The ARMS Methodology for

Operational Risk Assessment

in Aviation Organisations

Developed by the ARMS Working Group, 2007-2010

Executive Summary

ICAO has created a new standard for Safety Management Systems (SMS) in various aviation organisations, including among others airlines, maintenance organisations, ATC services, aerodromes. Risk Assessment has a central role in the Safety Management System.

For many reasons, Risk Assessment is a very challenging task. Older methods have been characterised by high levels of subjectivity and other difficulties.

An industry working group, ARMS (Aviation Risk Management Solutions) was set up 2007 in order to develop a new and better methodology for Operational Risk Assessment (ORA). The primary target group for the methodology is airlines but it will also be fully applicable to other aviation organisations.

The working group consisted mainly of safety practitioners from airlines. This should ensure that the proposed methodology is applicable to the real-life setting of an airline or other aviation organisation.

The methodology defines an overall process for Operational Risk Assessment and describes each step. The assessment process starts with Event Risk Classification (ERC), which is the first review of events in terms of urgency and the need for further investigation. This step also attaches a risk value to each event - which is necessary for creating safety statistics reflecting risk. The next step is data analysis in order to identify current Safety Issues. These Safety Issues are then risk assessed in detail through the Safety Issue Risk Assessment (SIRA). The whole process ensures that any necessary safety actions are identified, creates a Register for following up risks and actions and provides a Safety Performance Monitoring function. SIRA can also be used to make Safety Assessments, which is a requirement of the “Management of Change” element of the SMS.

Both ERC and SIRA are based on new concepts that make the assessments conceptually more robust whilst keeping them pragmatic and simple.

This report explains the methodology in detail. Its main purpose is to provide guidance and examples for safety professionals on how to apply the method. In addition to the method itself, the report reviews the difficulties in using the older methods and describes the ARMS working group.

Legal disclaimer

All organisations remain fully responsible for their own safety performance. Therefore, the ARMS Working Group, its members and supporting organisations do not accept any responsibility for any harm or damages of any kind, relating to the use of the ARMS methodology or its parts.

Table of Contents

1 Introduction

1.1 What is this document about?

Most aviation organisations are required by their National Aviation Authority to implement a Safety Management System (SMS). The International Civil Aviation Organisation (ICAO) has published a framework for a typical SMS with Safety Risk Management as the core component. Safety Risk Management can be split into three elements, (i) Hazard identification, (ii) Risk assessment and (iii) Risk mitigation.

Risk assessment has always been the most challenging part of the risk management process for aviation operations. This is due to the subjectivity involved in determining the severity of the consequences when a hazard is released and the lack of quantitative information on the probability of this occurring.

Another key component of the ICAO SMS framework is “Safety Assurance”, one element of which is “Management of Change”. This introduces the need for another type of risk assessment in the form of a formal “Safety Assessment”, usually related to planned changes in the operation.

This document presents a new methodology for Operational Risk Assessment (ORA) that attempts to overcome the classic difficulties and support the new SMS requirements in an effective manner.

The primary focus is on operational Flight Safety risks, i.e. any risks that could harm the occupants of an aircraft (passengers and crew), though the new methods can be applied to all aviation operational risks.

This document aims to deliver a *complete description* of the methodology: the *what*, *why* and *how*. The conceptual framework is thoroughly explained along with the risk management process and each of its steps. Worked examples are provided for all parts of the process along with an explanation of how the methodology can be appropriately customised for an individual organisation.

The reader should not mistakenly interpret the volume of this document as an indication of the complexity of the methodology. *The one-page summary (chapter 9) is enough for the everyday use of the methodology.* Most users will never have to study this document in full. It is there to satisfy the implementer who needs to understand more of the rationale behind the approach. *Chapters 4 and 5 together with the worked examples in chapter 6 contain the detailed explanation of the ARMS process.* The document also serves to try to record the full work of the working group for people who could not be part of the discussions which made the ARMS methodology what it is today.

1.2 Who can use the described method?

The method is intended not only for airlines and other air operators, but also for other aviation organisations (directly or indirectly) linked to flight operations, for example Maintenance organisations and Air Traffic Control organisations.

It is believed that this methodology will not only enhance the quality of risk assessment in individual aviation organisations but also enable increased cooperation between them. This is because the approach introduced is partly built on the idea of "global" risk, i.e. the total risk produced by all involved organisations and "delivered" to the organisation, which is actually operating the aircraft.

Chapter 5 addresses the customisation of the methodology for different types of aviation organisations. The described methodology may prove useful also for organisations outside aviation, even though this was not an objective of the original design.

The material is freely available to anyone, but when used in any publication, presentation, software or alike, full reference must be made back to the original ARMS work.

1.3 What is delivered?

At the conceptual level, the document introduces the overall principles of how operational risk assessments should be carried out and why. This section introduces several new concepts and recommended practices.

At the practical level, the document contains a complete and fully detailed method with matrices, colour codes, numbers and user guidance. This provides *an example* of how the conceptual methodology can be transformed into practical applications. It should be remembered that organisations may need or want to *customise* the practical application to suit their specific needs. Chapter 5 is dedicated to customisation. The details are also bound to evolve over time.

It is important to recognise the difference between these two levels. The recommendations at the conceptual level are intended to be universally applicable, while the practical application is only one way to apply the methodology. The content which refers to the practical application is highlighted by a light background shading.

1.4 About the ARMS working group

ARMS is an industry working group of individuals from organisations which support the work on a voluntary basis. The ARMS Mission Statement is presented in Appendix 6.1.

ARMS is a non-political, non-profit working group, with a mission to produce a good Risk Assessment methodology for the industry. The results are freely available to the whole industry and to anyone else interested in the concept.

ARMS was born at the initiative of some individuals with the starting point being a workshop in June 2007. More details on the beginning of the working group and its working methods are explained in appendices 6.2 and 6.3 respectively. Members of ARMS are listed in appendix 6.4.

The ECAST SMS Working Group that was set up in April 2008 immediately identified that practical guidance on Risk Assessment would be one of its most important deliverables. Once it had been briefed about the ARMS activity, it decided not to duplicate the development effort but to take the work of ARMS as the reference for operational Risk Management. The ECAST group has since followed the ARMS work closely and the ARMS deliverables are also the ECAST SMS WG deliverables on this topic.

Key people running the SMS activity in ICAO have also been kept up-to-date with the ARMS work through emails and presentations.

2 Why a new methodology for Operational Risk Assessment?

2.1 Objectives for Operational Risk Assessment

Operational Risk Management consists of three elements: Hazard Identification, Risk Assessment and Risk Reduction (mitigation, in ICAO terminology). *The main objective of Risk Management is to make sure that all risks remain at an acceptable level*.

Contributing to Safety Performance Monitoring through the establishment of risk-based Safety Performance Indicators can be considered a secondary objective. Risk information can also be used by the national authorities in their safety oversight.

Hazard identification is about collecting and analysing operational safety data, thereby identifying Safety Issues (see the Glossary for a definition of a Safety Issue). Such safety data typically includes safety reports, Mandatory Occurrence Reports (MOR), flight data events, and the results of safety surveys and audits. Hazard Identification provides the input for Risk Assessment.

The objective for Operational Risk Assessment (ORA) is the *Assessment of operational risks in a systematic, robust and intellectually cohesive manner*.

Operational Risk Assessment is needed in three different contexts:

1. Individual safety **Events** may reflect a high level of risk and consequently require urgent action. Therefore all incoming events need to be risk assessed. This step is called Event Risk Classification (ERC).

2. The Hazard Identification process may lead to the identification of **Safety Issues**, which need to be risk assessed to determine what actions, if any are needed. This step is called Safety Issue Risk Assessment (SIRA).

3. From time to time there will be a need to carry out **Safety Assessments**, typically related to a new or revised operational activity (e.g. new destination). The activity needs to be risk assessed at the planning stage, according to the "Management of Change" process of the company.

In the first two cases, the assessment is based on Hazard Identification data. The result is an operational risk profile, i.e. an overview of all operational risks. In the third case, there may be no data available if the planned activity is new to the organisation. In all three cases, the risk assessment must consider the *potential* consequences in addition to the observed *actual* consequences of events. The methods used in the three cases should be compatible so that outputs from one can be used in another.

In addition to the overall objectives, several practical requirements for ORA can be listed:

- The ORA method should be able to use all typical safety data as inputs (safety reports, flight data, LOSA type observations, audit findings, etc.) and be designed to use sources which produce large quantities of valuable safety data. These sources may be both internal and/or external.

- The method should not require data that is not easily available or that cannot be reasonably estimated.

- The method should be easy to use and not create an unreasonable workload. Large airlines may have to process several hundred safety reports per month. Hence the ERC process must be quick and easy to follow.

- Subjectivity should be minimised.

- The results should be understandable by non-experts and help identify any necessary actions.

2.2 Current methods of Operational Risk Assessment

There is a fundamental conceptual problem with the risk assessment of (historical) events which needs to be recognised. To understand the problem, it is necessary to go back to a very basic, elementary definition of risk:

"Risk is a state of ***uncertainty*** *where some of the possibilities involve a loss, catastrophe, or other undesirable outcome."*
(*Douglas W. Hubbard*[♣])

Hence ***uncertainty*** is a key element of risk. Therefore if the outcome is a known historical fact, we can refer to *loss*, damage, etc, but not risk. Risk should technically refer to something in the future, where the outcome is uncertain.

How then can we risk assess an historical event? This question raises some fundamental concerns about any attempt to risk assess reported safety events, flight data events, etc. With the emergence of large quantities of flight safety data, safety managers want to apply the concept of risk on the collected data, but this fundamental dilemma needs to be addressed.

Although an historical event contains no risk now, it *did* carry risk as it occurred. It is just that the risk was not necessarily realised. Therefore we want to capture the risk that the event carried as it occurred so we can recognise the risk that these events demonstrate within our operation.

[♣] Director of Applied Information Economics (AIE). Author of the #1 bestseller in business math on Amazon: "How to Measure Anything: Finding the Value of Intangibles in Business"

The most common approach to risk assessment in aviation has been to use the classical risk formula i.e. *severity x likelihood* to create a two dimensional matrix that guides the risk tolerability judgment. In trying to give values to *severity* and *likelihood*, the analyst has to answer the questions: "severity of what?" and "likelihood of what?". Unfortunately different analysts tend to answer these questions differently:

- Some refer to the severity of the *actual event* and its actual, real outcome.
- Others think of the severity of the *potential* outcome, an "imaginary but realistic" outcome, "the most probable type of accident" outcome or the "worst case scenario".
- The "likelihood of recurrence" question is equally subjective as one must assess the likelihood of something *similar* happening again, but it is unclear *how similar*.

This conceptual confusion is illustrated in appendices 6.5 and 6.6.

Hence, instead of trying to assess the risk present in the event as it unfolded, analysts are usually *de facto* trying to assess the risk of *a similar event taking place in the future* – but "a similar event" is a vague object for risk assessment, causing a significant increase in the subjectivity of the result.

The effectiveness of existing *Risk Controls* is an extremely important consideration in trying to measure risk. The simplistic *severity x likelihood* formula does not take the existing (nor potential) Risk Controls into account in a proper manner. This is primarily due to the lack of a robust conceptual framework which has resulted in this and other inherent problems in current methods being understated.

All risk assessment methods need to provide guidance for the analyst to help in the selection of the "correct" column or row in the risk matrix. Words like "occasional" and "rare" for likelihood or "major" / "minor" for severity do little in helping to achieve coherent, consistent assessments. Sometimes very detailed definitions for each column/row are provided. This can easily create the trap of considering only the *actual outcome* of the event, and trying to match it with the written definitions.

Current risk assessment methods tend to be applied universally to all of the three risk assessment contexts described in section 2.1. and generally fail to make the crucial differentiation between safety **Events**, **Safety Issues** and **Safety Assessments**. However as the above discussion illustrates, an historical event is not an ideal subject for a "forward-looking" risk assessment. Safety Issues are typically identified due to *a number of events* and can be precisely defined (as it is up to the analyst to define them!). They are safety problems that could potentially lead to an accident and are therefore very suitable subjects for a forward-looking risk assessment. Safety Assessments deal with future changes and can usually be sub-divided into several (potential) Safety Issues

In contrast to the simplistic methods based on the *severity x likelihood* formula, some complex methods have been developed which rely on *modeling* the aviation system and using advanced mathematics to represent relationships between certain factors and trying to calculate their safety impact. Whether such models can reproduce the complex and sometimes chaotic ways in which various factors interact in creating an accident is yet to be proven. Several developments based on this approach have been abandoned in the past, when it became evident that building *and maintaining* the model would introduce an unacceptable workload due to the constant changes in procedures, training syllabi, aircraft modification status and technology that is prevalent throughout the aviation system.

A new methodology must address the deficiencies in existing methods as well as meeting the objectives described in section 2.1

2.3 The new methodology

The new methodology aims to be both conceptually robust and practically useful in the real operational context.

- All the concepts and terms involved are defined (See Glossary). There is clear differentiation between safety **Events** and Safety **Issues**, which are addressed with different but compatible risk assessments.

- The Safety Issue Risk Assessment process is also applicable to Safety Assessments.

- Special care has been taken to ensure that the initial steps of Event Risk Classification (ERC) are easy and fast to perform, as they will have to be performed on all incoming events.

- A clear conceptual framework together with detailed guidance is designed to provide full clarity on *what* is being risk assessed and to help reduce subjectivity in the assessment itself. The impact of Risk Controls is integrated in the risk assessment, and therefore no longer an isolated or unperformed task. How this is achieved is explained later in the document.

- The result of each assessment is designed to be clear and understandable by operational line management.

The methodology may be customised to specific organisational requirements and preferences. It is also applicable to non-flying organisations such as Maintenance Repair Organisations (MRO), ATC and airport operators.

Whilst the new methodology will not remove all subjectivity from the risk assessment of aviation events, it is believed that it is significantly more objective than the other methods currently in use in aviation.

3 Overview of the ARMS Methodology

This chapter presents a short overview of the ARMS Methodology in order to give the reader the global picture of the Methodology, including its scope and key aspects. Chapter 4 will then explain each aspect in detail.

3.1 Scope and applicability

In discussing risk assessment in aviation, especially in the context of an airline there is a natural tendency to focus on *Flight Safety risk* and, in particular, the risk of an accident with multiple fatalities and hull loss. In practice, a single event may relate to more than one type of risk and airlines must manage different types of risks in parallel. These additional risks include:

- Financial risk – the risk of significant financial loss.
- Environmental risk – the risk of damage to the environment.
- Reputation risk – the risk of damage to the airlines' reputation – e.g. problems with uncommanded safety announcements during flight about the aircraft ditching pose no flight safety risk but will attract significant passenger attention and concern.
- (Flight) Operational risk – the risk of operational delays resulting from the grounding of an aircraft or aircraft fleet. This could be considered as part of the financial risk.
- Airworthiness risk – the risk that the aircraft may be not be airworthy due to maintenance or ground handling problems.
- Security risks – e.g. risk of loss due to deliberate actions endangering the flight

The ARMS methodology has been developed for Flight Safety risks, so in this document, the primary focus is on operational *Flight Safety risks*, i.e. any risks that could harm the occupants of an aircraft (passengers and crew). However, the working group believes that the methodology could easily be adapted for other types of risks.

As stated in section 2.1, Operational Risk Assessment is needed in three different contexts:

1. Individual safety **Events** may reflect a high level of risk and consequently require urgent action. Therefore all incoming events need to be risk assessed. This step is called Event Risk Classification (ERC).

2. The Hazard Identification process may lead to the identification of **Safety Issues**, which need to be risk assessed to determine what actions, if any are needed. This step is called Safety Issue Risk Assessment (SIRA). Safety Issues may need to be re-assessed on a regular basis to ensure that the risk is maintained at or below the acceptable level.

3. From time to time there will be a need to carry out **Safety Assessments**, typically related to a new or revised operational activity (e.g. new destination).

The activity needs to be risk assessed at the planning stage, according to the "Management of Change" process of the company.

The primary target group for the ARMS methodology are airlines and other aircraft operators. The secondary target group consists of aviation organisations, which have a link to aircraft operation but do not operate the aircraft themselves.

3.2 Relationship with older methods and key references

The ARMS methodology links with the following elements of the ICAO SMS framework:

- Risk Assessment (and mitigation)
- Safety Performance Monitoring and Measurement
- Management of Change

The ARMS methodology can be seen as a further elaboration of the principles that are behind the more generic method given in the ICAO SMS course material and the Safety Management Manual (SMM). Both approaches share the same objectives[♠].

It should be kept in mind that methods given in the ICAO SMS material and any NAA-level Acceptable Means of Compliance (AMC) documents are not necessarily restrictive, i.e. they present *one* way to comply without ruling out other acceptable methods.

3.3 Key points of the ARMS methodology

The ARMS methodology can be summarised with the following points:

- The overall end to end Risk Assessment process, starting from Hazard Identification and leading to Safety Actions has been defined and acts as the backbone for the methodology.

- All new incoming Safety Event Data needs to be reviewed within an acceptable timeframe so that there can be an immediate reaction to any urgent issues. This task is **Event Risk Classification (ERC)**, and is the first step in the ARMS Risk Assessment process. The ERC makes *a quick initial estimate on the risk inherent in the event*. The new concept of "event-based risk" is used to estimate the risk. The result is both a risk class (colour) indicating what needs to be done with the event – and a numerical value of risk (the ERC risk index value) which can be used in quantitative risk analysis. Once risk assessed, all events are stored in a safety event database.

- Since, as explained earlier, an historical event has no risk *today*, the actual event is extrapolated into what accident outcome *could* credibly *have* occurred. This is then risk classified taking into consideration the barriers that

[♠] In 2008, when the ARMS methodology was presented at ICAO, the feedback was that the methods presented in the ICAO SMS material are not the only acceptable ways to carry out the activities and no conflict was seen between the ARMS methodology and the ICAO guidance material.

avoided this event being that accident outcome. The question is: what *was* the risk, *at the time* when the event occurred.

- When the Safety Data in the database is analysed (Data Analysis), the main focus is on identifying any Safety Issues that affect the current operation.

- All identified Safety Issues are risk assessed using the **Safety Issue Risk Assessment (SIRA)** technique. The conceptual framework for this risk assessment is again a new one: risk is calculated as the product of *four* factors, (prevention, avoidance, recovery and minimisation of losses) instead of the old severity x likelihood formula. This new framework includes the risk controls (barriers) in the risk assessment. The output from SIRA is a risk value for each Safety Issue.

A key priority of the ARMS methodology is to reduce the subjectivity inherent in current risk assessment methods. Three steps that help to achieve this are:

- In the Event Risk Classification (ERC), all the circumstances that conspired to produce the event are known and are considered as they were, so the subjectivity associated with determining the likelihood of the event occurring has been greatly reduced.

