Once the data has been collected, then it should be stored in what is sometimes commonly referred to as a “safety library.” Some of the considerations for data storage are to ensure that adequate storage capacity exists for the data being collected. It may also be necessary to update or dispose of certain data after a certain period. Furthermore, the database that contains this data should be maintained to ensure that the valid and reliable data is available when needed. The storage plan should also address the need for redundant storage sites to ensure data availability.

Data Access and Availability

The data needs of database users should be identified, as well as the necessary tools required to access the data. In addition, the need for restricting access should be evaluated, and periodically reviewed. The data management plan should also consider data management responsibilities throughout the organization, such as controlling access to stored data, determining adequate bandwidth to support the volume of intended users, and determining adequate redundancy.

Data Protection Guidance

Data protection principles apply to all types of safety data. Even accident report data, which is publicly available, has some data protected such as the names of crewmembers or other information that may directly identify them. For voluntary data, the protection might be even higher as the aim is not only to protect direct identification of reporting individuals but also to encourage the reporting. Nevertheless, the protection of data and the safety benefits it may bring is closely related to local/national laws and State/service provider safety culture, which may encourage or inhibit reporting.

A cornerstone of safety management is the understanding that most voluntary data that is provided to a regulatory authority should be kept confidential and the identity of reporting individuals will remain anonymous, as allowed by law. If non-punitive voluntary data reporting agreements are not allowed by law and regulated as part of the certification/authorization process, States should consider proposing changes to the laws or regulations to allow for this proven data sharing concept.

Another important issue to be addressed is the authority/service provider policy for use of the safety information. An excessive or disproportionate protection of safety data can adversely affect the availability of data needed to perform safety management and may limit the authority's/service provider's ability to utilize this data effectively. Thus, efforts to ensure the protection of safety information should strike a very delicate balance of interests between the need to protect safety information, and the responsibility to administer justice. The policy should include guidance regarding the responsibility of the custodian of safety information and the rules concerning disclosure of the information. Legislation covering the access to information by non-aviation entities should always be taken into consideration when identifying what data will be collected as well as the procedures and conditions under which the data will be disseminated.

Data protection and trusting that such protection is effective can be achieved through various means. One potential method would be to have a third-party collect the data. This can be an independent part of the organization. Another method that has been used successfully is to establish a neutral third party to collect, de-identify, aggregate, and process the service provider data prior to making it available to the industry group or regulatory authority. In this manner, the neutral third party provides a protective barrier, thus ensuring data confidentiality. In some cases, this method may include the disadvantage that the third-party may lack the expertise to validate and analyze the data for aviation safety purposes.

In summary, any data protection process should be based on negotiated formal agreements that, at a minimum address:

- **Anonymity:** Provides that any identifiable data necessary during the analysis process will be eliminated permanently at the earliest possible time, in accordance with the associated data protection agreement.

- **Data access and control:** Identifies data that require protection and assigns overall responsibility for data protection. In addition, data access and control provides guidelines and procedures to protect data; provides authorized access to data, data processing and storage locations; provides authorized access to reports and other data outputs; and requires the destruction of data after the retention period has expired.

- **Data analysis facilities:** Provides secure, controlled access facilities for all systems, offices, equipment, workstations, computers, and peripherals associated with the data analysis program. Secure systems should also be provided for storage of all data analysis-related materials, including paper, media, and backup devices.

Safety Data Sharing

Since the aviation system is composed of many stakeholders that interact and affect the entire aviation product lifecycle, safety data analysis should be performed in an integrated manner. Safety management best practices encourage service providers to share de-identified aggregated information with the authority, so that the regulatory authorities can monitor trends in the aviation system (by sector or as a whole) and target its resources to address areas of highest risk.

Before determining what data should be shared and the related security issues, it is important to address common taxonomies. Data sharing requires that all information sources provide data with similar fields and taxonomies or be transformed to provide for this commonality. This topic was discussed earlier in the *Data Standardization* section of this chapter.

Data Integration/Fusion

Tools available today allow for the integration of data and synthesis of new databases with enriched data from a collection of existing databases. Technology has overcome impediments to the integration of databases with systems, which enable links between aviation data bases (e.g., airport weather data, de-identified aggregate flight information) without revealing protected information (e.g., flight numbers, airlines, pilot identities).

Additionally, regulatory authorities should advance data sharing, beyond the capability of any single aviation sector, by aggregating and integrating data. Atypical events, abnormalities, and exceedances may become apparent in computer graphics generated from the integration of data. Flight paths retraced from aircraft data and radar-track data, for example, may enable an analyst to notice which flights are significantly different from the rest. Then subject matter experts should investigate the differences and better understand the reason for such an occurrence.

Figure 2 illustrates the concept of data integration. In this example, flight safety around airports can be examined by combining, or integrating, data from many different sources. This picture is an integration of digital terrain data around an airport and aircraft flight tracks (blue line) approaching and leaving the airport.

