

## **Appel d'offres DGAC N° 96/01**

**Lot N° 7:**

# **Development of a Methodology for Operational Incident Reporting and Analysis Systems**

## ***FINAL REPORT***

**Authors:**

**J. Paries & A. Merritt, Dédale  
M. Schmidlin, Airbus Industrie**

**Supervisors:**

**J. Paries, Dédale  
J. J. Speyer, Airbus Industrie**

<b>1. INTRODUCTION .....</b>	<b>3</b>
<b>2. THE LIMITATIONS OF CURRENT OIRAS.....</b>	<b>5</b>
2.1 THE REPORTER.....	5
2.2 THE REPORT FORM.....	6
2.3 DATA BASES.....	6
2.4 DATA ANALYSIS.....	7
2.4.1 <i>Trend Analysis</i> .....	7
2.5 ARE WE LEARNING ANYTHING?.....	8
<b>3. AN IMPROVED OIRAS: FUNCTIONAL AND THEORETICAL CONSIDERATIONS.....</b>	<b>10</b>
3.1 FUNCTIONS OF AN OIRAS.....	10
3.1.1 <i>Extracting ‘safety lessons’</i> .....	10
3.1.2 <i>Additional functions</i> .....	10
3.2 THEORETICAL BASES OF OIRAS.....	11
3.2.1 <i>The definition of an incident</i> .....	11
3.2.2 <i>Difficulties in the concept of incident</i> .....	11
3.2.3 <i>Safety through specification</i> .....	12
3.2.4 <i>Safety through adaptation</i> .....	13
3.3 ANALYTIC APPROACHES.....	15
3.4 RISK MANAGEMENT MONITORING THROUGHOUT THE ‘SYSTEM’.....	16
<b>4. AN IMPROVED OIRAS: FUNCTIONAL SPECIFICATIONS.....</b>	<b>18</b>
4.1 BASIC FEATURES OF THE PROPOSED SYSTEM.....	18
4.2 THE FUNCTIONAL OUTPUTS OF THE SYSTEM.....	19
4.3 OIRAS FORMAT.....	20
4.3.1 <i>Objectives</i> .....	20
4.3.2 <i>Overall structure</i> .....	20
4.3.3 <i>The Risk Management Page</i> .....	22
4.3.4 <i>Feeding the Risk Management Page</i> .....	24
4.3.5 <i>Risk Management Strategies</i> .....	25
4.3.6 <i>Failure Modes</i> .....	25
4.3.7 <i>Recovery Modes</i> .....	26
4.3.8 <i>Using the organisational level menu : organising the multi-layer communication</i> .....	26
4.3.9 <i>Corrective Actions</i> .....	27
4.4 FEEDING THE INDIVIDUAL EVENT DATA BASE.....	28
4.5 THE REPORT FORM AND THE REPORTERS.....	29
4.5.1 <i>The Event Report Form</i> .....	29
4.5.2 <i>Reporters - Pilots only?</i> .....	29
<b>5. AN IMPROVED SAFETY OFFICE.....</b>	<b>30</b>
5.1 GOALS AND OBJECTIVES.....	30
5.2 DATA FLOW.....	30
5.3 TRACKING ORGANISATIONAL LEARNING: A NEW FOCUS.....	31
5.4 INFORMATION DISSEMINATION.....	32
<b>6. TRAINING REQUIREMENTS.....</b>	<b>34</b>
6.1 PHASE I: GENERATING QUALITY INFORMATION IN OIRAS.....	34
6.1.1 <i>Course objectives</i> .....	34
6.1.2 <i>Course Outline</i> .....	34
6.2 PHASE II: EXTRACTING QUALITY INFORMATION FROM OIRAS.....	38
6.2.1 <i>Course objectives</i> .....	38
6.2.2 <i>Course Outline</i> .....	38
<b>7. CONCLUSION .....</b>	<b>40</b>
<b>8. APPENDIX A. CONFIDENTIAL REPORT FORM.....</b>	<b>41</b>