- The ERC attempts to identify the likelihood of this event having resulted in an accident outcome by assessing the barriers that avoided this event being that outcome. The consideration of these barriers is still subjective but that subjectivity can be reduced by a good understanding of the barriers available in typical scenarios. [♣]

- In carrying out a Safety Issue Risk Assessment (SIRA), the analyst him/herself should first define and scope the Safety Issue before risk assessing it. A precisely defined Safety Issue is much easier to assess quantitatively. For example a windshear Safety Issue that concerns only one aircraft type and one airport is easier to examine than one that covers the whole airline fleet and route network. Careful definition will ensure that the risk assessment is more likely to be based on facts rather than imagination and guessing.

3.4 The Risk Assessment Process

A simplified outline of the Risk Assessment Process developed by the ARMS group is presented in figure 1.

Hazard identification is about collecting and analysing operational safety data, thereby identifying Safety Issues. Such safety data typically includes safety reports, flight data

[♣] Another interesting difference is that in the ARMS methodology, all Event Risk Classifications are independent of each other (see appendix 6.5 – third bullet point).

events, and the results of safety surveys and audits. Hazard Identification provides the input for Risk Assessment.

A knowledgeable person has to review such data relatively quickly so that any urgent matters can be addressed in a timely manner. This step is addressed through the Event Risk Classification (ERC) process.

The possibility of taking action based on individual events constitutes the first step in the process (red arrow "Urgent actions?").

All incoming safety data is also stored in a database. The database should be routinely analysed in order to detect any adverse trends and to monitor the effectiveness of earlier risk reduction actions. This analysis may lead to the identification of a potential Safety Issue which needs to be formally risk assessed to determine the level of risk and to design appropriate risk reduction measures. This is the bottom (yellow) arrow in figure 1.

Additionally, analysis of the database, prompted by an event or concern may reveal risks that should be dealt with immediately before a more formal SIRA is carried out; i.e. some issues which are obviously "wrong" are fixed without a risk assessment. E.g. a sudden increase in unstabilised approaches in airport X may lead to action without a formal risk assessment. This "quick response" is represented by the middle (blue) arrow. These issues should eventually have a formal SIRA carried out so that they can be properly measured and tracked in the Risk Register

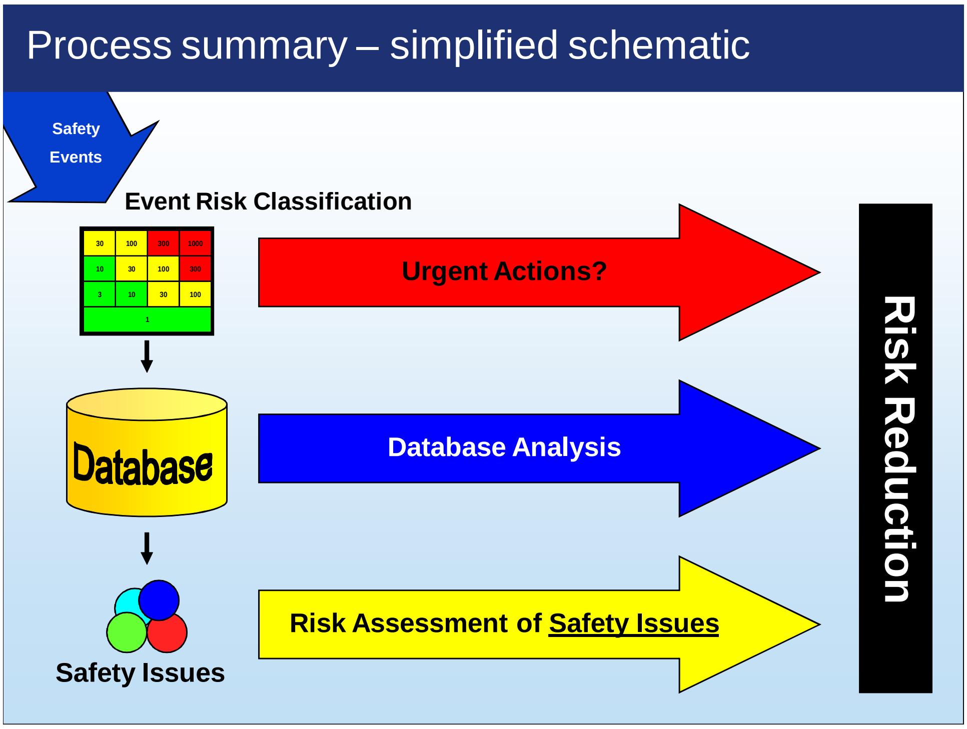
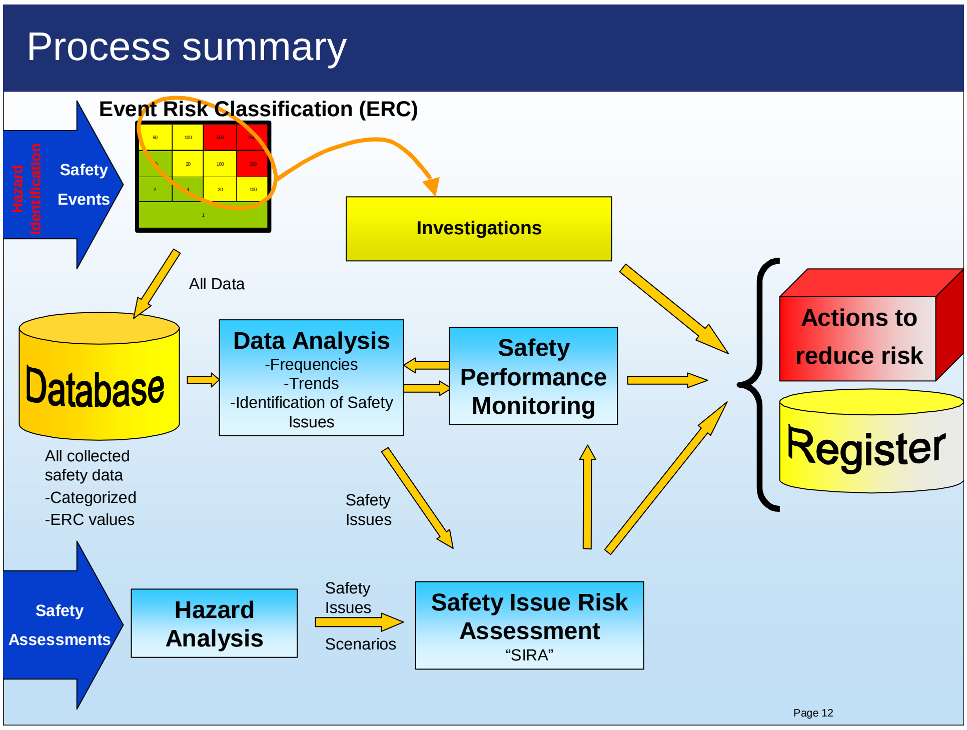

Process summary – simplified schematic

Figure 1. Simplified way to present the Risk Assessment process.

Figure 2 presents the same concept in more detail and with an additional input, Safety Assessment . It should be noted that for reasons of clarity some of the secondary arrows have been removed from this chart.



Process summary

Event Risk Classification (ERC)

Hazard Identification

Safety Events

Investigations

All Data

Database

All collected safety data
-Categorized
-ERC values

Data Analysis
-Frequencies
-Trends
-Identification of Safety Issues

Safety Performance Monitoring

Actions to reduce risk

Register

Safety Issues

Safety Assessments

Hazard Analysis

Safety Issues

Scenarios

Safety Issue Risk Assessment
"SIRA"

Page 12

Figure 2. The Risk Assessment process flowchart.

The same three steps that lead to risk reduction actions can still be observed in the diagram.

The proposed practical ERC application is a 4x4 matrix and the result will be red, yellow or green. An organisation will require red events to be investigated/actioned immediately and yellow ones to be investigated, but with less urgency. Green means "file the event in the database and use it for statistical analysis and continuous improvement". In this way, yellow and red events may lead to direct action, based only on one individual event. (See chapter 4, figure4)

All *actions* should be managed through the Register, which contains all the information concerning Safety Issues and assessed risk levels. The Register should also be used to track progress on "actions".

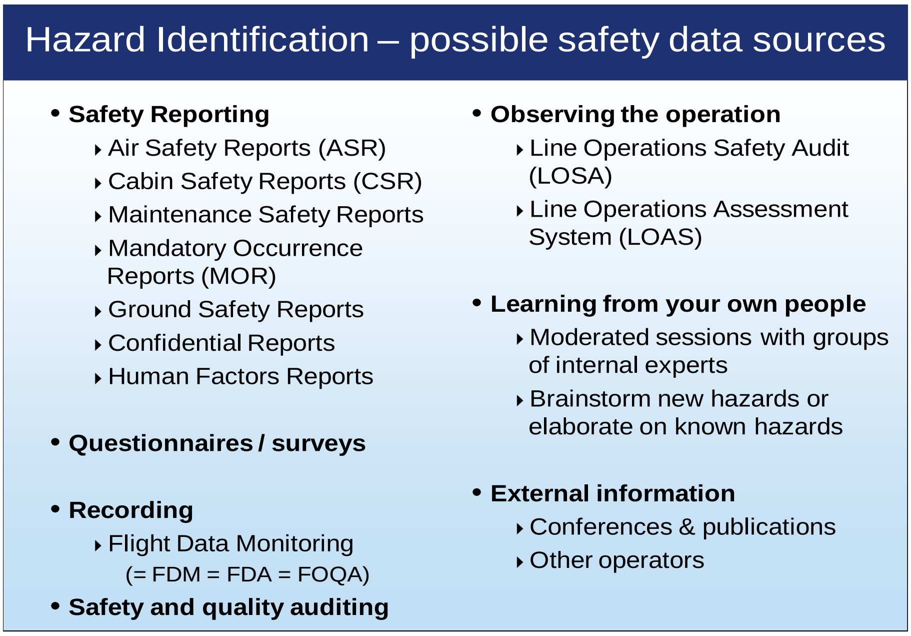
The other input to the overall risk management process is through a decision to carry out a Safety Assessment. When an operational change is planned a Safety Assessment should be launched to assess the associated safety risk. The first step is Hazard Analysis, which consists of listing all the potential hazards related to the change. Based on these hazards, the most critical related scenarios are developed, and can be assessed using the SIRA method. In some cases, there may be little or no data to help with the assessment so more subjective judgments will need to be made. (See section 4.10)

4 ARMS Risk Assessment methodology explained - step-by-step

The description of the Methodology in this chapter is supported by several documented examples in section 6.10.

4.1 The starting point: Hazard Identification data

There are several different sources and types of Safety Data, coming from the Hazard Identification process. A list of typical sources for an airline operator is presented in figure 3. For other types of aviation organisations there will be a range of other data sources available that could equally be considered.



Hazard Identification – possible safety data sources

- **Safety Reporting**
  - Air Safety Reports (ASR)
  - Cabin Safety Reports (CSR)
  - Maintenance Safety Reports
  - Mandatory Occurrence Reports (MOR)
  - Ground Safety Reports
  - Confidential Reports
  - Human Factors Reports
- **Questionnaires / surveys**
- **Recording**
  - Flight Data Monitoring (= FDM = FDA = FOQA)
- **Safety and quality auditing**
- **Observing the operation**
  - Line Operations Safety Audit (LOSA)
  - Line Operations Assessment System (LOAS)
- **Learning from your own people**
  - Moderated sessions with groups of internal experts
  - Brainstorm new hazards or elaborate on known hazards
- **External information**
  - Conferences & publications
  - Other operators

Figure 3. Typical sources for safety data.

The ARMS methodology deals with various types of Hazard Identification data. The main rule is that ERC is used for events (even when there is no actual consequence) and SIRA is used for issues (including hazards and latent conditions). Here some examples:

- *Observed events* would be entered and assessed in the same way as safety reports, with the ERC.
- *Observed findings* (threats, hazards, latent conditions) would be best analyzed with SIRA. In this case the first factor of SIRA, the “triggering event” would typically be the hazard.
- Audit findings can be assessed with SIRA. Findings from Questionnaires would follow the same logic.

- Fatigue is one of the Human Factor (HF) hazards that is currently receiving increasing attention and many organisations are implementing a Fatigue Risk Management System (FRMS) as one element of their SMS. The ERC provides a good tool for assessing the Flight Safety risk in reported fatigue related events (e.g. navigation error). On the other hand, many fatigue-related *Safety Issues* would be risk assessed using the SIRA (e.g. specific fatigue considerations of ultra-long-haul sectors).

Customisation of the ARMS methodology is discussed further in chapter 5.

4.2 Event Risk Classification (ERC)

The main objective of Event Risk Classification is to act as the first screening of all incoming safety data and to identify when urgent action is necessary. This type of screening is necessary whatever methodology is used for risk assessment. Typically, the event risk classification should take place preferably within one or two days of the event and be carried out by a person with operational experience who has been trained in risk assessment, hereafter called the Safety Analyst.

Section 2.2 and appendices 6.5 and 6.6 illustrate the problems when trying to perform event risk assessment with classic methods. To avoid such problems, the ERC within the ARMS methodology is based on the new concept of “event-based risk”[♣], which is an assessment of the risk associated with *that one event* and not the risk associated with *all similar events*. It should be kept in mind that the ERC may only be the first step in the risk assessment process and may be revised as a result of any investigation.

The ERC value is based on two questions:

- If this event had escalated into an accident, what would have been the most credible accident outcome?
- What was the effectiveness of the remaining barriers between this event and the most credible accident outcome?

It is worth noting that:

- The first question is looking to identify the accident outcome that is of most concern when this type of incident occurs, or put another way ‘what is the accident I am trying to avoid by having these incidents reported?’ This question is not asking for the most probable outcome, as that is usually “nothing” and therefore ignores any risk that the event carries, but neither is it necessarily looking for the worst possible outcome as the worst case scenario would often not be the most obvious accident to expect. For example, a low speed runway overrun or a ground collision during taxiing would be an accident but seldom one with 100% fatalities.

- There is likely to be some subjectivity between users in the answer to the first question depending upon how they consider the factors causing the event. However that variation is dealt with in question two through consideration of the remaining barriers, and hence the probability of that accident outcome. The risk colours and values in the ERC are intended to ensure that any variation in approach produces similar outputs in terms of risk (see appendix 6.8).

- In the longer term it is likely that organisations will identify the outcomes associated with types of events and hence remove the subjectivity associated with the first question for most incidents. Alternatively some users may wish to consider multiple outcomes but this, however is beyond the scope of the ARMS work at this stage.

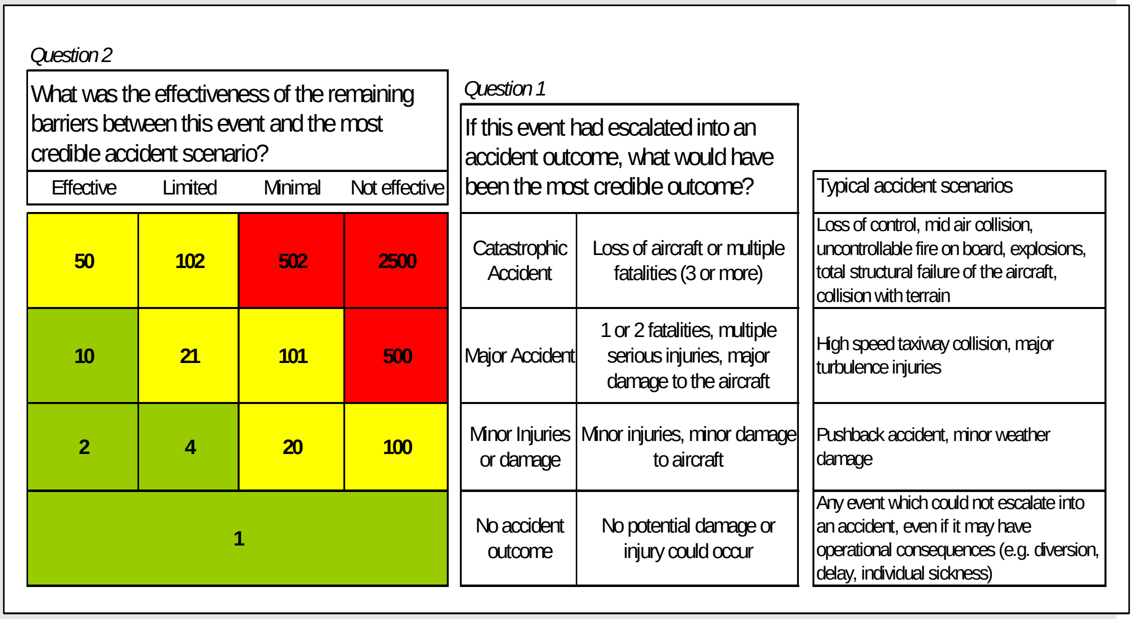
[♣] Described earlier in chapter 2.

- The second question only considers *remaining* barriers – to estimate the probability of further escalation into the most credible accident outcome (of Question 1). The barrier, which stopped the escalation, will be counted in (because it was still in place) along with any others that are believed to still remain. The already failed barriers will be ignored.

- It is recognised that there is still subjectivity in the answer to the second question and that expert knowledge will still be required to make an accurate categorisation. It is likely that some organisations will choose to develop methods to reduce this subjectivity.

- The reference in this analysis has to be *an accident*, because risk assessment only makes sense in relation to an accident. It does not change the fact that we manage incidents that are not actually accidents, it just recognises the fact that to measure the risk associated with incidents we need to reference them to the accident outcome. In some cases, the reference accident could be so minor that it would not qualify as an accident according to the ICAO definition. This explains the adopted use of the term "accident outcome".

The proposed practical ERC application is a 4x4 matrix, illustrated in figure 4 below.



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

Effective	Limited	Minimal	Not effective			Typical accident scenarios
🟨 50	🟨 102	🟥 502	🟥 2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
🟩 10	🟨 21	🟨 101	🟥 500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
🟩 2	🟩 4	🟨 20	🟨 100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
🟩 1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

Figure 4. ERC matrix

The following guidance helps in making coherent risk assessments.

Question 1: "If this event had escalated into an accident, what would have been the most credible accident outcome?"

- In your mind, try to escalate the event into an accident outcome.
- If it was virtually impossible that the event could have escalated into an accident outcome, then you are at the bottom row, at ERC value 1.

- If you can imagine credible accident scenarios (*even if improbable ones!*), then consider the most credible scenario and judge its typical consequence and pick the corresponding row in the matrix. The listed "typical accident scenarios" on the right of the matrix can be of help.