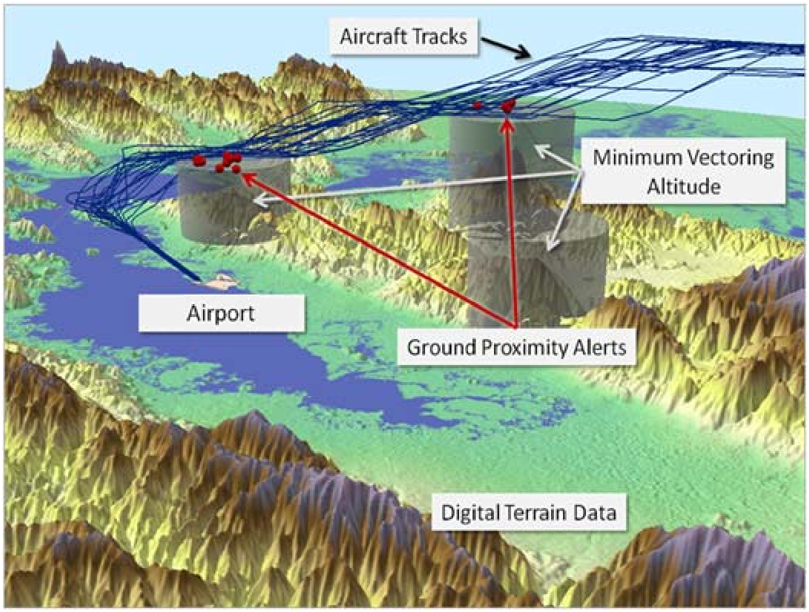

Figure 2: Data Integration Example

Other Data Considerations

Additional considerations regarding safety data that should be taken into account when establishing a well-functioning risk management process are: data security, data integrity, and data decay. Data security means ensuring that the data is secure and protected from any loss. Although this is an important subject, it goes beyond the scope of this document.

Consideration should be given to how safety data is handled, processed, and communicated within the aviation system, and means should be incorporated to maintain data integrity. Data corruption introduced by human error, hardware failure, and software processing errors can compromise data integrity and lead to invalid data and analysis results. Ideally, end-to-end integrity checks —such as using a cyclic redundancy check (CRC), or other equivalent assurance techniques— should be used to identify data corruption that may occur along the data handling/processing paths.

Furthermore, data decay can lead to inaccurate data. Many data values which are accurate can become inaccurate through time (i.e., data decay). For example, aircraft registration and aircraft type certificate holder information, and number of aircraft operated by a carrier can change over time. If not updated, the data decays into inaccuracy. Finally, in some cases fully satisfying one requirement may significantly jeopardize another. For example, data protection reduces the data reliability; and when taken to extremes, it can make data quality checks almost impossible.

In summary, Chapters 4 and 5 of this document discuss the importance of data attributes and management of data. The next chapters discuss using this data to identify hazards and in the risk management process.

6. HAZARD IDENTIFICATION

The Safety Management International Collaboration Group (SM ICG) defines a hazard as *a condition that could cause or contribute to an aircraft incident or accident*. During the hazard identification phase, the authority or service provider safety analyst[2] analyzes data to identify and document potential hazards as well as corresponding effects or consequences. The level of detail required in the hazard identification process depends on the complexity of the aviation process being considered.

Considerations for Hazard Identification

To ensure effective hazard identification, several elements should be considered. First, a systematic process to identify hazards in the system should be developed. There are numerous methods to be utilized; however, all include the following three elements:

a) Safety analysts should possess technical and/or managerial expertise.
b) Safety analysts should be trained or be experienced in various hazard analysis techniques.
c) A defined hazard analysis tool(s) should exist or be developed.

Second, the safety analyst should identify the data sources necessary to identify hazards. Finally, the safety analyst should select a technique or tool that is most appropriate for data available and the type of aviation system being evaluated.

[2] Safety analyst in the context of this document does not necessarily mean an expert in data analysis. An analyst could be an expert in a particular aviation sector or a safety panel consisting of a group of safety analysts or experts. It is generally good practice to minimize single point safety critical decision making with thorough review by a technically diverse group.

Potential Sources of Hazards

During hazard identification, all possible sources of hazards should be considered. Depending on the nature and size of the system under consideration, these can include:

a) Airborne or ground equipment (hardware and software);
b) Operating environment (including environmental conditions, airport infrastructure deficiencies, airspace, airport design and air route design);
c) Human performance;
d) Human-machine interface;
e) Operational procedures;
f) Maintenance procedures;
g) External interfaces (e.g., outsourced services);
h) Organizational procedures; and
i) Organizational change.

Hazard Identification Triggers

There are different instances for using the hazard identification process. Some of the major ones are:

- **System Design:** Hazard identification starts before the beginning of operations with a detailed description of the particular aviation system and its environment. The safety analyst then identifies the various potential hazards associated with the system as well as impacts to other interfacing systems.