# 1. Introduction

Commercial aviation is a very safe industry. The ratio of fatal accidents per number of flights is in the order of magnitude of  $10^{-6}$ . At this level of safety, although improvements are very difficult to achieve, still they are needed, particularly because of the growth of the industry. The benefits of reactive only solutions - design-fly-crash-fix - have been exhausted. Non-intuitive, proactive solutions must now be implemented to improve the safety record even further. The challenge behind such a commitment is to discover the unsafe features embedded in the system before they can produce any damage. Operational Incident Reporting and Analysis Systems (OIRAS) are increasingly considered a key tool from this perspective, and their value has been borne-out over the years. The Flight Safety Foundation's Icarus Committee has stated that "a properly managed in-house incident reporting program can help identify many deficiencies. By collecting, aggregating and then analysing incident reports, safety managers can better understand the specific problems encountered in line operations. Armed with that knowledge, they can create basic solutions instead of short-term fixes that only hide the real problems." (Icarus Committee, 1998).

On the surface, using incidents to predict and then prevent accidents seems a reasonable goal. Incidents often look like accident embryos. And the recurrence of similar incidents must reveal something about the risk of an accident. So one can expect to see accident precursors revealed by incident analysis. There are some more expectations and beliefs related to incident analysis, and they have been boosted by the availability of powerful computer data bases. The magic of large numbers combined with that of gigahertz storage even produced the illusion of spontaneous detection of weaknesses in the aviation system. The belief: "let's just feed the data base, and the computer will tell us where the problems are".

Unfortunately, there are a lot of data bases fed with a lot of data around the aviation world, but the computers remain silent - they alone can not tell us where the problems are. Acknowledging the need for a better understanding of the information that incidents can provide and how to process it, the Direction Générale de l'Aviation Civile (DGAC) issued a call for tender for a research study aiming at the development of a methodology for Operational Incident Reporting & Analysis Systems (OIRAS). This report is about the conclusions of that research. It does not intend to describe the details of one more incident reporting system. Instead, it will present and justify a different approach to incident reporting and analysis, through *a series of concepts* which can be implemented into an incident reporting and analysis system.

Throughout this report, many aspects of incident reporting and analysis will be tackled. All of them will be directly or indirectly linked to the same question: how to extract the lesson from the event(s). A metaphor may help to better grasp the problem. Using incidents to predict and then prevent accidents is like gold mining. Not all events are valuable. Someone has to sift through the dirt, and wash it away. Tons of mud must be filtered to find some gold dust. Nuggets are the exception. Then the critical issue is not the size of the sifting pan, but rather the capacity to discriminate a piece of gold from a bit of fool's gold or gravel. Most efforts invested in incident reporting have increased the size of the sifting pans and the number of miners; considerably less attention has been given to the discriminatory ability. Arguing that we don't really know what we're looking for until we see it, there is now a gold rush mentality - incident reporting systems have become an unstructured 'report everything' panorama of possibilities.

OIRAS need more guidance and structure to be efficient. Currently, we have many miners going over the same ground with the same tools, with an opportunistic approach to success. Is it any wonder that

they tend to find (and ignore) the same things? But sometimes a miner gets lucky. Experienced accident or incident investigators have an impressive ability to remember 'the' similar event, or to recognise significant patterns, or to guess the next implementation of Murphy's law. There is undoubtedly some kind of serendipity associated with this kind of human memory. But this is a quality of human intelligence, not an output of a data base (as some have imagined). One challenge for any OIRAS is to keep or adapt that ability when the size of the data reaches beyond any human memory capacity.

We do not claim to have discovered magic tools for data base manipulation. This report is not about how to introduce human intelligence into a data base, not even about an intelligent data base. We do not expect anything special to be introduced into the data processing capabilities. Our approach will be to use the data base a different way. The traditional approach is outside-in : incident analysis is typically understood as a way of identifying and fixing problems, with reference to risk models based on 'structuring' (engineering and procedural design) logic. Organisations are seen as machine bureaucracies, governed by standardised principles, and therefore predictable.

Adding to this false sense of simple predictability, most OIRAS have been adapted from accident investigation (AI) models which are by their very nature, reactive. These models assume that an event must be investigated in great detail to establish the precise causes before a safety lesson can be extracted. Establishing causes rather than lessons takes precedence (though obviously they overlap). To adopt the gold mining metaphor, accident investigators, upon hearing of the discovery of gold, proceed to dismantle the mountain rock by rock, certain that they will find gold more quickly in *other* mountains based on their work with this mountain.