Question 2: "What was the effectiveness of the remaining barriers between this event and the most credible accident outcome?"

- To access the remaining "safety margin", consider both the number and robustness of the remaining barriers between this event and the accident scenario in Question 1.
- Barriers that already failed are ignored. Only the barrier which worked and any subsequent barriers still in place are taken into account.
- For the vertical column selection, you should pick:

→The extreme right column, if the only thing separating the event from an accident was pure luck or exceptional skill, which is not trained nor required

→The 3rd column from the left, if some barrier(s) were still in place but their total effectiveness was "minimal" – e.g. this could be a GPWS warning just before an imminent CFIT.

→The 2nd column if the effectiveness of the barrier(s) was "limited". Typically, this is an abnormal situation, more demanding to manage, but with still a considerable remaining safety margin – e.g. a moderate error in loadsheet or loading vs. slight rotation problems at take-off.

→The extreme left column, if the safety margin was "effective", typically consisting of several good barriers – e.g. passenger smoking in the lavatory versus in-flight fire accident.

It is good to keep in mind that the available information about the event at this stage may be limited and the ERC is performed based on this limited information.

Appendix 6.10 contains worked examples on Event Risk Classification.

The ERC has two outputs. **The first output** is a recommendation on what should be done about the event.

For example, using the provided ERC matrix, the results should be interpreted as follows:

🟥 → Investigate immediately and take action.

🟨 → Investigate or carry out further Risk Assessment

🟩 → Use for continuous improvement (flows into the Database).

In the case of a red result, the event can be considered to be a Safety Issue in its own right. In the case of a yellow result it may be investigated and/or risk assessed with more refinement. This may be done using the SIRA by first creating a Safety Issue based on the event or some aspect of the event (e.g. a hazard). For example, a GPWS event may reveal poor ATC routings at a particular location, which is then taken as a Safety Issue and risk assessed using the SIRA.

The Safety Analyst may, based on his/her own judgment, sometimes decide on a higher risk than the ERC would indicate.

The second output of the ERC is a number, called the ERC risk index. This index gives a quantitative relative risk value and is very useful in compiling statistics (see section 4.6 on Data Analysis)

In the proposed ERC matrix, the risk indices run from 1 to 2500 and each square in the matrix has a unique value. The rationale behind the choice of these risk index values is presented in appendix 6.8.

If there are several possible “accident outcome” scenarios that can be imagined, you should run the ERC process on each and pick the one that gives the highest risk index.

4.3 Investigations

The purpose of the in-house investigation is to find out more about the event and its causes. Its scope may range from one phone call to setting up a multi-departmental investigation team which might take several months to provide a final report. Investigations involving external bodies are not considered here.

The investigation may include:

- Telephone calls or meetings to get information from involved people or specialists
- Studying prevailing weather and other conditions
- Studying technical records
- Analysing the safety database and studying historical data on similar events or conditions
- Writing the results in a report, which may be placed into the safety software, linked to the event.

Typically, the investigation identifies causes, contributing factors and conditions. It may lead to recommendations and actions.

4.4 Actions to reduce risks

Risk Assessment as such does not reduce risk. The SMS of the company will specify the functional groups who are required to identify the necessary actions and to follow up their implementation and effectiveness. Typically, the Safety Action Group(s) will focus on both of these. The organisation may also have a high level Safety Review

Board which will concentrate on monitoring the overall risk level and the completion of key actions and recommendations in the Risk Register.

The (Risk) Register is of major help in tracking recommendations, both for implementation and effectiveness. (see section 4.9).

4.5 Safety database

In addition to the ERC, all the safety data should be entered into the safety database. It is necessary to have a *"structured"* database, which can be used for data analysis and where individual events can easily be found. The sequence of the tasks, i) Event Risk Classification (ERC) and ii) entry of the event into the safety database will vary, depending on the individual operator's software and procedures.

The safety database facilitates different kinds of statistical analyses, including charts on event numbers, risk levels and rates, sorted by various criteria. Such analyses may drive some action, even before a Safety Issue is formally raised and a more formal risk assessment has been made (middle (blue) arrow figure 1). Analysis of the safety database will also provide some measures for Safety Performance Monitoring.

To create a *"structured"* database, it is necessary to classify the data based on several criteria. Typical elements related to each event are, for example:

- Date
- Aircraft type
- Aircraft registration
- Departure point and destination
- Phase of flight
- Location of event
- Event descriptor or type
- Aircraft systems involved (list of keywords)
- Operational issues involved (list of keywords)
- Event Risk Classification risk index value

In addition to these factual elements it is highly desirable to create other structured data such as the event "type or descriptor" "causal factors" etc. This will be extremely valuable in future database analysis.
Often the database is contained in the safety software tool used by the airline.

All commercial tools include keyword or descriptor taxonomies for classifying the events. The needed level of sophistication of the database is a function of the airline size and complexity. Further description of software tools is beyond the scope of this document.

4.6 Data Analysis

The main purpose of Data Analysis is to identify the Safety Issues affecting the current operation.
Data analysis is about examining the safety database to identify trends and clusters of related events. It's a learning and discovery process from existing data.

Charts, graphs and filters are produced that sort events by different combinations such as:

- Time period
- Aircraft type
- Airport/approach
- Event types
- Keywords
- Aircraft systems involved
- Operational issues involved

Sometimes the results will immediately highlight issues that very obviously need to be addressed – even before a formal risk assessment. For example, if an approach to an airport has a very high rate of unstabilised approaches, the matter obviously needs to be addressed.

Results can be presented as "number of events" or as "rate of events", the latter being often more meaningful. For example, the number of unstabilised approaches per destination airport will be driven by the different number of flights flown to these airports. The home base may show a high number of events simply due to the high number of flights. Calculating the *rate* of unstabilised approaches *per all approaches flown to that destination* will give a clearer picture of the situation.

It is important to realise that neither "number of events" nor "rate of events" take into account the (potential) *severity* of the events. Therefore, looking at such statistics can be misleading. The ERC risk index values provide a valuable opportunity to move from this "number" focus to a "risk" focus, giving a much better basis for decision making. The ERC values may be used for any type of statistical analysis. How to do this? The following examples illustrate two possible ways.

Example 1.Accumulated total risk.
Sum together the ERC values of a batch of events and state the cumulative risk value as the total risk for that batch of events.

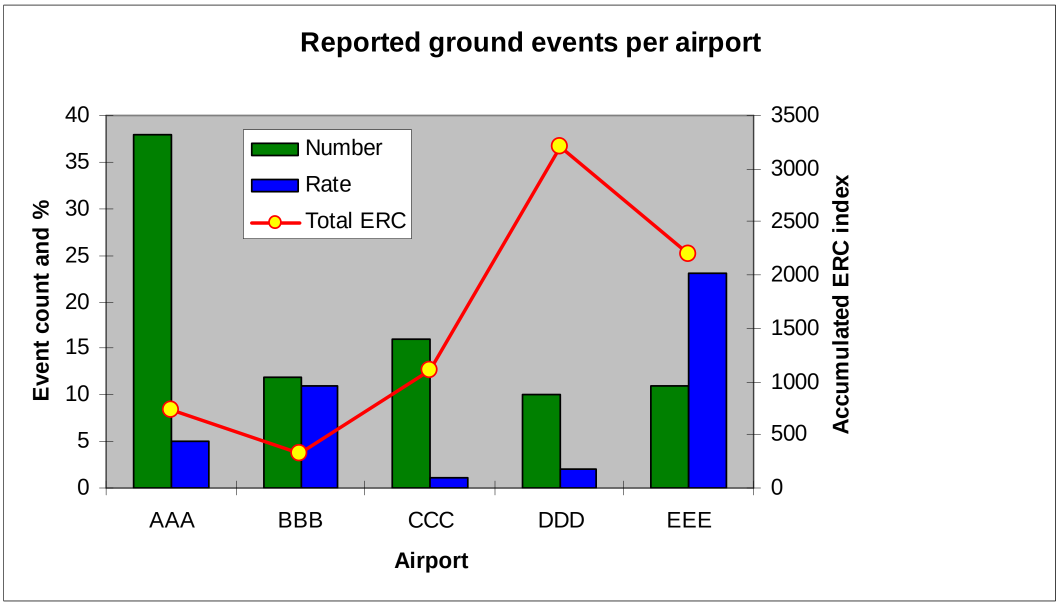


Figure 5. Fictitious example of cumulative ERC risk index use.

Figure 5 presents a fictitious example of a chart on ground events sorted by airport. This example illustrates the importance of looking at risk instead of only event numbers and rates. The results are presented as an event count, event rate and total risk per airport (cumulative ERC of all ground events in that airport). For airport DDD the risk is high despite a low event number and rate – i.e. the severity of the (potential) outcomes has been high in the events taking place in this airport. Therefore, the classic analysis based only on number/rate or events would lead to underestimating the importance of ground events at DDD. In fact, “ground events at DDD” could typically become a Safety Issue.

Example 2: Reporting rates per year
This is an example of adding the ERC colours to event rates per year.

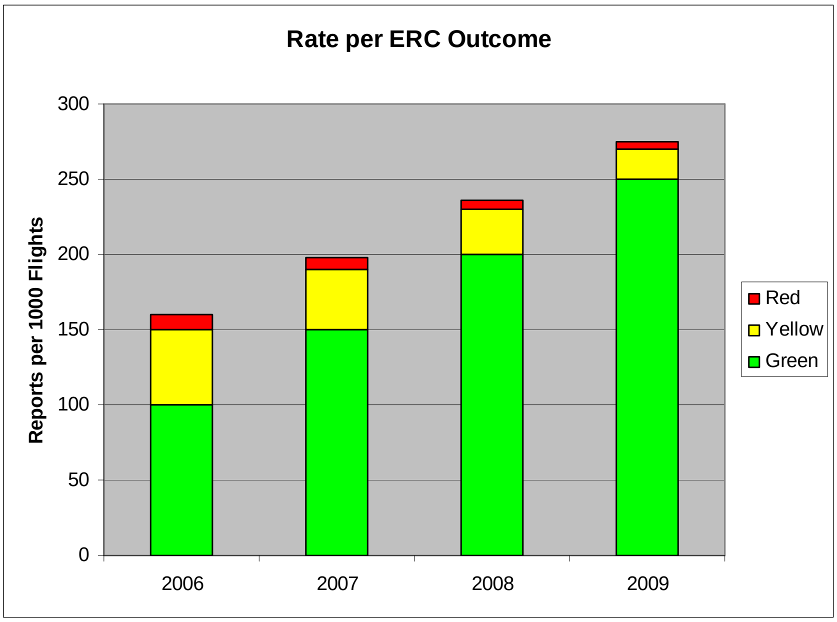


Figure 6. Fictitious example of ERC Outcomes relative to number of flights over four years

In this example every event from the database is grouped by the ERC outcome (red, yellow, green) per 1000 flights. This gives event rates per ERC outcome and can be monitored over time (per year or month for instance).

Other options include calculating the mean and/or standard deviation of the ERC risk index values. These can be used to assess the relative risk of such factors as aircraft type, location, safety event type etc. In addition trends of these values over time are very useful in Safety Performance Monitoring. See next section.

Remember that ERC risk index values are for *relative* risk, i.e. they are used for *comparing* different risks, not as absolute values.

4.7 Safety Performance Monitoring

A key requirement in SMS is to monitor the Safety Performance of the organisation. The purpose is to ensure that the target safety performance (and at least a minimum acceptable level of safety performance) is achieved. In practice, the data used for Performance Monitoring is virtually the same data that is used for Hazard Identification and Risk Assessment.

Safety Performance Monitoring can be based both on:

- Measures coming directly from some Hazard Identification source (e.g. safety reports or flight data)
- Risk-based measures.

The former tend to give information about a very specific and narrow aspect of the operation and are usually limited to a number or rate, thus not integrating the potential severity dimension. Risk-based parameters can give a more comprehensive picture of Safety Performance. They can be used at different levels:

1. Normal, Hazard Identification –based Safety Performance Indicators (SPI's) can be transformed into risk-based measures by replacing the event number with the accumulated ERC value. Such Safety Performance Indicators could be created to follow, for example:

- Total risk associated with Maintenance events
- Total risk of unstabilised approaches
- Total fatigue induced risk

2. Safety Issue Risk Assessment (SIRA) result values can be used in creating more global Safety Indicators, which are monitoring the risk of the identified Safety Issues. For example:

- Risk of "flying in uncontrolled airspace"
- Risk of "operation into airport XXX"

3. Using measures from 1 and 2 above it is possible to build an indicator which tracks the total operational risk.

The targets can be set, for example:

- As an absolute/minimum value
- As an allowed time above/below a certain limit
- As an allowed variation range (e.g. two standard deviations from mean)
- As a risk trend

4.8 Safety Issue Risk Assessment (SIRA)

As a result of data analysis, the organisation will gradually identify a number of Safety Issues affecting its operation. These must be risk assessed using the Safety Issue Risk Assessment (SIRA).

The first step is to define and scope the Safety Issue properly. Typical aspects to define are:

- Safety Issue title
- Description of Hazard(s)
- Description of related accident scenario(s)
- A/C types considered
- Locations considered
- Time period under study
- Departments whose involvement in the assessment is necessary
- Other

Defining the Safety Issue properly makes the assessment more factual. For example, once the airports have been fixed, the exact runway lengths are known; once the time period is fixed, the frequency of flights to various destinations and the current status of the aircraft (modifications, etc.) become fixed.

Sometimes, before making the quantitative SIRA assessment, the Safety Issue might have to be split into two or more sub-Issues. For example, if the Safety Issue is "approaches to airport Z", where airport Z is a high-elevation airport with a short runway, the Safety Issue may have to be split to two sub-issues: one to cover the risk of hard landings and another to cover the risk of runway overruns. The reason for splitting is that the applicable barriers, triggering events, etc. for the sub-issues may be different – therefore requiring a separate analysis for each of them.

SIRA assesses the risk using a formula where risk has four factors.

- Frequency/probability of the so-called Triggering Event
- Effectiveness of the Avoidance Barriers
- Effectiveness of the Recovery Barriers
- Severity of the (most probable) accident outcome

The background for this method is explained in appendix 6.9.

ARMS has developed an Excel-based application to illustrate how SIRA can be carried out in practice. This tool goes through the SIRA process step-by-step, starting with the Safety Issue definition, then describing the triggering event, all barriers and the accident outcome. Finally, a numerical estimation for the first three factors is made and the severity of the potential accident outcome is estimated, similarly to ERC. A factor of 10 of difference is used between the barrier effectiveness classes to make the choice easier (e.g. the barrier will fail "once in 100 times", or "once in 10 times"). . This Excel based tool is available at www.skybrary.aero.

JAR/FAR-1309 limits are used to produce the output result on a scale of five levels of risk:

Unacceptable levels of risk:

- *Stop*
- *Improve*

Tolerable levels of risk:

- *Secure*
- *Monitor*
- *Accept*

The exact meaning for each of the results has to be defined at the company level. Here is *an example* of what the results could mean:

- Stop: the concerned part of the operation (e.g. destination, aircraft type, procedure) has to be discontinued immediately until an acceptable risk reduction measure has been implemented. The matter receives immediate top management attention.
- Improve: Issue has to be raised and actioned at the Safety Action Group (SAG) and monitored at the Safety Review Board. Risk reduction measures

need to be identified and started within an agreed time frame. If risk reduction to acceptable level is not reached within agreed time period, top management decision about risk tolerance is required at the Safety Review Board level.

- Secure: The risk level and its trend needs to be monitored continuously (at least at SAG level) in order to prevent escalation to unacceptable level. Reinforcement of existing measures should be discussed at the next convenient opportunity (e.g. at next scheduled SAG meeting) and taking further reduction measures should be considered.
- Monitor: The Issue is followed regularly through the routine practice of database analysis and the monitoring of SIRA values for all Safety Issues in the Risk Register, i.e. it stays in the list of current or anticipated Safety Issues.
- Accept: No specific action is required since the risk is well within the acceptable level.

- The exact meaning of each risk level and the required action must be defined and agreed with company Senior Management. What is tolerable and for how long? How are high-risk Safety Issues and related actions monitored? This should be documented in the organisation's SMS Manual.

The Excel tool features a dedicated field where the result can be commented by the Safety Analyst. For many organisations the Excel tool may be a sufficient way of tracking Safety Issues. New worksheets can be easily cloned from existing ones and used as templates for SIRA updates.

SIRA is also applicable to Safety Assessments as a part of the *Management of Change* process. This aspect is covered in sections 4.10 and 4.12.

4.9 Risk Register

The risk register contains the information on identified risks that is necessary for managing them. Typical contents are:

- Safety Issues
- Their risk values
- Agreed actions
- Responsible people and target dates for actions
- Progress with actions and impact on risk levels

The Register is a good tool for people in line operations and the Safety Office working on safety management.

Some organisations may choose to track risks at a more refined level and include in the Register:

- Triggering events
- Undesirable Operational Events (UOE)
- Barriers and their tracked effectiveness[♣]

[♣] The issue of tracking barriers and their effectiveness is a vast topic in itself and may become an important aspect of a Safety Management System. However, even though the ARMS working group

- Safety decisions (which have to be recorded somewhere, anyway)

4.10 Safety Assessments

A Safety Assessment is a Risk Assessment focusing on a specific part of the operation. The objective is to assess whether that part of the operation is safe enough, i.e. whether the risk level is acceptable. Usually the focus will be on a *new or changing* part of the operation and the objective is to ensure that the planned operation will be safe. In this case, the assessment should be made before the decision on the new operation is taken; but in any case before the new operation is started.

The origin for the assessment could also be a *change* in the operating environment, as opposed to an internal company decision.

In both above cases, the Safety Assessment is part of the *Management of Change function* of the SMS. There will be not be complete company data that could be used in the risk assessment because the focus is in a *future* operation.

Sometimes Safety Assessments are made for *already existing* parts of the operation. In this context they are often called *Safety Cases* and the objective is to ensure that the safety level is (still) acceptable. In this case, company safety data should be available to support the assessment.

In addition to the main objective of assessing the risk level of the operation under focus, it is usually desirable to assess:

- If the risk level is too high, could it be reduced to an acceptable level?
- If yes, how?
- How difficult and expensive would it be?

Answers to such questions will be essential for the top management when they are evaluating the feasibility and profitability of a new operation.

It is important to realise that Safety Assessments are not merely a procedural step in the Change Management process. Their usefulness derives from the consequential actions that are taken to reduce the identified risks. The actions must be tracked to ensure that the risks are reduced as planned.