- **System Change:** Hazard identification starts before introducing a change in the system (operational or organizational) and includes a detailed description of the particular change to the aviation system. The safety analyst then identifies the various potential hazards associated with the proposed change as well as impacts to other interfacing systems.

- **On Demand and Continuous Monitoring:** Hazard identification is applied to existing systems in operation. Figure 3 shows an example of a process that contains both on-demand analysis and continuous monitoring. It should be noted that data monitoring also helps detect: hazards that are more frequent or more severe than expected; and adopted mitigation strategies that are less effective than expected. In addition, continuous analysis can be established with notification thresholds based on a set of critical items of interest.

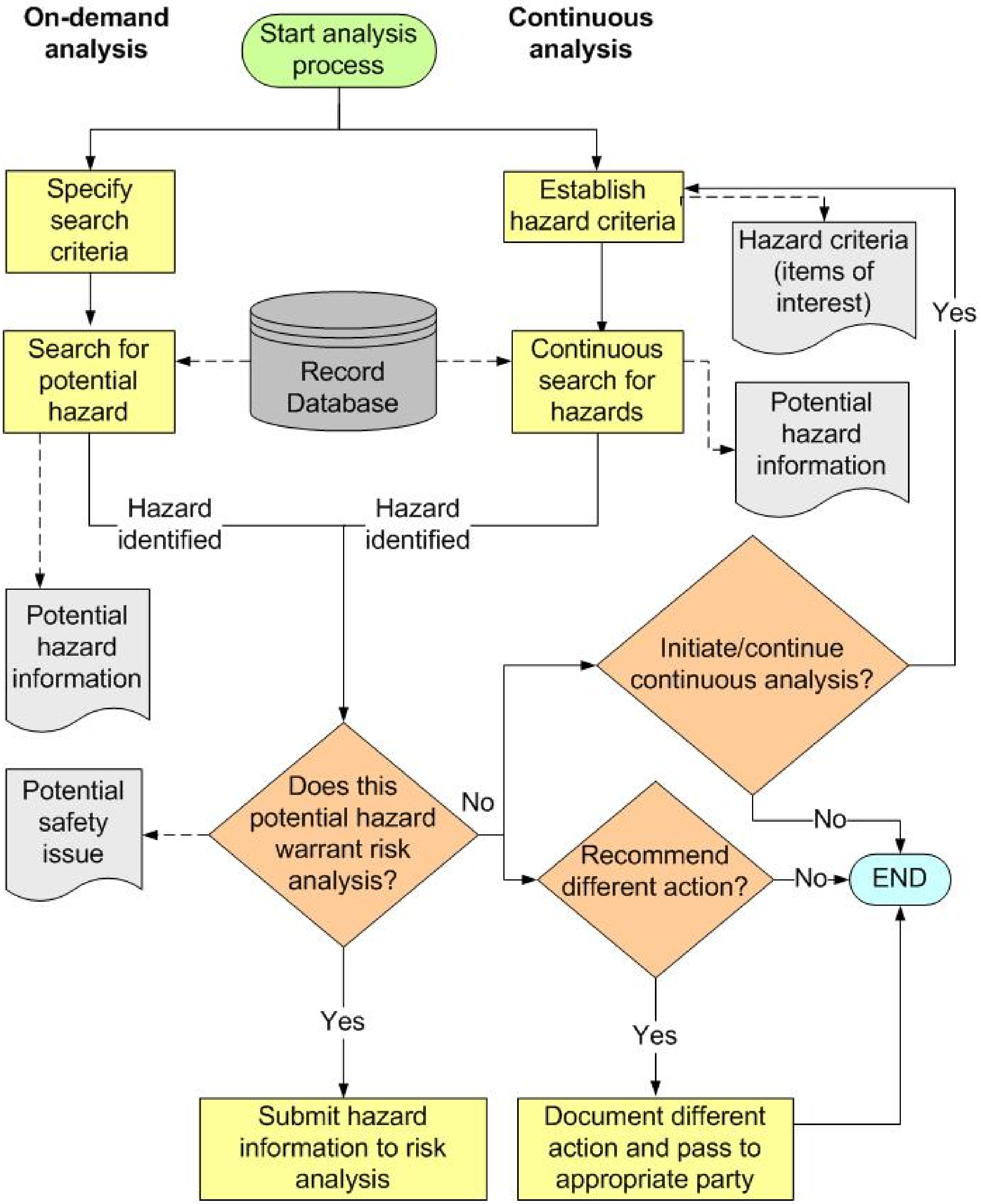
On-demand analysis
Start analysis process
Continuous analysis
Specify search criteria
Establish hazard criteria
Hazard criteria (items of interest)
Yes
Search for potential hazard
Record Database
Continuous search for hazards
Potential hazard information
Hazard identified
Hazard identified
Potential hazard information
Initiate/continue continuous analysis?
Potential safety issue
Does this potential hazard warrant risk analysis?
No
No
Recommend different action?
No
END
Yes
Yes
Submit hazard information to risk analysis
Document different action and pass to appropriate party

Figure 3: Hazard Identification in On-Demand and Continuous Analysis

Hazard Identification Methods and Tools

There are many methods and tools for hazards identification. Below are three examples[3].