Operational incidents and near-incidents are more like finding traces of gold or fool's gold. They are more frequent than accidents, and for logistical reasons alone they can not be investigated in the same detail. But adopting the AI model to OIRAS has encouraged analysts to look backwards rather than forwards, with the resulting over-emphasis on detail and causal factors. But do we need to know the precise linear causal chain behind every incident in order to deduce safety lessons? The most significant difference between accidents and incidents is the detection, protection or recovery factors that stopped the incident from developing into an accident. If we are to learn something different (something more) than what we currently learn with AI models, then these factors need greater prominence in any OIRAS. We also need to track the effectiveness of the interventions that originate from an OIRAS, to see if an organisation is truly "learning" from these reports.

In sum, we argue that most existing OIRAS derive from accident investigation protocols and have been somewhat effective in their role as a reactive safety strategy redressing identified deficiencies as perceived by current safety models, but we doubt the success of these systems as proactive tools for new and deeper organisational learning. As such we seriously doubt that current safety thresholds will be improved with the current application of OIRAS. Our approach recognises that OIRAS can provide unique information to an organisation about its risk awareness and risk management processes. We believe that an OIRAS data base will be more effective when it works top-down rather than bottom-up, so it can explicate the safety assumptions at work within an organisation, explicitly challenge them against the feed-back of facts gathered from occurrence reports, trace the rationale behind corrective action decisions, assess the efficiency of those corrective actions, and possibly challenge the safety assumptions again for the next iteration of the process. Ultimately, the success of any OIRAS should indeed be evaluated by the success of the interventions it proposes.

## 2. The limitations of current OIRAS

In Task One of this project, eight operational reporting systems were critically reviewed. These systems were:

- BASIS, British Airways Safety Information System
- ICAO ADREP, Accident/Incident Data Reporting System
- ECC-AIRS, pilot study on feasibility of EC reporting system
- MORS, Mandatory Occurrence Reporting System, CAA, UK
- OASIS and SIAM, Bureau of Air Safety Investigation, Australia
- CHIRP, Confidential Human Factors Incident Reporting Program, UK
- ASRS, Aviation Safety Reporting System, US-NASA
- EUCARE

These systems were found to vary on several dimensions:

- objectives of the system
- definition of "relevant event"
- sophistication of the safety model
- confidentiality
- reporting format
- coding and analysis systems
- feedback and information transfer

In the next section, we will briefly summarise the limitations and constraints operating upon current operational incident reporting and analysis systems (OIRAS).

### 2.1 The reporter

In the aviation industry, we rely on front line operators to report relevant events, i.e. we expect the actors of an event to be simultaneously observers and reporters of their own experience. This inevitably induces bias, especially for operational incidents where behaviours are the key issue:

- The perception of an event is subjective. It is driven, shaped and limited by the actor's intentions and awareness of the situation.
- "Everyone is a hero in their own story" - as reflected in event descriptions and causal attributions.
- Risk perception, the underlying basis of most reports, is highly subjective. If no risk is perceived, then usually no report is made.
- The operator decides what is worth reporting. One person's voluntary disclosure is another person's deliberately undisclosed violation.
- The reporter's perception is local, limited in time and space, while most events have broader systemic causality.
- The most significant events may not be reported because of denial, ignorance of safety implications, the desire to hide the problem, or fear of reprisal (despite guarantees to the contrary).

As the first filter of operational activity, actor/reporters provide a biased and incomplete sub-set of potentially relevant events.

## 2.2 The report form

Report forms are the second filter of operational activity, and they too are subject to bias.

- A report form must be sufficiently short and easy to use that operators are encouraged to use it, therefore the number of questions is very limited.
- Completely open questions (narratives) can fail to elicit useful information.
- Questions can guide the reporter, but they can also distort perceptions, leading the reporter to biased conclusions.
- The implicit safety model behind the OIRAS determines the selection of questions on the report form.
- The range of possible events is so broad that not all information can be captured by a standard form. It is often necessary for the analyst to contact the reporter to gain specific information.