The proposed method for carrying out the Safety Assessment is first to identify and analyse the associated *hazards* and then use the Safety Issue Risk Assessment (SIRA) technique to assess the risks related to the identified hazards. This method works when there are enough factual, quantifiable elements to feed the SIRA (e.g. new GPWS recovery procedure)

It should be noted that for purely qualitative “soft” changes (change of management structure, outsourcing of a service) it may be impossible to quantify the risk using ARMS or any other such method and hence the SIRA technique cannot be used. In such cases the assessment needs to be of a qualitative nature, based on judgments

identified many challenges in this area and discussed the topic, the issue is outside the scope of this document.

made by experienced people. A fully qualitative but “as objective as possible” estimate must be made using a defined process, typically in an evaluation group.

For all Safety Assessments, a key issue is: *how is the Assessment triggered*. A systematic triggering mechanism needs to be in place. This could be a permanent agenda item at the SAG and SRB to discuss whether anything “in the radar” would require a Safety Assessment. The SAG and SRB will also have to review and decide whether or not the result of a Safety Assessment is acceptable.

Examples of Safety Assessments are developed in appendix 6.10.

4.11 Hazard Analysis

Once the focus area of the Safety Assessment has been precisely defined it will be possible to list the related hazards. This can be done either systematically by using a recognised method, like FMEA (Failure Mode and Effects Analysis), or through an evaluation by a group of knowledgeable people.

A list of identified hazards in itself does not always provide the necessary material for SIRA. Hazards tend to combine with each other and with other factors such as visibility conditions. Therefore, the next step is to build *scenarios* where the identified hazards create Undesirable Operational States (UOS) that could result in an accident.

4.12 Using SIRA for Safety Assessments

The Hazard Analysis step typically produces several potential hazards and several potential accident outcomes, around one or more UOS’s. It may then be possible to limit the study to the most critical outcomes.

The scenario(s) must now be entered into the SIRA framework. This means identifying the UOS and the related most probable accident outcome, the triggering event and the barriers. The SIRA method would then be applied as explained in section 4.8 and illustrated through the examples in appendix 6.10. The Hazard Analysis step should have produced most of the data required for the SIRA.

In the case of several scenarios, the one producing the highest risk would drive the overall risk level of the Safety Assessment, but all scenarios could drive the resulting risk reduction actions.

5 Customisation issues for different types of organisations

Like in SMS in general, one of the most challenging aspects in setting up a well-functioning Risk Management process is that it needs to be customised to the specifics of the organisation in question.

Throughout the document, a clear distinction is made between the conceptual methodology, which should be universal, and the practical implementation of the methodology (printed on a grey background), which may be more or less customised at the company level. In addition, this chapter addresses some specific customisation issues.

5.1 Organisations without flight operations

As stated in section 3.1, the main focus of the ARMS Methodology is on *Flight Safety risks*, i.e. any risks that could harm the occupants of an aircraft (passengers and crew). Only organisations running a Flight Operation are directly exposed to Flight Safety risks.

It is important to realise that managing the Flight Safety risk is also the primary safety objective for the complete aviation system as a whole. Therefore, ideally, any risk assessments done anywhere in the aviation system should relate to the Flight Safety risk.

The aviation system consists of a large number of various service providers, most of whom do not exercise a flight operation and therefore will not have aircraft accidents but who can contribute both positively and negatively to flight safety as both a source of hazards and through controlling some barriers. It is easy to illustrate this by thinking of Maintenance Organisations or Air Traffic Control centers.

How should such organisations without flight operations carry out risk assessments? Sometimes their choice has been to assess risk in relation to an intermediate negative outcome, which has typically been;

- Releasing an unairworthy aircraft – for a maintenance organisation, and,
- Total loss of air traffic service capacity – for an ATC organisation.

The problem with this approach is that neither of the mentioned intermediate outcomes is actually an accident. The “unairworthy aircraft” state can be reached in hundreds of different ways, some of which induce an extremely high flight safety risk while others induce no flight safety risk at all. Therefore, such risk assessments need to ensure that there is a strong relationship between the assessed “airworthiness risk” and the flight safety risk. It is desirable that the MRO should risk assess both airworthiness and flight safety. It must be recognised that the SMS of an MRO will have a Hazard Identification and Risk Management process to identify safety issues and ensure that corrective action is taken. Some events that have a low or negligible flight safety risk may be as a result of a systemic failure that could manifest itself in a much more serious manner. The Risk Management process must ensure that action is taken and that such events do not fall into the “green” “no action required” category because there was no actual “accident outcome”.

One of the conclusions of the ARMS working group is that risk assessments in such aviation organisations should, if practicable relate to the ***flight safety*** *risk, in addition to the airworthiness risk*. In most cases, this will require working together with other organisations and especially the one running the Flight Operation[♣]. The service provider needs to know what is the real risk to flight operations created by various hazards they produce. The flying organisation needs to know what is the expected frequency of the triggering events (at the service provider) and how good the barriers on the service provider side are. The SIRA is a very useful tool for structuring such a dialogue and working towards the actual flight safety risk.

The ARMS Methodology is fully applicable to various types of aviation organisations and not only to organisations with flight operations. Relating to flight safety risks is a challenge, but using ARMS can help in meeting that challenge. Both ERC and SIRA are supposed to be used in relation to the potential outcome in the flight operation. Appendix 6.10 contains examples to illustrate this point.

The conceptual idea of ARMS could be used to make additional versions of ERC and SIRA for an MRO for example. Each event could be assessed in parallel using the different ERC’s and provide different index values. This way, different types of risks could be managed in parallel. Occupational Safety and Health (OSH) risk could also be assessed using the ARMS concepts. Such “customisation”, however, is beyond the scope of this document and is left to the individual organisation or future working groups.

5.2 Large organisations

In large organisations with high data quantities the need for systematic, robust processes, coherence and minimising analysis time per report become important requirements. Good tools and automation are critical success elements. The high number of data elements is both a blessing and a problem: Workload is increased but on the other hand many things become quantifiable.

One thing that may prove useful when faced with high report quantities is the use of templates, which guide the analyst in classifying similar repetitive events in a consistent way. For example, the following types of events may be reported in large quantities with almost identical content:

- Birdstrikes
- TCAS alerts
- Minor technical failures
- Passengers smoking in lavatories

[♣] See the excellent presentation by Jean-Marc Cluzeau, presented to the EASA workshop on SMS, 15-16 January 2008. Link to the presentations: http://www.easa.eu.int/ws_prod/g/g_events_archiv.php

In addition, there may be time periods when a specific problem repeats with very high frequency (technical condition, weather phenomena, work in progress at an airport, etc.). In such cases, it is good to have a well-documented, consistent way to classify the events, based on a few simple rules. Naturally, the template would give only the default result – if any additional factors were present, the analyst would have to correct the result.

Another potentially useful function can be a semi-automatic detection of Safety Issues. A data-mining tool could scan the safety database and propose certain detected patterns to be raised as potential Safety Issues. The detection can be based on the frequency or increasing trend of any value in the database (by aircraft tail number, aircraft type, aircraft system, time of year, airport, phase of flight, etc.). This way, at least the easily detectable patterns can be detected semi-automatically, leaving more analyst resources for finding the more challenging Safety Issue patterns. In addition data mining tools have been shown to be good at detecting associations that are easily missed by a normal analytic scan.

In a large organisation, with more data, it will be possible to quantify various phenomena. For example, in SIRA, it may be possible to use historical company data for estimating the frequency of a "triggering event" or the robustness of a barrier.

From the organisational point of view, there may be more resource available but also more data to analyse. A good software tool is vital for managing the data and making it available to all user groups.

In large organisations there are likely to be several people who perform risk assessments. This can lead to inconsistency. Therefore the consistency of risk assessment needs to be monitored in the Safety Management System.

5.3 Small organisations

Using the ARMS methodology in a small organisation is not different from what has been described in this document. Typically, the small size may be reflected in data quantity, available tools, available human resource and expertise and the level of support provided by the company infrastructure. These factors, which can be perceived as difficulties, may be balanced by more direct communication channels, low bureaucracy and faster capability to take action and to adapt to changing conditions.

Both ERC and SIRA can and should be used as described. Low quantities of data may be a challenge for detecting Safety Issues, assessing them with SIRA and for setting up a credible Safety Performance Monitoring system. This increases the desirability of channelling the various types of safety data to one single database, or to put them through the same ERC, if possible. As for the database solution itself, it may be both acceptable and a cost-imposed constraint to use a simple inexpensive solution though the cost of commercially available tools is usually a function of the number of users, making them more affordable to small organisations.

Safety Assessments must be carried out, just as for any other type of organisation. Again, external data may be very useful for quantifying various factors in the analysis.

Due to low data quantities, smaller organisations can have the tendency to witness the following effects:

- Every event category/keyword etc. gets a low number of "hits" thereby making statistics based on "count" difficult to use
- This increases the value of ERC-based risk statistics and analyses, which will allow easier prioritisation of issues.
- It becomes crucial to use external data both for studying Safety Issues with SIRA and for any Safety Assessments. The slogan is: "if it happened to someone else with the same a/c type / destination / engine / etc, couldn't it happen to us too?"

5.4 Customisation of risk matrices

The ERC and SIRA are definitely the areas where many users will be tempted to customise. There are several potential areas for customisation:

- ERC matrix colours
- ERC risk index values
- Guidance text around the ERC matrix (for columns and rows)
- Way to manage the SIRA calculation process (Excel, multiple matrices, etc.)
- Phrasing of the four SIRA dimensions (the questions)
- Phrasing of the SIRA answers
- Meaning of the various possible results, for both ERC and SIRA

While customisation often brings added value and is sometimes necessary, it may lead to bigger changes than actually intended. A seemingly small change may actually be a fundamental change to the method, and this may go unnoticed. Moreover, the benefits of customising should be weighed against the benefits of harmonised methods with somewhat comparable results from one user to another.

For each customised risk matrix, the exact meaning of each risk level and the required action needs to be defined and agreed with the organisation's senior management. What is tolerable and for how long? How are high-risk Safety Issues and related actions monitored? (See section 4.8).

Here is a summary of do's and don'ts for ERC and SIRA customisation.

ERC do's:

- If you need to assess incoming events based on multiple 'risk dimensions' like *airworthiness, cost or company image*, create an additional ERC so that each event is classified separately for each type of risk and so each result can lead to different types of action. This may be unrelated to actual flight safety risk, but can be a suitable practical arrangement in the real operational environment, where other risk dimensions need to be considered.
- Adapting the ERC for a maintenance or ATC organisation will involve changing some of the wording. It is however crucial that, where the ERC is

being used to classify flight safety risk, the vertical axis still refers to real flight safety accident outcomes and not intermediate outcomes such as 'Unairworthy aircraft' or 'Loss of separation'. Where an ERC type approach is desired to assess the risk of these "intermediate outcomes" this should only be considered as a subset of the ARMS ERC approach.

- Leave the final risk classification decision to the Safety Analyst.
- You can propose some guidelines for the most frequent cases, but highlight that they are only basic guidance and that the Safety Analyst has the final say.
- After any change in the ERC, make sure that it is correctly calibrated, i.e. events that should get a high risk class, actually get it, and vice versa.

ERC don'ts:

- Do not try to give very precise guidance for each column/row. In practice, such guidance only works correctly with some of the data but not with all of it. E.g. "emergency" may be a good guidance for many cases of "minimal" barrier effectiveness but not for all of them.
- By the same token, do not overanalyse the existing terms (e.g. "limited"). Consider that you have four classes ranging from 'very high safety margin' to 'no margin' and try to position the event to the class where you think it best fits.
- A typical error in trying to create guidance for the horizontal axis is to start referring to "what stopped the accident sequence" which is not the same as the correct concept of "what was left".
- Do not try to take the thinking and judgment away from the Safety Analyst. (S)he is the only one who can assess the event in a holistic manner, taking into account all known factors, the context and the environment.
- Do not change the ERC risk index values unless you can justify the revised numbers to someone else.

SIRA do's:

- The example Excel application is only one way to implement the SIRA. Feel free to implement it in another way, while respecting the principle of creating the result based on the four given factors.
- Make sure the SIRA is correctly calibrated, i.e. Issues which should produce an "unacceptable risk" result, do produce it, and that low risk issues do not get too high a risk rating. It may be a good idea to use a recognised reference like the JAR/FAR-1309 to set the tolerability limits.
- In building the SIRA method, define the Safety Issue as precisely as possible, so that the assessment becomes as factual as possible – minimising the subjectivity.
- Make sure the range of the input parameters is sufficiently large, covering, for example, very frequent "triggering events".
- Use flight hours instead of flight sectors when more suitable and adapt the method accordingly.
- Be clear when the assessment is made for the whole operation and when it is made only for a part of the operation. For example, the risk level of a Safety Issue present only at one destination may be "compensated" by the relatively low percentage of flights going to that destination, while the risk may well be

unacceptably high for the flights to that destination. In such cases, the risk should be assessed exclusively for the flights to the affected destination.

- Try to use hard data as inputs to the SIRA whenever possible.

SIRA don'ts:

- Do not try to apply a detailed, quantified SIRA to issues which are unquantifiable (senior management change) or too large (merger with another airline). In such cases, a simpler, more subjective method can be used by a qualified group of people.

6 Appendices

6.1 The ARMS Mission Statement

The Mission of the ARMS Working Group is to produce useful and cohesive Operational Risk Assessment methods for airlines and other aviation organisations and to clarify the related Risk Management processes.

The produced methods need to match the needs of users across the aviation domain in terms of integrity of results and simplicity of use; and thereby effectively support the important role that Risk Management has in aviation Safety Management Systems.

Through its deliverables, the Working Group also aims at enhancing the commonality of Risk Management methodologies across organisations in the aviation industry, enabling increased sharing and learning.

In its work, the Working Group sought contributions from aviation safety experts having knowledge on the user needs and practical applications of risk management in the operational setting.

The deliverables of the Working Group are methodology definitions –and not software tools.

The results of the Working Group are available to the whole industry.

6.2 Birth of the ARMS Working Group

The need for a good operational risk assessment method has existed for a long time. The emergence of Safety Management Systems and the related ICAO Standard underlined this need.

The initiating kick for ARMS came when Andrew Rose (then BA, later NATS) and Jari Nisula (Airbus) met at the “FAA 2006 Conference on Risk Analysis and Safety Performance in Aviation” in Atlantic City, NJ, where both were speakers. They shared a common understanding of the problems with risk assessment and agreed to try to initiate some work towards a better method. After some months of developing an initial list of objectives and problem statements the two co-chaired a workshop in June 2007, hosted at Airbus in Toulouse, France.

ARMS was born as a result of that first workshop, where people showed commitment to work together on this topic. The name ARMS (proposed by Ivan Sikora, Emirates) was initially only the name for the virtual working space, the NLR-hosted SharePoint (Airline Risk Management Sharepoint). The group gradually became known under the name ARMS, which was then agreed to stand for Airline Risk Management Solutions.

6.3 ARMS Working methods

The ARMS development work was a balanced cooperation of more than 10 people, where different parts of the solution got major contributions from several subgroups and through valuable individual innovation by different ARMS members.

The following 2-day workshops were held:

Toulouse (hosted by Airbus), Jun-07
Main focus areas: shared understanding of the issues, scoping the work, learning about current practices and proposed solutions.

Amsterdam (hosted by NLR), Mar-08
Main focus area: method for risk assessing one single event.

Lisbon (hosted by TAP), May-08
Main focus areas: managing several risks, organisational context of risk management.

Geneva (hosted by easyJet), Sep-08
Main focus areas: refinement of methodology, documenting.

Toulouse (hosted by Airbus), Nov-08
Main focus areas: Finalising development, focus on deliverables.

There was significant development work taking place between the workshops. The following teleconferences were organised:

- 18-Jun-08 teleconference + webex
- 24-Jul-08 teleconference + webex
- 09-Oct-08 teleconference
- 04-Nov-08 teleconference + webex

During workshops, work was done both in sub-groups and as one big group. Workshops were prepared and chaired by Jari Nisula, except the first one where the role was shared with Andrew Rose.

Year 2009 and the first two months of 2010 were dedicated to two related tasks: testing the methodology in real life and documenting it comprehensively.

Creating this main document, together with a few other documents (e.g. PowerPoint presentations) was the principal task of this time period. They are aimed at providing a useful set of tools for communicating the methodology. The contents of these documents were guided and enriched by the real-life experiences of airlines and other aviation organizations who had started using the methodology. Numerous teleconferences were organised in 2009 and 2010 to discuss the project and to obtain collective agreement on the contents of the documentation.

6.4 ARMS Members

The participants in the first workshop (June 2007) were a mix of people who:

- Had practical experience on operational risk assessment at airlines and the related needs and challenges
- Came to present proposed solutions to some parts of the Risk Assessment challenge, including methods and software tools.

After the first workshop the Working Group started developing the new methodology. The members came mainly from airlines – some from other aviation organisations. In practice, a core team was formed, which was instrumental in the work; while some other people / organisations contributed to some extent during the development period, or remained in communication with the ARMS group. Initially all interested people were welcomed to join the group, until the growing group size limited this. A few new members joined in towards the end of the development, which was a good time to bring in new eyes and have another reality check on the deliverables.

ARMS Working Group members and contributors:

Capt. Charles Barbknecht	Air Berlin
Capt. Andreas Beaujean	Air Berlin
Harard Hendel	Airbus
Jari Nisula	Airbus
Jean-Marc Cluzeau	Air France Industries (replaced by Franck Danthez)
Tom O’Kane	Aviation Safety Consultant (ex-BA)
Dr. Kwok Chan	Dragonair
Gavin Staines	DHL
Capt. Dave Prior	easyJet
Capt. Philippe Pilloud	easyJet Switzerland
Ivan Sikora	Emirates
Dave Stobie	Emirates
Harri Koskinen	Finnair
Capt. Mika Pyyhtiä	Finnair
Capt. Kristjof Tritschler	Germanwings
Martin Nijhof	KLM
Capt. Ruud Wittebol	KLM
Simon Gill	Mirce Akademy
Andrew Rose	NATS (ex-BA)
Joao Brites	Netjets
Claudia Cabaco	Netjets
Gerard van Es	NLR
Michel Piers	NLR
Filip Denoulet	Privatair
Jan Peeters	Privatair
Bob Dodd	Qantas Airways
Nancy Harmer	Shell Aircraft International
Liam Sisk	SR Technics, Dublin
Marie Ward	SR Technics
Capt. Carlos Nunes	TAP
Capt. Martin Fleidl	Tyrolean Airways

6.5 Limitations of current methods

As discussed in section 2.2, there are conceptual difficulties in risk assessing historical events. The first fundamental question one has to answer is: *which* risk is assessed. Theoretically, there are four choices:

1. What **is** the Risk of an accident? (ZERO – there **was** no accident)
2. “What **was** the Risk that the event **would have** escalated further in an accident, yesterday, given what had already happened”?
3. “What **is** the Risk that **exactly** the same **will happen** again and end up in an accident”?
4. “What **is** the Risk that a **similar** event **will happen** in the future and end up in an accident”?