Brainstorming

Brainstorming is an unbounded but facilitated discussion within a group of experts. A facilitator prepares prompts or issues ahead of the group session and then encourages imaginative thinking and discussion between group members during the sessions. The facilitator initiates a thread of discussion and there are no rules as to what is in or out of scope during the subsequent discussion. All contributions are accepted and recorded and no view is challenged or criticized. This provides an environment in which the experts feel comfortable in thinking laterally.

Advantages:

- Good for identifying new hazards in novel or non-complex systems.
- Involves all key stakeholders.
- Relatively quick and easy to undertake.
- Can be applied to a wide range of types of systems.

Disadvantages:

- Relatively unstructured and therefore not necessarily comprehensive.
- Depends on the expertise and profile of the participants.
- May be susceptible to the influence of group dynamics or top management goals.
- Can rely heavily on the skills of the facilitator for success.

Hazard and Operability (HAZOP) Study

HAZOP is a systematic and structured approach using parameter and deviation guidewords. The technique relies on a very detailed system description being available for study and usually involves breaking down the system into well defined subsystems and functional or process flows between subsystems. Each element of the system is then subjected to discussion within a multidisciplinary group of experts against various combinations of the guidewords and deviations. The group discussion is facilitated by a chair and the results of the discussion recorded by a secretary, including any hazards identified when a particular guideword and deviation combination is discussed. When a particular guideword and deviation combination does not produce any hazards, or is not thought credible, this should also be recorded to demonstrate completeness. The guidewords and deviations should be prepared in advance by the HAZOP chair and may need to be tailored to the system or operation being studied.

In an aviation context, typical guidewords might include:

- Detection
- Co-ordination
- Notification
- Transmission
- Clearance
- Authorization
- Selection
- Transcription
- Turn

[3] From the European Commercial Aviation Safety Team (ECAST) Safety Management System and Safety Culture Working Group Guidance on Hazard Identification

- Climb
- Descend
- Speed
- Read-back
- Monitoring
- Signage
- Handover
- Supervision

Typical deviations might include:

- Too soon / early
- Too late
- Too much
- Too little
- Too high
- Too low
- Missing
- Twice / repeated
- Out of sequence
- Ambiguous
- Reverse / inverted

HAZOP Approach Advantages:

- Systematic and rigorous.
- Involves interaction of views from multidisciplinary experts.
- Can be applied to a wide range of types of system.
- Creates a detailed and auditable record of the hazard identification process.

HAZOP Approach Disadvantages:

- Requires a considerable amount of preparation.
- Hard to use in a non-complex system.
- Can rely heavily on the skills of the HAZOP chair.
- Can be time consuming and therefore expensive.
- Can inhibit imaginative thinking and therefore certain kinds of hazards.

Checklist

Checklists are lists of known hazards or hazard causes that have been derived from past experience. The past experience could be previous risk assessments of similar systems or operations or from actual incidents that have occurred in the past. This technique involves the systematic use of an appropriate checklist and the consideration of each item on the checklist for possible applicability to a particular system. Checklists should always be validated for applicability prior to use.

Advantages:

- They can be used by non-system experts.
- They capture a wide range of previous knowledge and experience.
- They ensure that common and more obvious problems are not overlooked.

Disadvantages:

- They are of limited use when dealing with novel systems or non-complex systems.
- They can inhibit imagination in the hazard identification process.
- They would miss hazards that have not been previously seen.

7. RISK ANALYSIS

The next step in the safety management process is to assess or analyze the risk associated with the potential outcomes for each particular hazard, in which each risk is the product of severity and probability. Thus, severity and probability should be expressed in measureable terms, based on the potential outcomes of the hazards identified, such that hazards can be ranked and compared to established risk guidelines, which will assist in determining the appropriate extent and timing of risk mitigation.

In assessing risk, one can use both quantitative and qualitative methods. Using quantitative data is preferred, as it tends to be more objective. However, when some of the quantitative data are not available, it is acceptable to rely on qualitative data and expert judgment. Qualitative judgment varies from person to person, so if only one person is performing the analysis, the result should be considered an opinion. With a team of experts involved in the analysis, one can consider the result qualitative data and expert judgment. Therefore, the quality of analysis relies on the background of the experts on the selected team.

Advantages of quantitative data:

a) Data is expressed as a quantity, number, or amount.
b) Data tend to be more objective.
c) Data allow for more rational analysis and substantiation of findings.
d) Data can be used for modeling.