In sum, a report form that is completely open will fail to attract quality information; a report form with too many questions will not be answered, and a report form based on the implicit safety model of the analyst constrains and therefore biases the reporter to see the world through the eyes of the analyst.

## 2.3 Data Bases

Data bases are a third source of unintentional bias in OIRAS.

There are several reasons why people choose to store information in a data base:

- because they will *need it* later (full retrieval)
- because they will *need some of it* later (partial retrieval)
- because they think they *might need some of it* later (an insurance policy)
- to create a record/history of what has gone before (recreate the past)
- to justify a program's continued existence (quantity implies quality)
- because they can (computer capabilities).

Current OIRAS databases have been created for all of the above reasons, yet the ad nauseam recording and classifying of incident and near-incident data and their causes has proved too 'resource heavy' for even the most dedicated organisation.

OIRAS data bases have proved problematic for many organisations for several reasons:

- In order to be stored for later retrieval, there must be some categorising of the initial information.
- This is not a problem with regard to the objective physical parameters of the flight, but it is an issue in the more subjective description of the event and the causal attributions.
- As with the report form, it is impossible to anticipate all contingencies, therefore it is impossible to create an exhaustive list of keywords.
- Also, keywords are static, binary (either present or not present) and can only be combined in a linear additive fashion. This is a very poor approximation of the real world.
- Information is retrieved according to how it is stored, hence the categorisation derived from the analyst's safety model determines the output parameters. (Put simply, if there is no keyword called 'technical failure' in the data base, then 'technical failure' will never be found to be a cause of incidents in such a data base.)
- A model of safety, either explicit or implicit, which guides the categorisation schema, becomes a self-fulfilling prophecy. One can extract from the data and confirm (to the extent possible with the constraints mentioned above) only what one already knows. For example, many OIRAS bias the keyword categorisation toward CRM. Consequently, CRM is often cited as both the cause of the problem and its cure (more CRM training will redress the perceived CRM deficiency).

- Little is learned from such circular reasoning other than what one already knows.
- Much of the information in the databases is never retrieved once it is entered.
- If a keyword search does identify a case, the analyst usually has to go back to the original report to understand all the details in context (because of the general inadequacy of the keywords).
- Once a database grows beyond the memory of the analyst, it becomes a storehouse, but it does not become the memory of the analyst - material is "forgotten".
- The predetermined keyword structure is a powerful biasing agent. Reports are analysed to "fit" the keywords. Details that don't fit are ignored. As a result, what we don't know remains unknown, and worse, is not given credence.

With all the work on database creation and management, there is little being done to record and track the safety responses made by the organisation, and the safety challenges still requiring a resolution. A data base that tracks and evaluates the effectiveness of the organisation's responses to the incidents, a meta-analysis permitting an overview of the safety system, would serve two purposes:

- It would refocus the system on its improvement strategies and show which strategies were effective. For example, the recurrence of a strategy over time would suggest the failure of that strategy to improve the system.
- The data base would also serve to explicate the underlying safety models being used within the organisation. For example, the recurrence of a "more training" strategy would suggest an organisational over-reliance on training as a response.

## **2.4 Data Analysis**

There are currently two streams of data analysis. As a report is received, it is entered into the predefined data base. (Despite how resource-heavy this process has proved to be, it is currently the unquestioned norm in the industry to enter every report into a data base.) Reporters are notified that their reports have been received. The analyst then decides the action to be taken, and initiates it. The action is usually determined by the analyst's perception of organisational risk inherent in the incident. If the incident is perceived as being sufficiently serious, resources are dedicated to understanding it more fully. This is the clinical approach. Depending on the event, different personnel from the organisation are involved in the problem-solving. In essence, the clinical or case-study approach is like a mini accident investigation.

The second stream of analysis - trend analysis of the data base - has failed to fulfil its promise.

### **2.4.1 Trend Analysis**

Physical objective parameters of a flight are easy to record and difficult to dispute. They can and have been used effectively to track patterns. This information can be retrieved from most OIRAS, however the ultimate recording of objective "deviation" data does not happen within an OIRAS but in FOQA or other flight data recording systems. (Recall that an OIRAS contains only a biased sub-set of the relevant events in the system.)