Usually, without posing this question consciously, analysts tend to try to assess risk 4, i.e. the risk of a *similar* event taking place in the future. The problem is that “*a similar event*” is not at all defined. The only thing that is said that *it is not exactly the same*♣. This results in a significant amount of subjectivity in the assessment.

This approach led to the following problems:

- There was confusion about “severity of *what*”. Some analysts were rating based on the severity of the *actual* outcome of the event, some on the *potential* outcome and some on what is considered a *credible outcome* . This is all very subjective.
- “Likelihood of recurrence of *what”* – confusion. The event will never reoccur exactly the same, so in fact the question is about the recurrence of *something similar*, which is extremely subjective. For example, if the event was a birdstrike at takeoff from JFK affecting an A320, should one consider the typical frequency of such events on A320’s only, all similar size a/c in the fleet or all a/c types; should one consider JFK only, all NYC airports or all airports in the current network; should one consider takeoffs only or also approaches?
- Once the risk assessment has been done, each event has a risk value, which is dependent on the likelihood (in practice the frequency) of *similar* events. Therefore, if the frequency of the event type changes, theoretically the analyst should re-assess the past events because the “likelihood of recurrence” value should now be updated. If this is done, it introduces a huge workload and an extra management task. If it is not done, the risk assessment is no longer correct.
- When organisations want to have an idea of the total risk, they may want to sum together the risk values of individual events. For example, they may follow the trend of the total operational risk in time or compare the total risk of birdstrike events to total risk of turbulence events. In this case, such cumulative risk values are not correct because the likelihood/frequency has already been taken in account when the risk for each event was assessed. The result would reflect roughly (severity x likelihood) x likelihood, which is biased too much towards likelihood at the expense of severity.

♣ It is a bit like defining someone’s nationality by saying “she is *not* Italian”.

6.6 Limitations of current methods – example

You learn about an event, which took place yesterday:
A single-aisle aircraft with 110 passengers almost overran the runway end at landing due to a maintenance error affecting the braking capability. Actual outcome: a few blown tires.

If you try to apply the classic *severity x likelihood* formula (in line with what has been explained in section 7.5) you are now faced with the following questions:

Severity of what?

- Actual outcome: blown tires?
- Most likely potential accident scenario: overrun with some injuries & major aircraft damage?
- The worst-case scenario: overrun with 100% fatalities?
- Shall you consider bigger A/C? More passengers? Critical airports?
- Etc.

Likelihood of what?

- The same maintenance error?
- Near-overrun events?
- Actual overrun events?
- Any A/C type? Any location?
- Etc.

These options illustrate the significant subjectivity of the older methods, primarily caused by the ill-defined object of the risk assessment.

6.7 Event-based Risk and the ERC

Event-based risk refers to the risk that was present in the experienced event, without trying to consider all ‘similar’ events. Instead of trying to risk assess “a similar event in the future”, it risk assesses the *risk that was present* in that one event, that day.

For determining the event-based risk, the guiding question is: “how worrying was the event as an experience”. When one analyses what makes some events more worrying than others, one can identify two key dimensions:

- How close did it get to a potential accident?
- How bad would the accident have been?

Refining these questions, the first one becomes: “What was the effectiveness of the remaining barriers (between this event and the most credible accident outcome?” and the second: “**If** the event had escalated into an **accident**, what would have been the most credible outcome?” These two dimensions link perfectly with the definition of risk: The first one with ‘probability’ and the second one with ‘severity’. Therefore, the resulting value is not ‘severity’ but ‘risk’.

As each risk value now belongs to and depends only on one single event, these risk values can be used to get correct cumulative risk values by summing the individual values together. This way, one could get a total risk value for one airport, one particular route, one approach, all birdstrike events or for one particular month, etc.

6.8 Rationale behind the proposed ERC risk index values

The choice of the proposed ERC risk index values is based on the following considerations:

- It was agreed that the scale both horizontally and vertically needs to be exponential. A linear scale would not reflect the needed difference of "weight" between the classes.
- Looking at the real reported events, the difference of risk between the least and most risky event is indeed very significant. Therefore, it was agreed that the difference in the order of magnitude between the lowest and highest index needs to been in the range of 1 to 1000.
- Real accident data was studied and the accidents were classified based on Question 1 of the ERC. It was observed that the relationship between the quantified losses in each class was 1:5:25. This was used on the vertical scale. For symmetry purposes the same relationship was used for the horizontal scale.
- The bottom row is one single block instead of four squares. This is because the bottom row corresponds to the case "No potential damage or injury could occur" and therefore it does not make sense to estimate the "effectiveness of remaining barriers".
- In the first version of the ERC matrix some squares contained identical risk index values. It was decided that each square should have a unique number, so that the index value would immediately indicate its place in the matrix. Furthermore, from a software perspective, a single numerical field is now enough to capture the result of the Event Risk Classification. Therefore, indices 20, 100 and 500, which appeared in several squares in the first version, were adjusted by adding a small increment to make them different. The top row values were increased by 2 and the second row values by 1. This adjustment is so small that its impact on the ERC values is negligible. The only purpose is differentiation.

6.9 The Safety Issue Risk Assessment (SIRA) method

One of the major limitations of the classic *severity x likelihood* formula is that it does not support taking into account the barriers (i.e. the Risk Controls). Typically, the analyst needs to first assess the risk considering current barriers (without any specific way to quantify their effectiveness) and then make another assessment, considering new additional barriers.

SIRA introduces an improved formula for risk assessment. It has four factors:

- Frequency/probability of the Triggering Event
- Effectiveness of the Avoidance Barriers
- Effectiveness of the Recovery Barriers
- Severity of the accident outcome

The model behind SIRA is presented in figure 7. Once the Safety Issue has been defined, the analyst has to create the applicable accident scenario(s). These scenarios can then be risk assessed using SIRA. Typically, the highest risk produced by a scenario becomes the Safety Issue risk value.

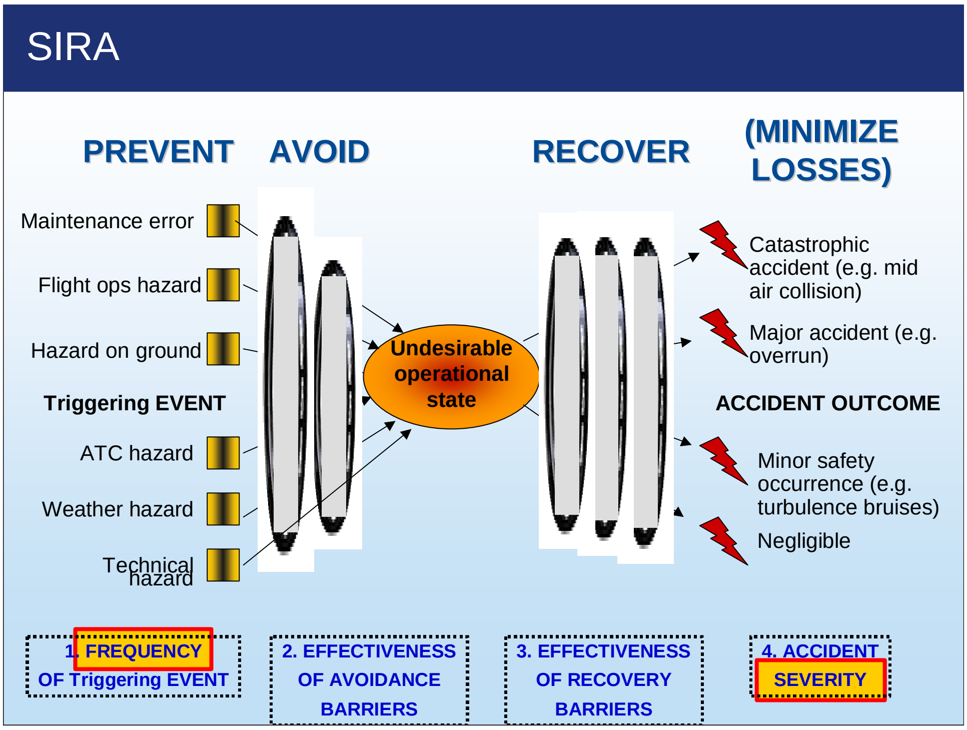

SIRA
PREVENT
AVOID
RECOVER
(MINIMIZE LOSSES)
Maintenance error
Flight ops hazard
Hazard on ground
Triggering EVENT
ATC hazard
Weather hazard
Technical hazard
Undesirable operational state
Catastrophic accident (e.g. mid air collision)
Major accident (e.g. overrun)
ACCIDENT OUTCOME
Minor safety occurrence (e.g. turbulence bruises)
Negligible
1. FREQUENCY OF Triggering EVENT
2. EFFECTIVENESS OF AVOIDANCE BARRIERS
3. EFFECTIVENESS OF RECOVERY BARRIERS
4. ACCIDENT SEVERITY

Figure 7. The model behind the Safety Issue Risk Assessment.

The triggering event may be from various origins (some examples are given in the figure). The first factor is an estimate of the exposure to this event. It may often be expressed in terms of X times / Y flights.

The Undesirable Operational State (UOS) is defined by ARMS as:
"The stage in an accident scenario where the scenario has escalated so far that (excluding providence) the accident can be avoided only through successful *recovery* measure(s). Risk Controls prior to the UOS are part of Avoidance and post-UOS are part of Recovery."

For example, the UOS could be "ending up on a collision course with another aircraft". A recovery measure would then be, for example, a TCAS alert combined with the correct pilot (or aircraft[♣]) reaction.

The second and third factors in the SIRA formula are estimates about the effectiveness of the avoidance and recovery barriers. Finally, the fourth factor is the severity of the accident outcome, in line with the ERC vertical scale.

The values for these four factors can be classes (e.g. A, B, C, D) or numerical values. In effect, the first three factors commonly define the "mean frequency of the accident due to this Safety Issue" while the last factor indicates the severity of the accident. To build a proper methodology, it is necessary to decide which combinations of frequency and severity are tolerable. JAR/FAR-1309 tolerability limits for aircraft design is one source for such limits.

It is important to remember that SIRA is performed on *Safety Issues*, while ERC is used for *events*.

6.10 Example cases of risk assessment

6.10.1 Examples of Event Risk Classification (ERC)

It should be kept in mind that at the moment when the ERC is performed, the person making the classification will often have to rely solely on the information in the report. Sometimes this information is very limited. This is one of the reasons why the ERC should not be considered a final refined risk *assessment*, but rather an initial *classification* of events by the estimated risk. The following examples also reflect the reality of having a low quantity of information available for the ERC.

While studying these examples, the reader might not always think that the given result of the assessment is the most appropriate one. The exact actual result of the assessment is not the main point here – the primary purpose is to illustrate the methodology and the reasoning processes used to make the assessments. It is quite normal that different people might not see some things in the same way. Each person will typically relate to the operation they are used to and this alone can create differences in the results. Moreover, if a more severe "accident outcome" is chosen it is usually accompanied by more barriers being in place to prevent it, with the result ending up at the same "action" colour.

[♣] TCAS with automatic evasive action by the aircraft itself has been studied.

The original report text, which describes the event, is in *italics*. The standard step-by-step advice for carrying out the ERC, which has been extracted from the "ARMS in a Nutshell" fold-out of chapter 9, is presented in bullets and in *italics*.

ERC Example 1

Air Safety Report:
TCAS "Climb" RA in uncontrolled airspace on a low-level transit. TC clearance for low level transit was "Rwy 01, VFR departure, left turn back to XX NDB, then heading 115º for 20 NM, thereafter to YYY, initial altitude 2300 ft." The crew wished to join controlled airspace but were offered this departure by ATC.

After take-off they were given Radar Service and Deconfliction Service. Speed was 180 kt, heading was 105º, about 15 to 20 NM from XX NDB. The crew was constantly receiving traffic advisories and avoidance headings from Radar Service to avoid traffic. The airspace was full with VFR aircraft and TCAS showed constantly 5 and more aircraft at a range of 5 NM. Crew was highly alerted to monitor and identify traffic and requested again to join controlled airspace.

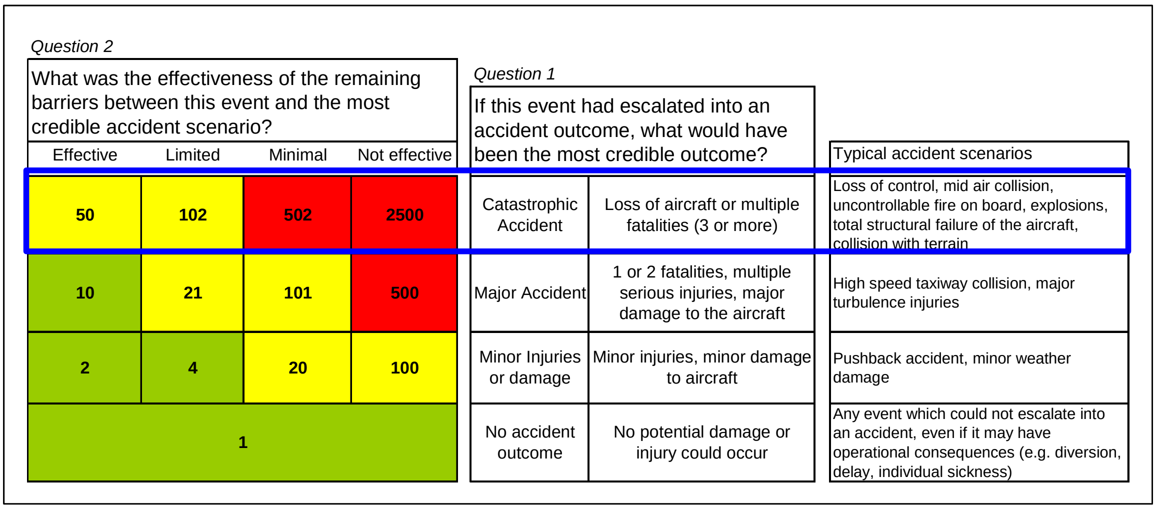
Although avoidance headings had been given, a TCAS Climb RA was triggered with 2000ft/min or more. After clear of conflict the crew descended back to 2300ft and reported back to Radar

Answer Question 1:

- *Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour.*
- *Do not filter out improbable scenarios. Question 2 will take the (low) probability into account.*
- *Among the scenarios with an accident outcome, pick the most credible one, and select the corresponding row in the matrix.*

The resolution manoeuvre was rather aggressive, so it is reasonable to assume a significant loss of separation. Considering also the amount of traffic in the vicinity - of all potential accident scenarios, a mid-air collision scenario is the most credible one. This may seem like a very improbable scenario, but in line with the second bullet above, the "probability" aspect of risk will be taken into account in the Question 2 below. Here, the important thing is to focus on identifying the accident scenario.

This leads us to select the top row in the ERC matrix:



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

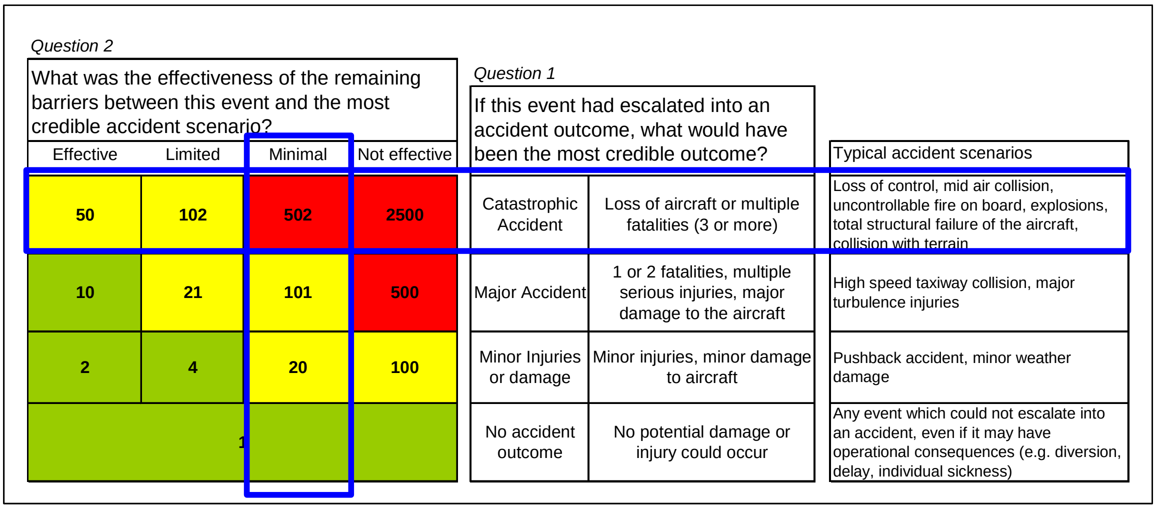
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

Answer Question 2:

- *To assess the remaining safety margin, consider both the number and robustness of the remaining barriers between this event and the accident scenario identified in Question 1.*
- *Barriers, which already failed are ignored*
- *Select the column of choice. See section 4.2 for detailed guidance.*

The chosen accident scenario is a mid-air collision. This second question now has to be answered in relation to that scenario. The barrier that stopped the escalation was the TCAS. Visual detection of the other aircraft would have been another potential barrier and a warning from ATC a third one. What is the combined effectiveness of these remaining barriers?

TCAS is generally effective, but it requires that the system is operative on at least one aircraft. It is not uncommon that VFR traffic operates without a transponder, rendering the TCAS system useless. Similarly, ATC's capability to detect the VFR traffic and warn about it could be severely compromised. Visual detection and avoidance of other (small) aircraft is unreliable. Therefore, the remaining barriers are considered of Minimal effectiveness.



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

This results in the square with a risk index of 502 and colour red:

Typically, this would mean stopping the operation in the zone(s) where the event took place, until there are guarantees there is good reason to believe the risk level has decreased significantly. An (internal) investigation and a refined risk assessment would normally be carried out.