Advantages of qualitative data:

a) Data is expressed as a measure of quality.
b) Data is subjective.
c) Data allow for examination of subjects that can often not be expressed with numbers but by expert judgment.

It should be noted that if modeling is required and data is available, the risk assessment should be based on statistical or observational data (e.g., radar tracks, hardware failure rates). When there is insufficient data to construct purely statistical assessments of risk, judgmental inputs can be used, but they should be expressed in quantitative terms. For example, the true rate of a particular type of operation may be unknown, but can be estimated using judgmental input. In all cases, quantitative measures should account for the fact that historical data may not represent —or can lead to a false configuration of— future operating environments. In such cases, some adjustment to the input data may be required.

Figure 4 shows an example of a risk analysis process used to determine the type and priority of corrective risk controls.

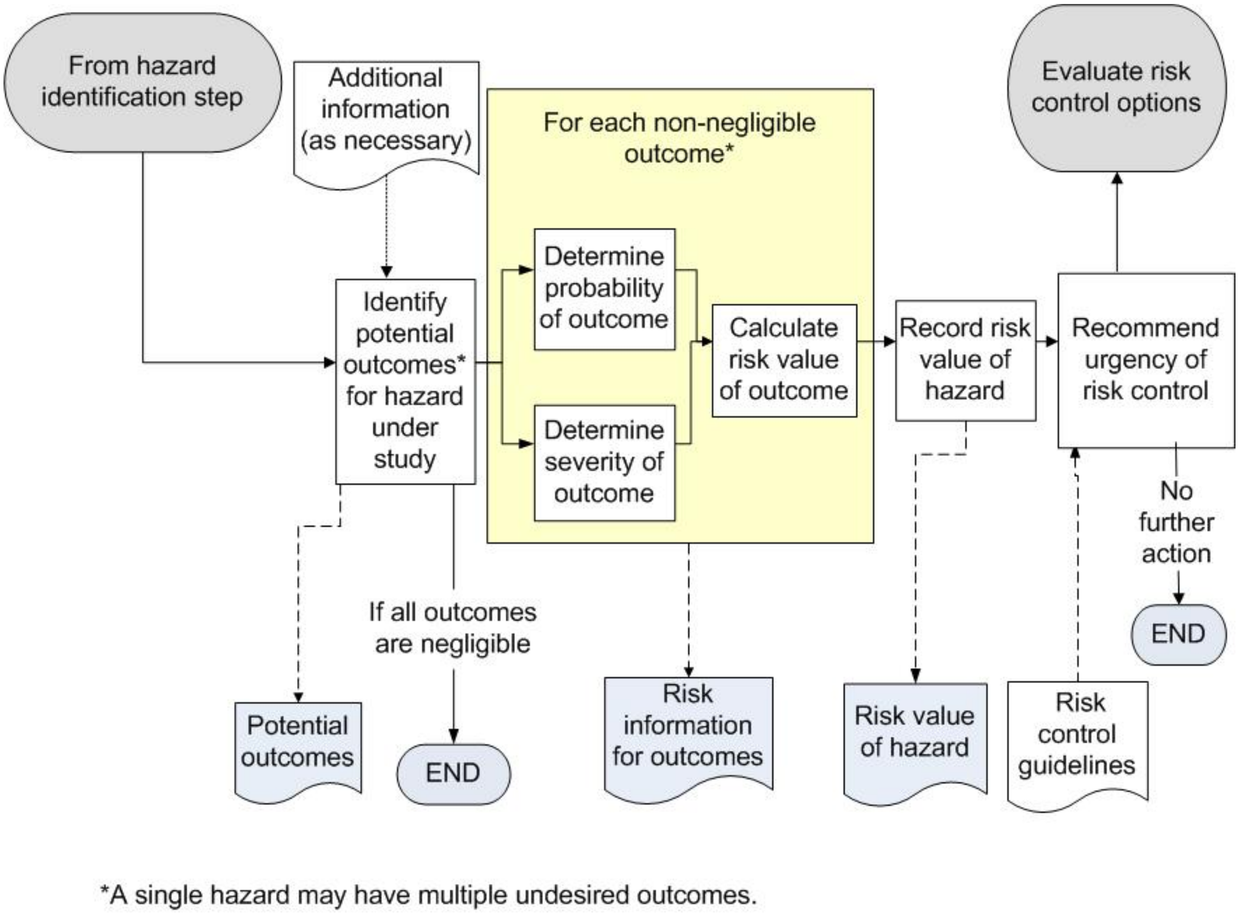
From hazard identification step
Additional information (as necessary)
For each non-negligible outcome*
Evaluate risk control options
Identify potential outcomes* for hazard under study
Determine probability of outcome
Determine severity of outcome
Calculate risk value of outcome
Record risk value of hazard
Recommend urgency of risk control
No further action
END
If all outcomes are negligible
Potential outcomes
END
Risk information for outcomes
Risk value of hazard
Risk control guidelines
*A single hazard may have multiple undesired outcomes.