Attempts to derive meaningful trend analysis from the more subjective parameters of OIRAS databases have been less successful for several reasons:

- It is difficult to compress raw data into structured information without losing key information (especially if what is significant can only be determined retrospectively).
- The limits of keyword categories (to fully capture a context).
- The limits of data bases (not all relevant events are reported or reported accurately)

- The inability to forecast which parameters may be important, sometime necessitating an expensive revisit and revision of the data base.
- Poor inter-rater reliability of analysts due to -
  - different implicit safety models
  - poor training in the analysis process
  - subjective nature of the causal attributions made by reporters and analysts
  - the wide-ranging causal possibilities in complex systems

These logistical problems are magnified dramatically when one tries to combine data from different data bases, as would be the case for a regulator or manufacturer. Many airlines use analysts who are knowledgeable about the context (e.g., they use a 747 captain to analyse reports from the 747 fleet). This local understanding of a problem is lost when data are combined. Combining subjective data from disparate sources makes trend analysis highly suspect. The more objective the data, the more plausible the trend analysis. Unfortunately, OIRAS are by their very nature, subjective.

Quite apart from logistical constraints, perhaps the most fundamental obstacle to trend analysis has been the lack of intelligent questions asked of the data bases. Data base probes usually take the form of summary statistics of different combinations of keywords. Even so, it is the analyst who has to interpret this data and pose more complex questions. This step may be difficult if the analyst is unaware of his own safety model and assumptions, or if he is aware but unwilling to test those assumptions. This problem is most acute for trend analyses of causal factors, considering that causal attributions are a direct manifestation of the analyst's safety model. ("I retrieve the causes as I entered them" - the database is just a mirror of the analyst's thinking.)

An alternate explanation for the lack of meaningful trend analysis may be that due to the inescapably flawed nature of the OIRAS databases, analysts prefer to develop hypotheses based on the clinical case-study approach, and then probe the system precisely and proactively (directly, in real time) rather than rely on the database (reactive and incomplete). Example: upon detecting a particular problem, the Safety Office decides to survey the pilots about this specific issue in order to determine more precisely the true prevalence of the event, and its associated risk, in the system.

For a combination of reasons, trend analysis has not been very successful within OIRAS. This realisation must also raise questions about the true utility of OIRAS data bases.

## 2.5 Are we learning anything?

Apart from the logistical issues associated with data base storage and retrieval of subjective data, perhaps the real challenge in any OIRAS is to challenge our thinking about the system's safety and to learn something we didn't already know.

In an OIRAS, there are several challenges, including:

- being able to be truly "surprised" by the data, i.e., being open to the data in a way that allows us to challenge our own assumptions about safety.
- serendipity - being able to "see" previously unrecognised significant events or patterns
- 'generalising' the understanding of a single event into a comprehension of generic weaknesses or failures in the safety defences of the system.
- understanding the system's complex interconnections while looking at single events (seeing the forest *and* the trees)
- developing hypotheses from the reports which can be tested with the existing data base or through proactive probing of the system
- building the credibility of the lesson learned about the weakness discovered in the safety of the system.



- recognising when a safety strategy has been overoptimised or is no longer effective
- recognising when a solution to one problem can create another problem in the system (as we have seen with some instances of automation).

To summarise the current limitations and constraints surrounding OIRAS, these systems are effective only to the extent that they can test (confirm or deny) existing though often implicit safety models. There are upper bounds on the quality and management of the data, especially the subjective data, and the resources needed to administer and interact intelligently with these data-heavy systems are costly. Even so, most data in OIRAS remain unused (never retrieved from the data base), and organisational learning is reactive and/or stunted. In a complex safety system employing many safety tools, important modifications need to be made to current OIRAS to warrant their useful continued existence.

## 3. An improved OIRAS: Functional and theoretical considerations

### 3.1 Functions of an OIRAS

#### 3.1.1 *Extracting 'safety lessons'*

The functions of an operational incident reporting and analysis system (OIRAS) can be of significantly different nature. The first obvious function is *certainly extracting an explicit 'safety lesson'* from the occurrence(s). In other words, incident analysis is understood here as a way of identifying and fixing safety problems as such.