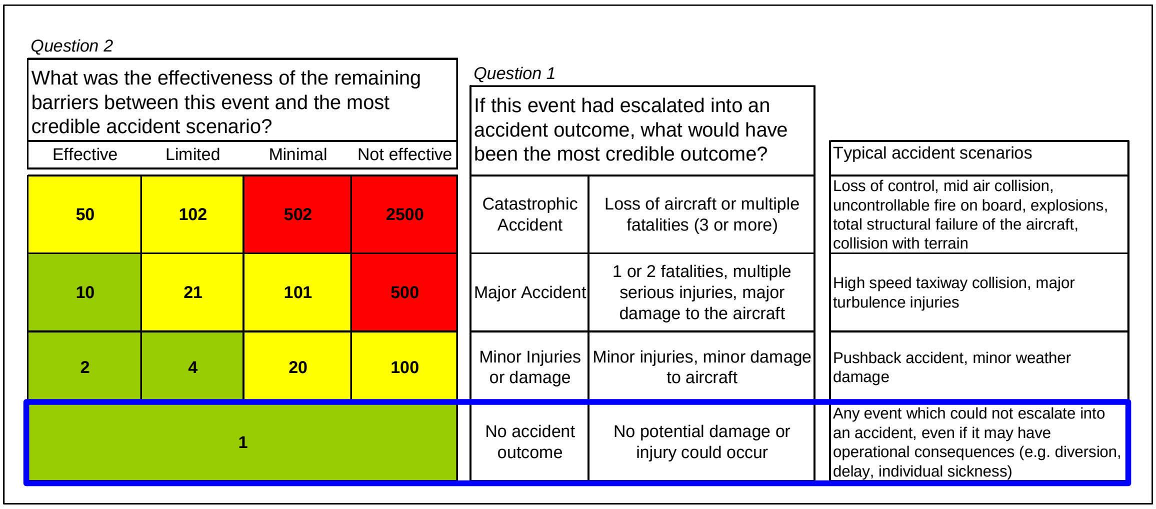
ERC Example 2

Air Safety Report:
Flaps failed to retract after landing in moderate rain. "FCTL flaps locked" message.

Answer Question 1:

- *Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour.*

The event is a simple failure after landing. The resulting situation may be a nuisance, but does not have an impact on the safety of the flight. Therefore, we are in the case "No potential damage or injury could occur". The risk index is 1and also Question 2 no longer applies.



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

ERC Example 3

Air Safety Report:
During cruise, ECAM caution 'Green Sys Hyd Lo Press', followed by low quantity. Pan declared, continued to XXX. Procedures carried out in accordance with ECAM\QRH. Comms with ATC, Company, Fire Services.

Held at YYY to complete procedures + briefing. 15 mile final, FMS gear extension. Full fire/emergency cover. Airport XXX seemed initially reluctant to accept us. However, after explanation of need for long runway they agreed.

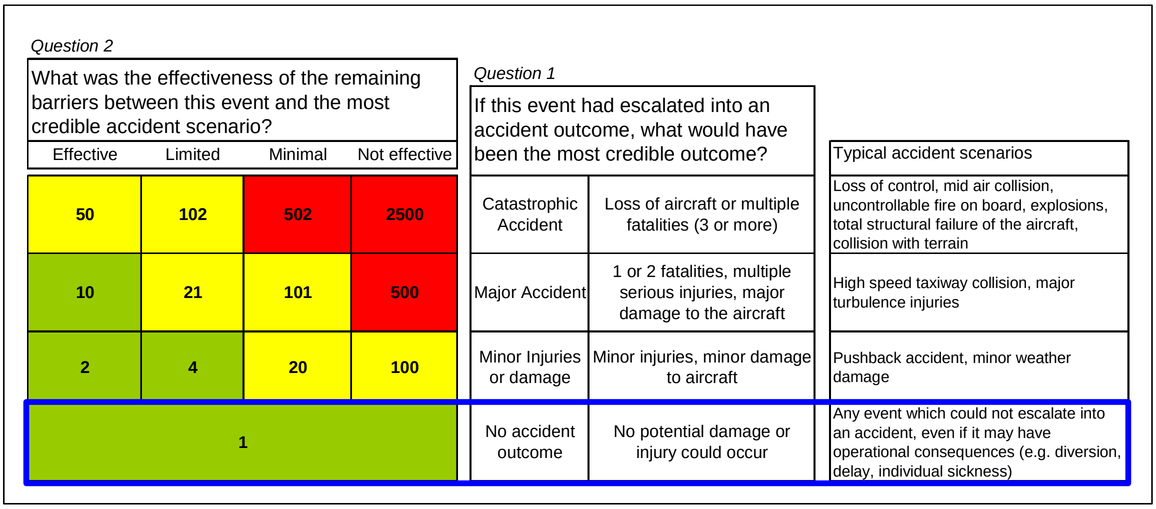
Answer Question 1:

- *Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour.*

The factors that could have made this event escalate are mainly related to the crew's capacity to handle the situation. It would be normal that different airlines would come to different conclusions about whether a scenario with an accident outcome could be associated with this failure. Such differences would be due to the level of confidence in the current pilot training, in their skill and experience, and to some extent due to individual subjectivity of the analyst.

In this event, the failure could be considered to affect the flight in two ways: directly due to degraded aircraft performance (2 out of 4 thrust reversers inop, some spoilers inop) and indirectly due to extra workload and the unusual situation.

Let's imagine that the analyst has good confidence in the flight crews. Considering the context (day time, airport with long runway, etc.), it is reasonable to conclude that the consequences of the failure alter the normal operation very little. Therefore, the analyst selects risk index 1 (bottom row) and also Question 2 no longer applies.



Question 2

Question 1

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				If this event had escalated into an accident outcome, what would have been the most credible outcome?		
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

ERC Example 4

Air Safety Report:

Encounter with a kite during ILS approach.
When passing 1800 ft on the ILS approach for runway 33, the aircraft's path was crossed by a kite, at an estimated distance of 5 to 15 meters. Tower was informed of the event. The aircraft is a Business Jet with no cabin crew. No other aircraft reported having seen the kite.

Answer Question 1:

- *Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour.*

The first judgment is about whether any scenarios leading to an accident outcome can be imagined (including improbable ones). Here the analyst must keep in mind that the Accident Outcome may be an actual accident (as per ICAO) or a “minor accident”, involving only minor injuries or damages.

We can consider that the hazard itself (the kite) could have hit the aircraft, and we can consider possible crew reactions to the situation. Therefore, at least three scenarios could be imagined (even if all three are more or less improbable):

1. Flight Crew makes abrupt manoeuvres trying to avoid the kite and this leads to minor injuries in the cabin.
2. The kite hits the aircraft (e.g. engines) and causes a Loss Of Control (LOC) accident.
3. The kite hits the aircraft and the consequences distract the Flight Crew to the extent that the landing is not fully under control, leading to a very hard or a crash landing, with damages and/or injuries.

The important point here is that these scenarios are not neglected because they seem too improbable:

- *Do not filter out improbable scenarios. Question 2 will take the (low) probability into account.*

The ERC consists of two questions, the first one only deals with the potential consequences and the second one addresses the probability by considering the remaining barriers. These two steps should not be mixed!

- *Among the scenarios with an accident outcome, pick the most credible, and select the corresponding row in the matrix.*

Picking the most credible of the listed scenarios is a subjective judgment. When the different scenarios are differences of magnitude of the same accident type, it is usually relatively easy to pick “the most credible” accident outcome. For example, it is usually not so difficult to decide between a high speed overrun (--> catastrophic) and a low-speed overrun (--> major).

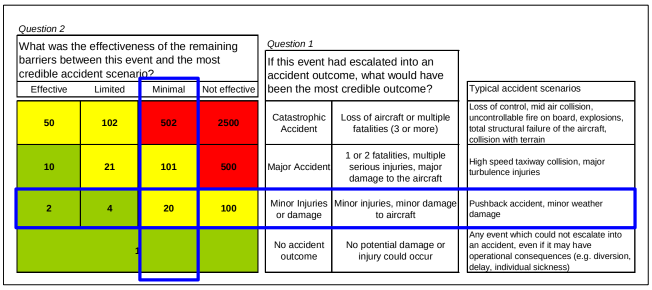
Here, however, there are three quite different scenarios. Let’s imagine that the analyst considers both the first and second scenario credible. Therefore, she will classify both with the ERC. The result will be the highest of the two risk indices.

The first scenario would lead to minor injuries and would therefore correspond to the second row from the bottom in the ERC matrix (“minor injuries or damage”). The most credible accident outcome of the second scenario (LOC) would be a “Catastrophic Accident” (top row in matrix).

Answer Question 2:

- *To assess the remaining safety margin, consider both the number and robustness of the remaining barriers between this event and the accident scenario identified in Question 1.*
- *Barriers, which already failed are ignored*

In the first scenario, the injuries would be caused by the sudden avoidance manoeuvre of the flight crew. Such a manoeuvre is fully plausible in the given context. Are there any barriers in place to protect the occupants if such a manoeuvre is used? Most importantly, the passengers should have their seat belts fastened. There should be no dangerous loose objects in the cabin. However, experience from this operation (without cabin crew) shows that these primary defences fail routinely. Therefore, the safety analyst considers the effectiveness of these barriers "minimal":



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

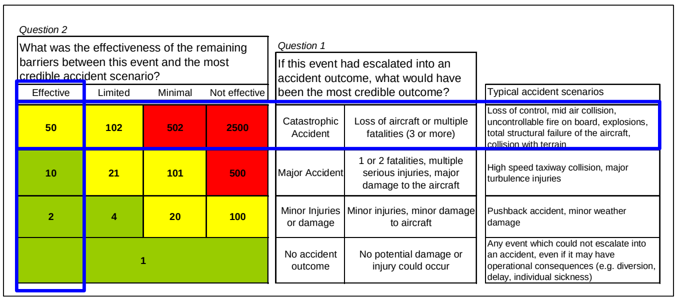
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

Scenario 1.

In the second (LOC) scenario, there is more safety margin:

- Technical barriers: it would be unlikely that the kite could eliminate vital redundant systems, like both engines, to the point that they would be completely lost.
- If the kite caused limited damage to the fuselage or to some aircraft systems, the aircraft should still remain flyable.
- Potential increased workload / reduced availability of flight instruments would be less critical due to the 2-man cockpit.

Based on this reasoning, the safety analyst considers that the barrier effectiveness was "effective":



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

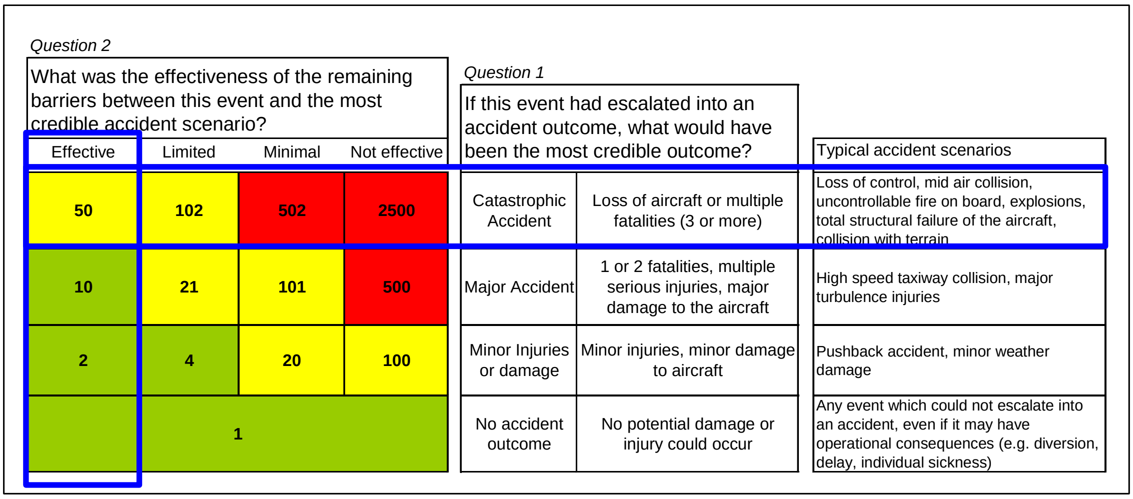
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
	1			No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

Scenario 2.

The results are:

- Scenario 1: YELLOW, risk index 20
- Scenario 2: YELLOW, risk index 50

The higher of the two (50) will be taken as the global result:



Question 2				*Question 1*		
What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				If this event had escalated into an accident outcome, what would have been the most credible outcome?		
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

It can be seen, that the main result (= the colour) for both scenarios is the same. Therefore the urgency and way to action the item would be the same. This is typical, when two scenarios are built from the same event, as the more severe outcomes tend to be “behind” more barriers. It should not be usual to have to entertain more than one accident scenario for each event in ERC though.

ERC Example 5

Air Safety Report:
Airprox reported by pilot of commercial aircraft on approach to AAA airport following visual sighting of microlight aircraft passing within 1 mile of final approach path, no avoiding action necessary. The aircraft was on an ILS approach although good visibility existed. The microlight did not reliably show on the controller’s radar screen.

Answer Question 1:

The reason aircraft are separated is to avoid a collision between them and hence the potential accident outcome in this case is a catastrophic accident. Although it could be argued that a microlight collision may not cause the loss of the commercial aircraft, it is considered that the most likely outcome of a collision would be catastrophic and hence the top line is selected.

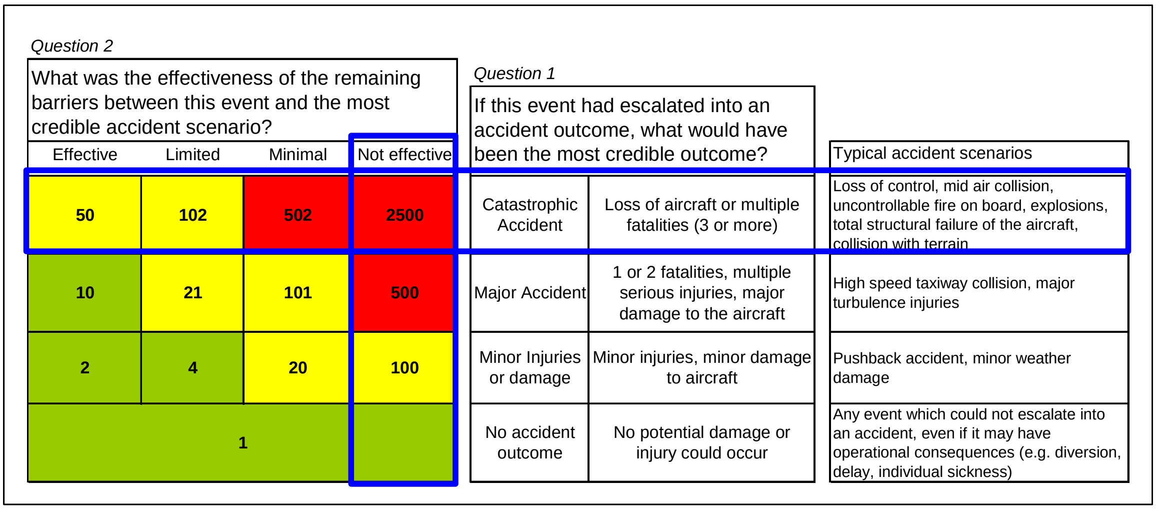
Answer Question 2:

The microlight was not spotted on the radar so ATC barriers were ineffective in this case and need not be considered. The microlight appears not to have been operating a transponder so any ground based or aircraft based collision avoidance barriers were also ineffective.

In this case the aircraft did not collide because the microlight was not actually crossing the track of the commercial aircraft and additionally the commercial pilot visually acquired the microlight due to good visibility and effective look out. Both these barriers acted to avoid the collision but their effectiveness needs to be fully considered.

As the commercial aircraft was flying an ILS approach under ATC control in controlled airspace, combined with the difficulty is spotting a small aircraft such as a microlight, it would not be considered that visual acquisition by the commercial pilot is a reliable barrier to avoid a collision. Furthermore it has to be noted that visual conditions were not a requirement for this approach. As details from the microlight pilot are not available it is difficult to assess the reliability of this trajectory as a barrier to collision. It does however have to be noted that the pilot had already strayed well into controlled airspace so it would not be unreasonable to suggest that the ability of the microlight pilot to avoid a collision may not be high.

Therefore, between the real-life situation and the considered scenario, there were at best ‘minimal’ barriers, but it is most likely that we would consider that there were no effective barriers. This corresponds the rightmost column (“not effective”):



Question 2 What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				*Question 1* If this event had escalated into an accident outcome, what would have been the most credible outcome?		
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

The resulting colour is red and the risk index is 2500. Typically, the red status would suggest that immediate action should be taken to reduce the risk associated with this event – or if imminent improvement is not possible, then the risky part of operation needs to be suspended.

ERC Example 6

Air Safety Report:
The condition of runway/taxiway markings and lights, lack of vertical signage and frequent failures of the ground radar make the ground operation at airport XXX very hazardous.

The report describes Hazards (or latent conditions) at a particular airport and not really an Event where something would have happened. While it is possible to run this through the ERC, it is often more appropriate to use SIRA for such cases. This example is treated as SIRA example 3.

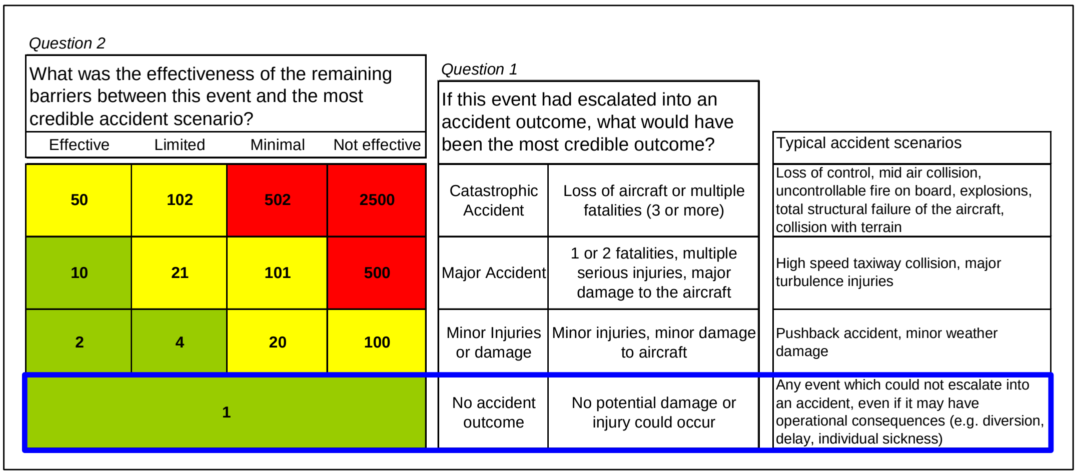
ERC Example 7

Maintenance Safety Report:
Aircraft taxied back to departure gate after maintenance. Mechanic getting out of cockpit after taxi realised the cockpit door was completely missing.

Answer Question 1:

Typically, in these kind of situations, the event tends to get a high risk rating *locally* in the maintenance organisation because administratively the aircraft was not airworthy due to an unfinished maintenance task, and due to the high embarrassment effect of something so visible being missed.