Figure 4: Sample Risk Analysis Process

It should be noted that risk can be viewed and controlled against various risk profiles, in which one can view risk across a single aircraft flight, a fleet of aircraft, an industry segment or segments, etc. The risk profile is dependent on the overall safety objectives of a particular aviation sector (authority or service provider).

Additionally, a key aspect of any risk analysis is the documentation of various assumptions that lead to a specific risk classification. These can be revisited in the future and updated when necessary, especially if the operational environment changes.

8. RISK MITIGATION STRATEGIES

The objective of risk mitigation is to implement appropriate plans to mitigate the risk associated with each outcome of identified hazards until they reach an acceptable level of safety. The safety analyst develops, documents, and recommends appropriate risk mitigation or risk control strategies. A risk control is anything that mitigates the risk of a hazard's effects/consequences. A risk control strategy includes options and alternatives that lower the risk or eliminate the hazard. Examples include: implementing additional policies or procedures; developing redundant systems and/or components; reviewing training specification and results; and using alternate sources of production.

When the level of risk is determined to be unacceptable, the analyst identifies and evaluates potential risk mitigation strategies that would reduce the risk to a level acceptable to the organization's management, as expressed in organizational (authority or service provider) policies. Then the analyst assesses how the proposed mitigation strategies would affect the overall risk. If necessary, the analyst repeats the process until a combination of strategies reduce the risk to a level acceptable to the organization's management. If the results of a risk assessment reveal an unacceptable level of risk, the operations or processes should be stopped immediately until some mitigation action leads to an acceptable level.

As a next step, an evaluation of each proposed risk control should be performed. Ideal risk control candidates are inexpensive, easy to perform, implemented quickly, completely effective, and do not introduce substitute risk (risk of unintended consequences). Since most situations do not meet these ideals, candidate risk controls should be evaluated and selected based on balancing the attributes of effectiveness, cost, timeliness of implementation, and complexity. Once risk controls have been selected and implemented, then they should be monitored and validated to ensure that the intended goals have been achieved.

The risk mitigation approach selected may fall into one or more of the following categories:

- **Risk Avoidance Strategy:** The risk avoidance strategy averts the potential of occurrence and/or consequence by selecting a different approach or by not participating in the operation, procedure, or system (hardware and software) development. This technique should be pursued when multiple alternatives or options are available. The risk avoidance strategy is more likely used as the basis for a "go" or "no-go" decision at the start of an operation or program.

- **Risk Reduction Strategy:** The risk reduction strategy means a reduction of frequency of operation or activity, or an adoption of specific actions to reduce the severity of the consequences of the accepted risks. This strategy can lead to a risk transfer action if the specific actions to reduce the risk are controlled by another party.

- **Risk Transfer Strategy:** The risk transfer strategy shifts the ownership of risk to another party. Organizations transfer risk primarily to assign ownership to the organization or operation most capable of managing it. The receiving party should accept the risk, which should be documented (e.g., Letter of Agreement, Statement of Agreement, Memorandum of Agreement). An example of risk transfer is the transfer of an aviation system from the acquisition organization to the organization that provides maintenance.

- **Segregation of Risk Exposure Strategy:** In this strategy, action is taken to isolate the effects of risks or build in redundancy to protect against them. An example of segregation of exposure is to limit operation into an aerodrome surrounded by complex geography to aircraft with specific navigation capabilities.

- **Risk Assumption Strategy:** The risk assumption strategy is simply accepting the likelihood or probability and the severity of consequences associated with a risk's occurrence. It is not usually acceptable to use an assumption strategy to treat high risk associated with a hazard. The safety risk should still be mitigated to reduce it to lower levels before it can be accepted. When selecting this approach, available countermeasures should be prepared against the assumed risks in advance.

In summary, the guidance described in Chapters 6, 7 and 8 provide general methods that can be used to identify hazards, assess the risk associated with the outcomes of the hazards, and mitigate the risk to acceptable levels. The next chapter provides examples of hazard identification and analysis methods utilized by some authorities.

9. EXAMPLES OF CURRENT AUTHORITIES' RISK MANAGEMENT METHODS

The SM ICG conducted a survey of participating authorities' existing data collection, hazard identification, and analysis processes to establish a current baseline of existing practices. The purpose of establishing this baseline is to provide examples of existing methods and tools, along with reference URLs for additional information, to States that are developing their safety management processes. Authorities provided both mature processes and those nearing deployment. A few examples resulting from the survey are contained in the table below. Following the table, the first example from the table —the *Decolagem Certa* (DCERTA) System— is more thoroughly addressed as a case study related to an existing risk management process.

Table 1: Examples of Authorities Risk Management Methods

Regulatory Authority	Name of the Process/System	Description and Purpose of the Process/ System	References for Additional Information
National Civil Aviation Agency (ANAC) of Brazil	Decolagem Certa (DCERTA) System	Brazil has developed an automated system, known as the *Decolagem Certa* (DCERTA) System, which verifies regulatory compliance of general aviation flights regarding the technical crew (license, rating, and medical certificate), aircraft, and operated aerodromes, based on information contained in Flight Plans presented by pilots at airports AIS. This system provides data for safety analyses, which in turn have been used to generate trend indicators allowing the establishment of a risk-based auditing program.	http://www2.anac.gov.br/decolagemcerta/
European Aviation Safety Agency (EASA)	European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS)	The mission of the European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) is to assist National and European transport authorities and accident investigation bodies in collecting, sharing, and analyzing their safety information in order to improve public transport safety.	http://eccairsportal.jrc.ec.europa.eu/index.php?id=1
Federal Office of Civil Aviation (FOCA) of Switzerland	SRM (Safety Risk Management)	The FOCA has implemented an agency internal SMS compliant with the ICAO framework (Doc. 9859). Hazard identification is conducted based on data-driven triggers coming from occurrence reports, surveillance findings, Air Accidents Investigation Branch (AAIB) investigations and other sources. Analysis is normally qualitative (hazard identification studies (HAZID), HAZOP). Subsequent risk analysis is either qualitative or quantitative or both. Results are captured in a hazard catalog/risk portfolio. Inputs from a stakeholder's SMS is also integrated.	http://www.bazl.admin.ch/

United States Federal Aviation Administration (FAA)/ Aircraft Certification Service (AIR)	Monitor Safety/ Analyze Data (MSAD)	Monitor Safety/ Analyze Data (MSAD) is a data-driven methodology to identify, assess, and mitigate aircraft product hazards in-service, which uses product-defined hazard criteria to surface potential hazards from aviation safety data. MSAD uses a standard taxonomy for organizing continued operational safety (COS) data to promote quick identification of emerging safety trends through dependent variable analysis. Safety issues are analyzed to determine risk which is used to determine the extent and timing of corrective action. MSAD uses a causal analysis approach. This approach may identify underlying contributing factors, such as process breakdowns, which are then communicated to the appropriate Aviation Safety Organization (AVS) oversight business process owner.	http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/215154
Transport Canada Civil Aviation (TCCA)	TP 13905 "Risk Management, Type 2A (Short Process)"	The document TP 13905 "Risk Management, Type 2A (Short Process)" defines the process to be followed in detail. Advisory Circular (AC) 107-001 "Guidance on SMS Development" also provides details on risk management.	http://www.tc.gc.ca/eng/civilaviation/publications/tp13905-menu-1906.htm
New Zealand CAA	Risk Profile Ratings	Operators will be rated using a scale of 1 to 5, in each assessed area, in which 1 is an exemplary rating. It is a qualitative rating and relates solely to the interaction the CAA staff member is having with the client at that time, or to changes in the organization recorded in the CAA database. Ratings of 2 to 5 will be used to record higher levels of risk. Risk items are weighted according to the CAA's assessment of their likely effect on an operator's overall risk. When the ratings in each of the assessed areas are combined, a comparative risk profile can be derived, in which the risk profile rating (expressed as a percentage of the possible) of an individual operator can be shown as a diagram, compared to the ratings of all other operators with the same document. Ratings are confidential between each operator and the CAA.	http://www.caa.govt.nz/Surveillance_System/The_Risk_Profile_Ratings.htm
Japan Civil Aviation Bureau (JCAB)	Aeronautical Safety Information Management and Sharing System (ASIMS)	Operators are required to report accidents, incidents, and occurrences that may affect safe operation to the ASIMS system. JCAB analyzes causes and evaluates safety risks of those reported events. The results are used for conducting effective oversight and taking necessary safety actions.	

Example for Civil Aviation Authority Data Utilization

Case: ANAC – Brazilian Civil Aviation Authority – *Decolagem Certa* (DCERTA) System.

National Civil Aviation Agency (ANAC) of Brazil, by analyzing the accident and incident data of the General Aviation sector, observed that a large number of the operations that resulted in accidents presented some kind of non-compliance to the regulations. The large number of operators in General Aviation and the limitations of ANAC in its financial and human resources presented difficulty to control these situations through inspection activities. In an attempt to solve this problem, ANAC decided to create a systematic approach to identify the focuses of risk and optimize inspections through a data driven method.

ANAC has developed a system called *Sistema Decolagem Certa* (DCERTA), translated as "Safe Takeoff System." The system collects data about the flight plans in the moment they are made and interacts with the agency's databases, searching for non-compliances about the pilot's licenses, ratings and medical certificate, the aircraft certificate, and operational procedures for each flight. This data collected through DCERTA system is primarily regulation compliance data, but they are also safety related, once the regulations are put in place to assure safety aviation services for the society.