However, from the *Flight Safety* point of view, the missing door does not introduce a risk. First and foremost, that fact that the door is missing *would certainly be noticed* by Flight / Cabin Crew *before the flight*, even if the mechanic had missed it. Secondly, the door does not carry a vital *safety* function (whereas it does have a *security* function). Therefore, the ERC classification would be the following:



Question 2 What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?				*Question 1* If this event had escalated into an accident outcome, what would have been the most credible outcome?		
Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

This example highlights the importance of relating to the actual Flight Safety risk, and not to the local Maintenance Organisation impact. However, the latter may be an important additional local consideration from the quality perspective, and get a high importance rating therein.

6.10.2 Examples of Safety Issue Risk Assessment (SIRA)

The examples presented here have been Risk Assessed using the SIRA Excel tool. The Excel files contain the full assessment, while the text below gives more explanations on the why's and how's of the assessment.

SIRA Example 1:

Electrical power anomalies on a large transport aircraft flight from AAA to BBB required the crew to select the battery bus, which can provide power for a limited period of up to 90 minutes. The crew elected to continue to BBB. One hour and 40 minutes later the battery power was depleted and they lost their remaining cockpit systems. They then decided to divert to CCC and came to a rest off the runway due to no thrust reversers and poor braking. There were no injuries to crew or passengers. Investigation revealed that the failure of a relay ("XYZ") caused a "standby bus off" light to illuminate and that the main battery charger was not receiving power.

Step 1: Define the Safety Issue precisely

The Safety Issue is the total loss of electrical power due to the failure of the relay XYZ on aircraft type C, time period of study being the next 12 months.

Step 2: Develop the related accident scenarios.

The accident scenario is total loss of the aircraft due to the loss of cockpit systems, reduced/no braking capability etc.

Step 3: Analyse the Scenario using the SIRA model:

The triggering event is the failure of the relay. The probability of this happening can be calculated using technical reports and is relatively low. The Undesirable Operational State (UOS) in this case is flying with no or "battery only" aircraft power. The barriers to prevent this occurring are the multiple redundant aircraft electrical power systems, which together form the "avoidance barriers". Their combined reliability will give the value for the second factors of SIRA.

Once the UOS exists then the recoverability will be isolation of failed systems to recover electrical power and perhaps starting the APU to create another source of generated electrical power. If these efforts do not succeed the next step is to land at the nearest airport whilst battery power is still available. These give the value to the third factor in SIRA. In this particular case the crew continued to fly until the battery power was exhausted.

Step 4: Determine/estimate the values for the four factors of SIRA.

For example:

- The triggering event is the failure of the relay and from technical reports this is calculated to be relatively low - 10^{-4} (about every 10,000 flight sectors)
- The Undesirable Operational State is flying with no or "battery only" aircraft power and the barriers to prevent this occurring are the multiple redundant aircraft electrical power systems. These are estimated to fail approximately once per 100 times - 10^{-2}
- Recoverability from the UOS will be isolation of failed systems to recover electrical power and perhaps starting the APU, or failing that landing at the nearest airport whilst battery power is still available. This is estimated to be unreliable about once per 10 times - 10^{-1}
- The accident outcome is deemed to be "Catastrophic".

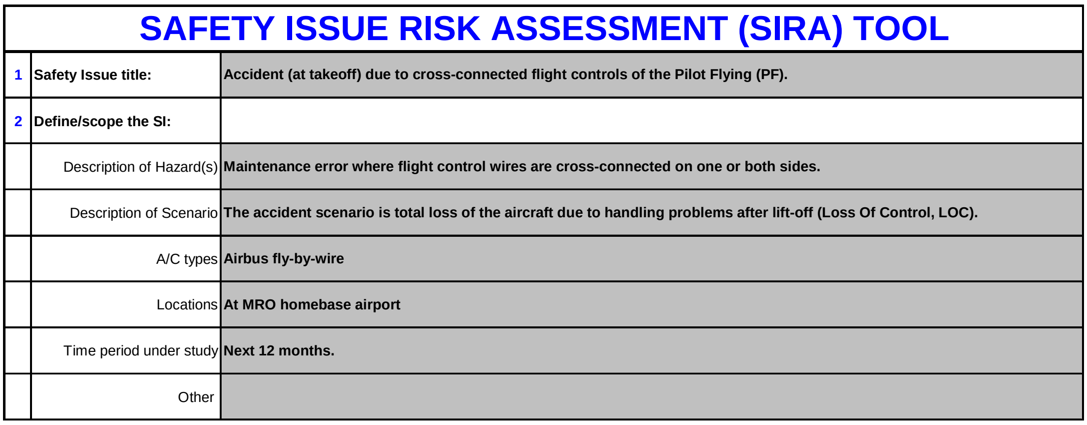
With these figures the result is "Secure". This might mean a reassessment of the procedures in the QRH, reassessment of crew training and emphasising the requirement for an immediate diversion if flying on standby power.

SIRA Example 2:

An incident happening to another company motivates the MRO "MyMx"to study the Safety Issue of cross-connecting the flight controls (left-right or push-pull). MyMx has no idea how improbabe it is that such a maintenance error could take place.

Step 1: Define the Safety Issue precisely

The Safety Issue is an accident (at takeoff) due to cross-connected flight controls of the Pilot Flying (PF). MyMx currently is maintaining only Airbus fly-by-wire aircraft, so these will be the a/c types under study.



SAFETY ISSUE RISK ASSESSMENT (SIRA) TOOL

1	**Safety Issue title:**	**Accident (at takeoff) due to cross-connected flight controls of the Pilot Flying (PF).**
2	**Define/scope the SI:**	
	Description of Hazard(s)	**Maintenance error where flight control wires are cross-connected on one or both sides.**
	Description of Scenario	**The accident scenario is total loss of the aircraft due to handling problems after lift-off (Loss Of Control, LOC).**
	A/C types	**Airbus fly-by-wire**
	Locations	**At MRO homebase airport**
	Time period under study	**Next 12 months.**
	Other	

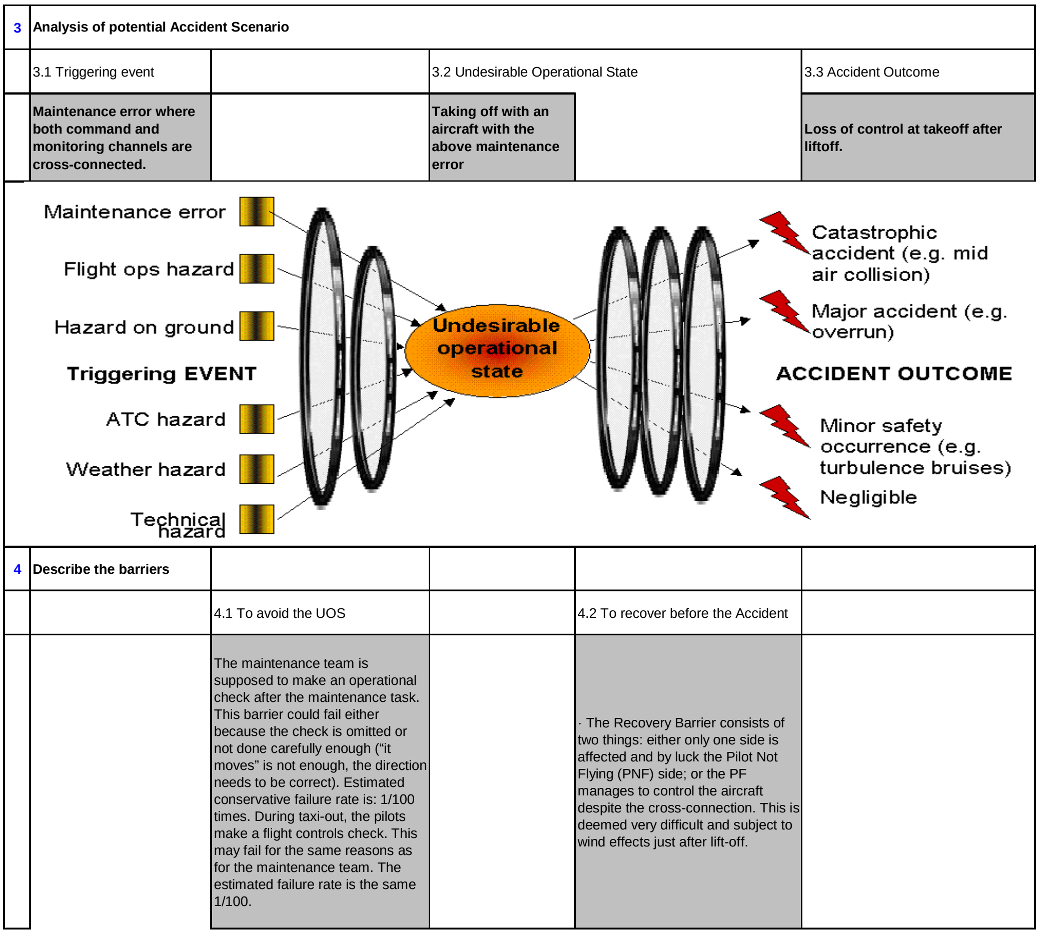
Extract from the SIRA excel tool (defining the Safety Issue).

Step 2: Develop the related accident scenarios.

The accident scenario is total loss of the aircraft due to handling problems after lift-off (Loss Of Control, LOC).

Step 3: Analyse the Scenario using the SIRA model:

- The triggering Event is the maintenance error of cross-connecting the wires on one or both sides (capt/first officer). This must involve cross connecting both the command and monitoring channels, otherwise the aircraft itself would detect the problem.
- The Undesirable Operational State can be defined as "taking off with an aircraft with the above maintenance error". (note that the UOS always takes place within the Flight Operation)
- The accident is LOC at takeoff.
- With the above definitions, the Avoidance barriers are: any actions post-maintenance that would enable either the MyMx or the operating flight crew to detect the problem before (or latest during) the takeoff roll.
- The recovery barriers are flight crew actions enabling a safe flight despite the aircraft taking off with cross connected controls.



3	**Analysis of potential Accident Scenario**				
	3.1 Triggering event		3.2 Undesirable Operational State		3.3 Accident Outcome
	Maintenance error where both command and monitoring channels are cross-connected.		**Taking off with an aircraft with the above maintenance error**		**Loss of control at takeoff after liftoff.**

Maintenance error
Flight ops hazard
Hazard on ground
Triggering EVENT
ATC hazard
Weather hazard
Technical hazard
Undesirable operational state
Catastrophic accident (e.g. mid air collision)
Major accident (e.g. overrun)
ACCIDENT OUTCOME
Minor safety occurrence (e.g. turbulence bruises)
Negligible

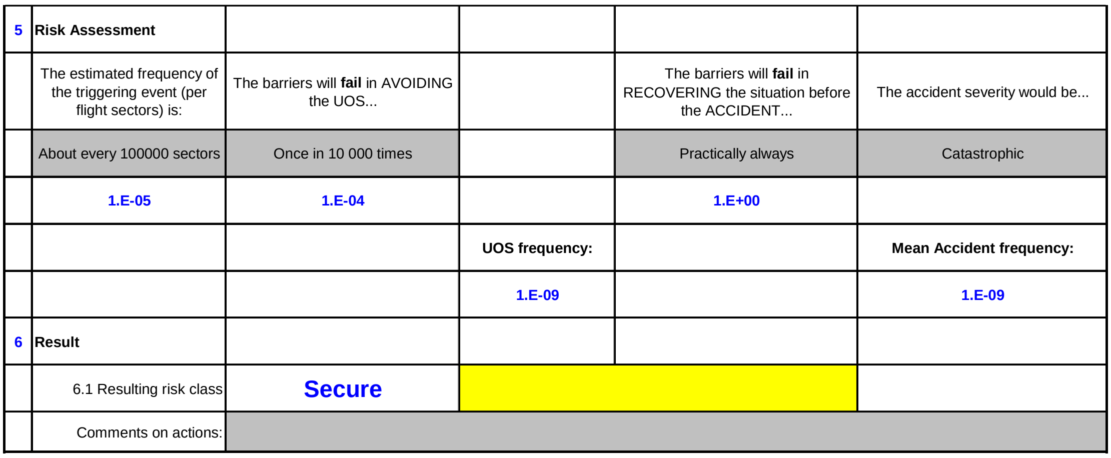
4	**Describe the barriers**				
		4.1 To avoid the UOS		4.2 To recover before the Accident	
		The maintenance team is supposed to make an operational check after the maintenance task. This barrier could fail either because the check is omitted or not done carefully enough ("it moves" is not enough, the direction needs to be correct). Estimated conservative failure rate is: 1/100 times. During taxi-out, the pilots make a flight controls check. This may fail for the same reasons as for the maintenance team. The estimated failure rate is the same 1/100.		· The Recovery Barrier consists of two things: either only one side is affected and by luck the Pilot Not Flying (PNF) side; or the PF manages to control the aircraft despite the cross-connection. This is deemed very difficult and subject to wind effects just after lift-off.	

Extract from the SIRA excel tool (analysing the scenario).

Step 4: Determine/estimate the values for the four factors of SIRA.

- Triggering event: There is no information on how frequent or rare such a maintenance error could be. It has never taken place in MyMx in its 8 years of existence. Therefore, this SIRA risk assessment is carried out “backwards”, leaving this value initially open.
- Avoidance barriers: the maintenance team is supposed to make an operational check after the maintenance task. This barrier could fail either because the check is omitted or not done carefully enough (“it moves” is not enough, the direction needs to be correct). Estimated conservative failure rate is: 1/100 times. During taxi-out, the pilots make a flight controls check. This may fail for the same reasons as for the maintenance team. The estimated failure rate is the same 1/100. For both to fail, we get an Avoidance Barriers failure rate of: 1/10,000 times.
- The Recovery Barrier consists of two things: either only one side is affected and by luck the Pilot Not Flying (PNF) side; or the PF manages to control the aircraft despite the cross-connection. This is deemed very difficult and subject to wind effects just after lift-off. Therefore, it is considered that a conservative “fails practically always” barrier effectiveness level must be used.
- A Loss of Control at takeoff is considered a Catastrophic accident.

As the Triggering Event frequency is unknown, we work backwards by targeting a resulting risk class, which is “secure” or better. By fixing the barrier values and the accident type and varying the Triggering Event frequency, it can be seen that the maximum allowable frequency is: “every 100,000 sectors”.



5	**Risk Assessment**				
	The estimated frequency of the triggering event (per flight sectors) is:	The barriers will **fail** in AVOIDING the UOS...		The barriers will **fail** in RECOVERING the situation before the ACCIDENT...	The accident severity would be...
	About every 100000 sectors	Once in 10 000 times		Practically always	Catastrophic
	1.E-05	**1.E-04**		**1.E+00**	
			UOS frequency:		**Mean Accident frequency:**
			1.E-09		**1.E-09**
6	**Result**				
	6.1 Resulting risk class	**Secure**			
	Comments on actions:				

Extract from the SIRA excel tool (calculating the result).

In this case, the frequency has to be interpreted “every 100,000 times that the sidestick wiring is re-installed”. This gives the MRO an idea of how effective their work procedures must be so that they can be confident this error frequency is never reached. It should be noted that the MRO will also work on making their part of the Avoidance Barriers more robust, allowing the second factor to improve.

This example illustrates how the non-flying aviation organisations can and should refer their risk assessments to the accident taking place in the flight operation. This is easier if there is a good cooperation between the MRO and the safety teams within their client operators, allowing a mutual sharing and learning process.

SIRA Example 3 (from ERC example 6):

Air Safety Report: The condition of runway/taxiway markings and lights, lack of vertical signage and frequent failures of the ground radar make the ground operation at airport XXX very hazardous.

The report describes Hazards (or latent conditions) at a particular airport and not really an Event where something would have happened. While it is possible to run this through the ERC, it is often more appropriate to use SIRA for such cases.

Step 1: Define the Safety Issue precisely

The Safety Issue is the poor visual guidance during taxiing at airport XXX, combined with frequent failures of the ground radar. The time period is the next 12 months and the aircraft type considered is the only one type Y that this operator flies to this destination.

Step 2: Develop the related accident scenarios.

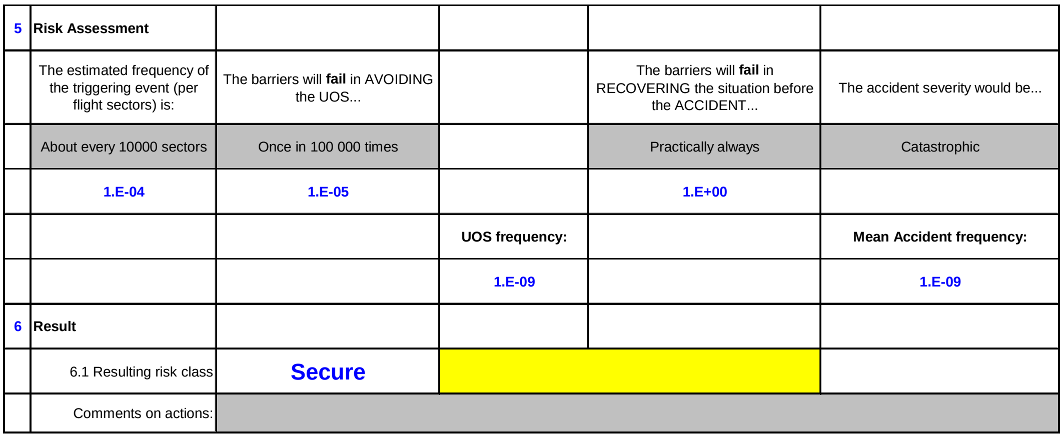
The accident scenario under consideration is a ground collision (with another aircraft or vehicle due to one getting to the wrong place). This is a viable scenario during Low Visibility conditions.

Step 3: Analyse the Scenario using the SIRA model:

- Triggering event: The frequency of flights to/from this destination. (see note below).
- As is common, the UOS could be chosen in various different ways. It could be defined as "getting lost at XXX during low visibility conditions due to above hazards" or as "*Getting on a (ground) collision course at XXX during low visibility conditions due to above hazards*". Experience shows that it is better to pick an UOS which is already very close to the accident, as this will make sure the "recovery barriers" are really recovery barriers. In this case, the latter UOS choice (in *italics*) is selected.
- The Accident would be a ground collision, which can be considered catastrophic, as typically more than 3 lives could be lost.
- The Avoidance Barriers includes everything the pilots have to help them navigate on the ground correctly at XXX: terminal charts, moving maps provided by the aircraft, etc. Let's assume that in the aircraft type Y, the only available support is the classic terminal area map.
- The Recovery Barriers include everything that could resolve the collision course situation without a collision. The main barriers would be the flight crew itself and the controllers (ground, tower) who could potentially detect the conflict and take/request avoidance action. The time window for this after the UOS is limited typically to less than a minute.

Step 4: Determine/estimate the values for the four factors of SIRA.