The data is used to identify the most frequent non-compliances, the regions where each one is more frequent, and even the service provider that presents higher rates of non-compliances. The mitigating actions are taken in two different approaches:

1. At first, the non-compliance, when confirmed as a violation is treated according to the regulations. This is *reactive risk management*, which punishes the violations in order to inhibit the service provider maintaining a lawless and, therefore, unsafe operation.

2. The second approach is *proactive risk management*. By statistically analyzing the data, it is possible to identify the most "non-compliant" operators, and in which sector they require more attention (e.g., an operator that has poor personnel licenses control). This allows ANAC to plan focused inspections on those operators identified as higher risk and correct their operations before any bigger event occurs.

Still in *proactive risk management*, it is possible to remotely oversee the aircraft operators and define indicators and future goals to be achieved. For example, ANAC oversees several aviation sectors (business aviation, instruction, general aviation, etc.) through three main indicators — one for the total of non-compliances, one for personnel-related non-compliances, and another for aircraft-related non-compliances. The relationship between non-compliances and unsafe operations can be observed in Figures 4 and 5.

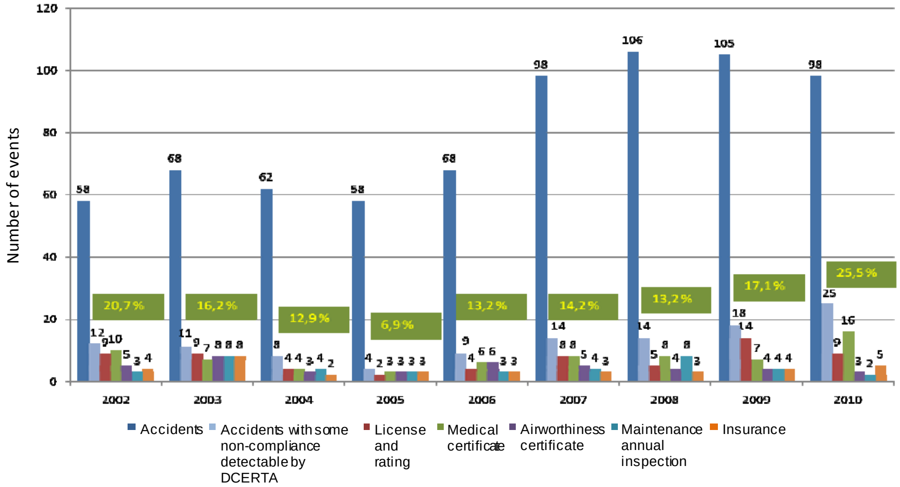

Figure 5: Non-compliances and Related Events

In Figure 5, the blue bar represents the quantity of accidents in Brazilian Civil Aviation (general aviation included) and the other bars represent a different non-compliance detected by the DCERTA System.

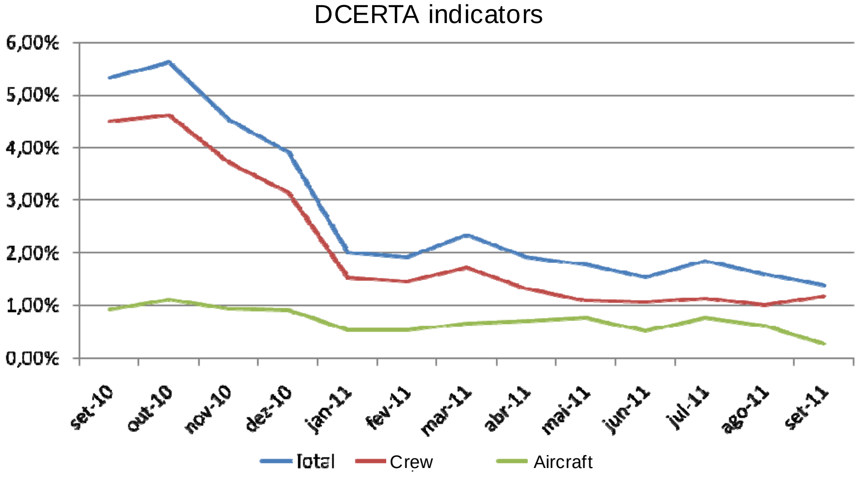

Figure 6: DCERTA Indicators

In Figure 6, the blue line represents the percentage of flights that presented some non-compliance in the DCERTA System. The red represents non-compliances related to crew situation and the green shows aircraft situations. As the graphic shows, the total number of flights that presented some non-compliance for September of 2011 corresponds to less than 1.5% of the total number of flights. On the other hand, in figure 5, the total number of flights that presented some non-compliance among the operations that resulted in accidents represented 25.5% of the total during 2010.

This analysis shows very clearly the relationship between non-compliance and the level of risk involved in the operation, which makes the DCERTA System a very useful tool for the Brazilian Civil Aviation Agency safety risk management.