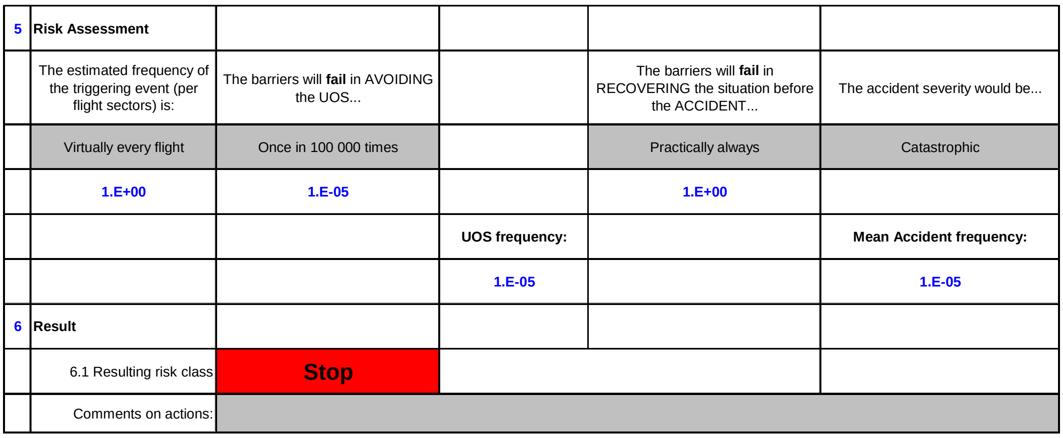
- Triggering Event frequency: Let us initially use the Triggering Event value corresponding to the frequency of flights to this destination. That would be 1 in 10000 sectors. See note below for later elaboration.
- Avoidance: Getting on a collision course requires Low Visibility conditions, getting lost (due to bad markings) and the presence of another a/c or vehicle in the area where the plane gets lost. Statistically, low visibility conditions are present at this airport 4% of the time. Getting lost in such conditions is estimated to happen 1/1000 times. The presence of other a/c or vehicles is constant. This gives a rate of 4/100,000 times.
- Recovery: Successful recovery within the short time window is very unsure. We will use the “fails practically always” level.
- The collision accident would be catastrophic.



5	**Risk Assessment**				
	The estimated frequency of the triggering event (per flight sectors) is:	The barriers will **fail** in AVOIDING the UOS...		The barriers will **fail** in RECOVERING the situation before the ACCIDENT...	The accident severity would be...
	About every 10000 sectors	Once in 100 000 times		Practically always	Catastrophic
	1.E-04	**1.E-05**		**1.E+00**	
			UOS frequency:		**Mean Accident frequency:**
			1.E-09		**1.E-09**
6	**Result**				
	6.1 Resulting risk class	**Secure**	🟨		
	Comments on actions:				

Extract from the SIRA excel tool (calculating the resulting risk level).

The result “secure” would indicate that the risk level as such is acceptable. However, this was assessed in the context of the whole operation of the airline, influenced by the fact that flights to this destination are very rare (1/10,000 sectors). If the assessment was done exclusively for the flight to/from XXX, the result would be the following:



5	**Risk Assessment**				
	The estimated frequency of the triggering event (per flight sectors) is:	The barriers will **fail** in AVOIDING the UOS...		The barriers will **fail** in RECOVERING the situation before the ACCIDENT...	The accident severity would be...
	Virtually every flight	Once in 100 000 times		Practically always	Catastrophic
	1.E+00	**1.E-05**		**1.E+00**	
			UOS frequency:		**Mean Accident frequency:**
			1.E-05		**1.E-05**
6	**Result**				
	6.1 Resulting risk class	**Stop**			
	Comments on actions:				

Extract from the SIRA excel tool (XXX operation only).

This shows that the risk is acceptable thanks to the low frequency of flights to XXX, but that *on every single flight to/from XXX, the risk level is unacceptably high*. Ironically, the more the airline flies to other destinations, the more acceptable this risk becomes, even if the actual risk of “ground collision in XXX” is not affected by the flights to other destinations! (and even if the total operational risk increases with increasing traffic).

Therefore, it is reasonable to say that this Safety Issue should be assessed exclusively for the flights to/from XXX. It does not make sense that an airline keeps in its route network a destination that induces an unacceptably high operational risk.

NOTE: It is important to realise when the risk assessment should be limited to only the part of the operation concerned, i.e. to assess the “local” risk instead of the “global” risk. Otherwise, unacceptably-high-risk elements within the operation may be maintained with the excuse that exposure to those elements within the global operation is very limited.

6.10.3 Examples of Safety Assessments (Management of Change)

Safety Assessment Example 1:

Procedures for the connection of ground power after arrival on stand.

The current practice is to start the APU after landing and subsequently shutdown both engines before the Ground Power Unit (GPU) is connected. This is perceived as a normal, conventional, safe operation. The proposed change is to keep number 2 engine running until the GPU is connected. This would reduce APU cycles and save fuel.

The Safety Issue is the risk of ingesting personnel who approach the aircraft into the operating engine.

Triggering event: arrival of aircraft with this procedure in effect. (→ every flight)

UOS: an operating engine with ground personnel within the danger zone of ingestion.

Accident outcome: Person ingested into engine (fatal). → Major.

Avoidance barriers: Procedures to keep all personnel away from aircraft until the GPU has been plugged and the engines have been shutdown. The revised procedure would have both personnel and equipment approaching the aircraft to plug in the GPU. (→ estimated to fail 1/1000 times)

Recovery barriers. Barriers that would keep people who went to the aircraft despite the running engine, away from the engine danger zone. Depends on location of engines, ingestion size of danger zone, etc. If somebody accidentally goes to the aircraft, he might realise that the engine is running, or simply not need to go close to the engine, but there is no actual protection in place (→ estimated to fail 1/1000 times).

SIRA result (using the excel tool): “IMPROVE” (risk too high). → This means the proposed change is beyond the acceptable level of risk and cannot be implemented unless new avoidance or recovery barriers can be created.

6.10.4 Examples covering the whole Risk Assessment process

The complete ARMS risk assessment and management process is explained in schematic form in the "ARMS in a Nutshell" Quick Reference Guide (Section 9). The following examples should be considered in conjunction with that pullout sheet.

Example 1:

Consider the ERC example one (TCAS). The red result means several things:

- Typically, immediate risk reduction must be possible or flying to such areas must be suspended.
- Even one single event with a red ERC rating becomes a "Safety Issue" of its own. It has to be judged whether the SI will cover only the particular zone where the event took place or also other/all similar areas.

As single event, the event contributes to ERC statistics. As a Safety Issue, it will now be assessed using the SIRA. The SIRA assessment must then be repeated from time to time to make sure the risk level becomes/remains acceptable.

Example 2:

Consider the ERC example 4 (kite). The yellow result typically leads to further investigation and/or more detailed risk assessment. Again, as a single event, the event is in the database with all other events and contributes to all statistics and trend analyses. But in addition to that, an investigation is now launched to understand more in detail what happened and why.

The investigation findings may typically lead to risk reduction actions. If the case cannot be considered a one-off, then a Safety Issue would be opened to cover the issues. It could be scoped "kite encounters when flying to airport X" or "kite encounters" or "kite encounters in country Y", etc. The Safety Issue would then have its own risk assessment, and resulting risk value, using SIRA. It could well be that the SIRA shows the full catastrophe potential of the Safety Issue, which so far materialised only in the form of events with minor or no consequence. In other words, the fact that the few related events ended well, is no guarantee that the observed issue is not "very high risk".

7 Glossary

Accident
An unintended event that causes death, injury, environmental or material damage.

Accident (ICAO, Annex 13):
An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which:
a) a person is fatally or seriously injured as a result of
- being in the aircraft, or
- direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or
- direct exposure to jet blast,

except when the injuries are from natural causes, self inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew: or
b) the aircraft sustains damage or structural failure which:
- adversely affects the structural strength, performance or flight characteristics of the aircraft, and
- would normally require major repair or replacement of the affected component,

except for engine failure or damage. when the damage is limited to the engine, its cowlings or accessories: or for damage limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin: or
c) the aircraft is missing or is completely inaccessible.

Accident Outcome
An outcome that involves actual physical harm or damage. It includes outcomes that do not meet the ICAO annex 13 definition of an ‘accident’, but still involve actual physical harm or damage.

Accident Scenario
The imagined progression from the actual outcome (of ERC) or the triggering event/hazard release (in SIRA) to the accident outcome.

One Safety Issue (or sub-issue) may relate to several accident scenarios. For example, the Safety Issue “demanding approach to airport X” may contain two scenarios, one leading to CFIT and another to a very hard (crash) landing. Usually a Safety Issue cannot be directly risk assessed, but the related Accident Scenarios can.

Event Risk Classification (ERC)
The initial risk classification of operational safety events, using the ERC matrix.

Hazard:
Condition, object or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function. (ICAO)

Management of Change
The assessment of risk as a result of a predicted/planned change to the operation together with the consequential actions taken, ensuring the safety of the operation due to the change.

Operational Risk Assessment (ORA)
Assessment of operational risks in a systematic, robust and intellectually cohesive manner.

Register
Documented record of all information concerning Safety Issues, assessed risk levels, the agreed actions to reduce risk levels and information on their progress.

Risk:
A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome (Doug Hubbard)

Probability of an accident x losses per accident (classic engineering definition)

The predicted probability and severity, of the consequence(s) of hazard(s) taking as reference the potential outcomes. (adapted from ICAO by ARMS)

Risk Controls:
Measures to avoid or to limit the bad outcome; through prevention, recovery, mitigation. (SHELL)

Measures to address the potential hazard or to reduce the risk probability or severity. (ICAO)

<u>Preferred use by ARMS:</u>

Synonyms:

- Risk Control
- Barrier
- Protection
- Defense

Used by ARMS:

- Risk Control
- Barrier

Not used by ARMS:

- Safety Barrier (misleading)
- Protection, defense (for harmonisation reasons)

Not used by ARMS due to multiple meanings:

<u>Threat</u>
Another meaning in the TEM context
In most instances the word “scenario” can be used instead

Mitigation
Classic = post-accident risk controls
ICAO = all risk controls (prevention, recovery, mitigation)
Used by ARMS: *controlling* risks or *reducing* risks (verbs)
Used by ARMS: Risk Controls, Barriers (nouns)

Risk Value (Risk Index Value)
A numerical weighting given to each square of a risk matrix to enable differentiation of risk for the purpose of quantitative analysis.

Safety Analyst
A person with the experience, training, responsibility and authority to perform risk assessments and to analyse the safety database for Safety Issues.

Safety Assessment
A risk assessment focusing on a predicted or planned change to a specific part of the operation.

Safety Case
A Safety Assessment on an existing part of the operation in order to demonstrate that the safety risk is at an acceptable level.

(Safety) Event:
Any happening that had or could have had a safety impact, irrespective of real or perceived severity (ARMS)

Safety Issue:
A manifestation of a hazard or combination of several hazards in a specific context. The Safety Issue has been identified through the systematic Hazard Identification process of the organisation. A SI could be a local implication of one hazard (e.g. de-icing problems in one particular aircraft type) or a combination of hazards in one part of the operation (e.g. operation to a demanding airport). (ARMS)

Safety Issue Risk Assessment (SIRA)
The risk assessment of Safety Issues, which includes the risk controls (barriers) in the assessment. The conceptual framework for this risk assessment is one where risk is calculated as the product of *four* factors, (prevention, avoidance, recovery and minimisation of losses) instead of using the old severity x likelihood formula.

Safety Management System (SMS)
A Safety Management System is a systematic, explicit and proactive process for managing safety that integrates operations and technical systems with financial and human resource management to achieve safe operations with as low as reasonably practicable risk. (ICAO)

Safety Performance Indicators
Specified metrics used to measure the safety performance of an operation or organisation.

Safety Performance Monitoring
The process by which the safety performance of the organisation is verified by comparison with the safety policy and approved safety objectives. (ICAO)

Triggering Event:
In Safety Issue Risk Assessment (SIRA) the first of the four factors - the event or condition, which triggers the accident scenario by introducing the initial risk factor. Whether the sequence will then escalate into an UOS or Accident will depend on the avoidance and recovery barriers. (ARMS)

Undesirable Operational State (UOS):
The stage in an Accident Scenario where the scenario has escalated so far that (excluding providence) the accident can be avoided only through successful *recovery* measure(s). Risk Controls prior to the UOS are part of Avoidance and post-UOS are part of Recovery. (ARMS)

8 Acknowledgements

The ARMS working group wishes to thank the organisations who supported this effort by letting their people participate in the development work and by hosting workshops.

ARMS thanks ECAST and the ECAST SMS Working Group for having included the methodology in the ECAST deliverables.

ARMS thanks the safety software companies for their interest in this new methodology and for embodying it in their software products – thereby significantly speeding up the shift from older methods to the ARMS methodology.

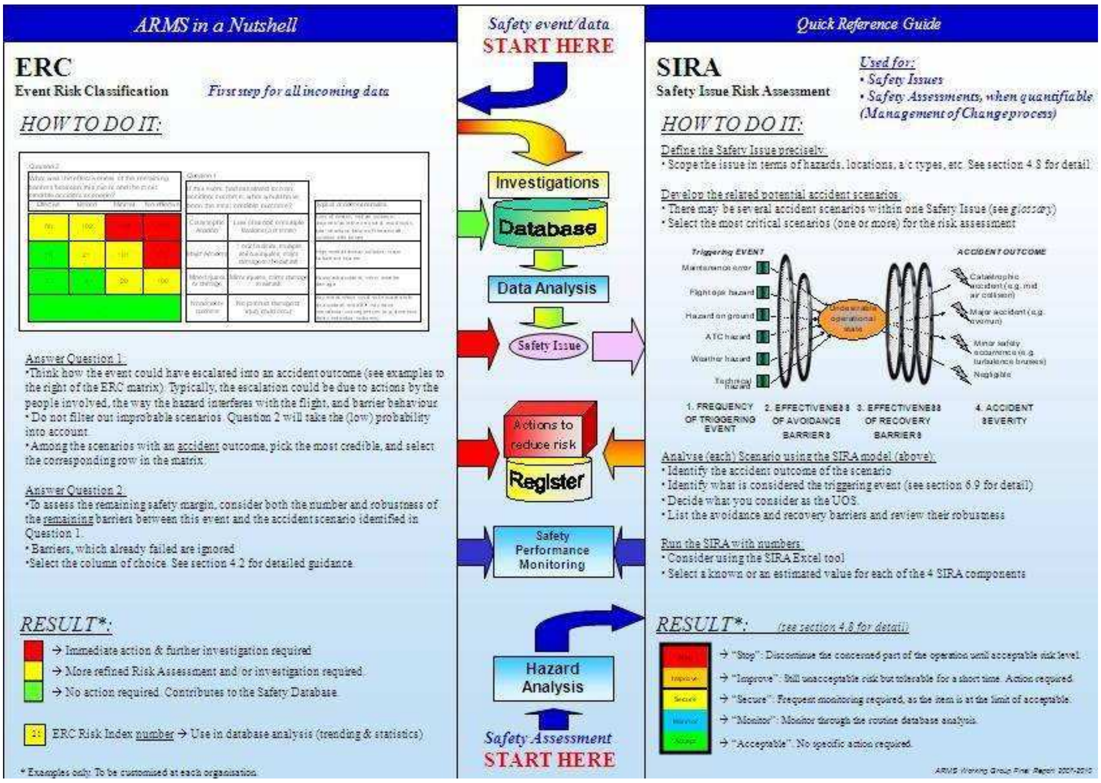
ARMS thanks City University London for having hosted one meeting.

9 ARMS Quick Reference Guide

The ARMS *Quick Reference Guide* (QRG) is a summary of the ARMS process flow and the two key procedures: Event Risk Classification and Safety Issue Risk Assessment. The purpose of this Guide is to be the daily quick reference for the Safety Analyst. The Quick Reference Guide is presented on one single A3 sheet and is thus suitable for printing and hanging on the wall for continuous reference. The printable version is available on Skybrary.

The QRG is not a substitute for the complete ARMS document but rather a summary for someone who has already read the document.

The middle section of the QRG illustrates the Risk Management process as a flow chart. A colour coding is used: for example, events which are classified green in the ERC, will flow directly to the Database (green arrow). Events which are classified red or yellow, may have to be investigated (red/yellow arrow). All ERC and SIRA results contribute to Safety Performance Monitoring (blue arrows).



ARMS in a Nutshell

ERC
Event Risk Classification

First step for all incoming data

HOW TO DO IT:

Answer Question 1:
- Think how the event could have escalated into an accident outcome (see examples to the right of the ERC matrix). Typically, the escalation could be due to actions by the people involved, the way the hazard interferes with the flight, and barrier behaviour
- Do not filter out improbable scenarios. Question 2 will take the (low) probability into account
- Among the scenarios with an accident outcome, pick the most credible, and select the corresponding row in the matrix.

Answer Question 2:
- To assess the remaining safety margin, consider both the number and robustness of the remaining barriers between this event and the accident scenario identified in Question 1.
- Barriers, which already failed are ignored
- Select the column of choice. See section 4.2 for detailed guidance.

RESULT:*

🟥 → Immediate action & further investigation required
🟨 → More refined Risk Assessment and/or investigation required.
🟩 → No action required. Contributes to the Safety Database.

21 ERC Risk Index number → Use in database analysis (trending & statistics)

* Examples only. To be customised at each organisation.

Quick Reference Guide

SIRA
Safety Issue Risk Assessment

Used for:
- *Safety Issues*
- *Safety Assessments, when quantifiable (Management of Changeprocess)*

HOW TO DO IT:

Define the Safety Issue precisely:
- Scope the issue in terms of hazards, locations, a/c types, etc. See section 4.8 for detail

Develop the related potential accident scenarios:
- There may be several accident scenarios within one Safety Issue (see *glossary*)
- Select the most critical scenarios (one or more) for the risk assessment

Analyse (each) Scenario using the SIRA model (above):
- Identify the accident outcome of the scenario
- Identify what is considered the triggering event (see section 6.9 for detail)
- Decide what you consider as the UOS.
- List the avoidance and recovery barriers and review their robustness

Run the SIRA with numbers:
- Consider using the SIRA Excel tool
- Select a known or an estimated value for each of the 4 SIRA components

RESULT:* *(see section 4.8 for detail)*

→ "Stop": Discontinue the concerned part of the operation until acceptable risk level.
→ "Improve": Still unacceptable risk but tolerable for a short time. Action required.
→ "Secure": Frequent monitoring required, as the item is at the limit of acceptable.
→ "Monitor": Monitor through the routine database analysis.
→ "Acceptable": No specific action required.

ARMS Working Group Final Report 2007-2010