A safety lesson may be extracted from:

- one or a few similar incidents, because they can be considered as *precursors* of an accident, which means that they clearly appear as an incomplete sequence of a well identified accident scenario.
- one or a few similar incidents, because they indicate the possibility of an event or a situation which was missed in the system safety analysis, or clearly indicates that an important *assumption about the safety of the system is challenged*. In that case, like in the previous one, the effective approach is a 'clinical' analysis of the event(s), similar to that of an accident investigation.
- a large population of minor incidents, because analysing that population can uncover specific unsafe patterns of events or circumstances, or to realise that some actual frequencies are not consistent with safety assumptions, or to discover dangerous trends. In this case the approach is an epidemiological one : cues emerge from large numbers, or at least are expected to (see §2.5).
- a large population of minor incidents, because analysing that population allows to discover correlation between those events and specific environmental, procedural, or situational parameters, thus suggesting that there may be a 'causal' relationship between the events and those parameters.

#### 3.1.2 *Additional functions*

However, the potential contribution of an OIRAS to safety management is not limited to the *extraction of explicit safety lessons* to be worked on by the relevant people (safety managers, regulators, ...). Here is a non exhaustive list of possible additional functions :

- *keeping the operators informed about how they actually perform*. Giving them real feedback through statistical figures, or even providing them with anecdotal information ('this happened to your peers'), can efficiently trigger behavioural changes without any structured modification into the system (training, procedural change, and the like). In one airline, the mere fact of informing the pilots that, according to the FOQA program outcome, a majority of them were over-rotating a specific type of aircraft spontaneously led to the correction of the problem.
- *making the threat more visible*. Safety cannot be based only on a blind adherence to procedures. Humans are more efficient with a procedure when they feel a need for that procedure to help or protect them. Some fear within the system is therefore a necessity. But systems like aviation are so safe that the experience of danger is extremely remote from an individual perspective. Risk is below individual perception thresholds. Sharing the global system experience is the only way to keep some fear within the system.

- *showing coping strategies.* Some incidents not only appear as an incomplete sequence of an unexpected accident scenario, they also reveal unexpected protections which luckily prevented them from developing into a real accident. It is important then to try and 'institutionalise' the effect of luck through specific training, a change in the procedures, or merely through informing the operators.
- *triggering further investigations.* An incident can suggest that 'there may be something more serious to check'. In other words, an incident can raise questions about the existence, frequency and severity of abnormal situations in the system, and therefore trigger further investigations, which can take the format of a data base query, an informal questionnaire, or a full scale audit.
- *organisational learning.* Investigating incidents can facilitate short and long term organisational learning if employees are directly involved in that process, instead of being merely the final receivers of the conclusions. Effective incident analysis often implies bringing together distributed partial knowledge about the system. Involved employees can then develop and complement their understanding of the equipment and operational issues, develop their analytical and imaginative skills, discover more issues, learn about their own understanding limitations, share experience and understand the opaque interactions between specialised activities. They can develop a collective understanding of the improvement options.

## 3.2 Theoretical bases of OIRAS

### 3.2.1 The definition of an incident

Annex 13 to the ICAO Chicago Convention defines an incident as an event linked to the operation of an aircraft, which is different from an accident, and jeopardised or could jeopardise the safety of the operation. It defines a serious incident as an incident whose circumstances indicate that an accident almost happened, and clarifies that the difference between an accident and a serious incident lies merely in the final outcome. Indeed Annex 13 defines an accident as an event linked to the operation of an aircraft and during which a damage (to people or to the aircraft) worse than a given threshold has been experienced, or during which the aircraft has disappeared.

The concept of 'incident' has therefore mainly two boundaries :

- the first one discriminates 'incidents' from 'accidents' : it is based on the level of damage experienced during the event. There is a threshold of damage below which the situation would be considered 'incidental' and above which the situation would be considered 'accidental'.
- the second boundary discriminates 'incidents' from 'normal' events : it is based on the threat to safety which 'appeared' through the event. This boundary is much more difficult to define. It is related to our comprehension of what makes the system safe or unsafe (e.g. committing an error may or may not be considered an incident depending on the circumstances, the nature of the error, the relationship perceived between errors and incidents,..). It is also related to the level of safety which is expected from the system (e.g. in the nuclear industry, the mere unavailability of a second rank defence is considered an incident even if it has not been needed).

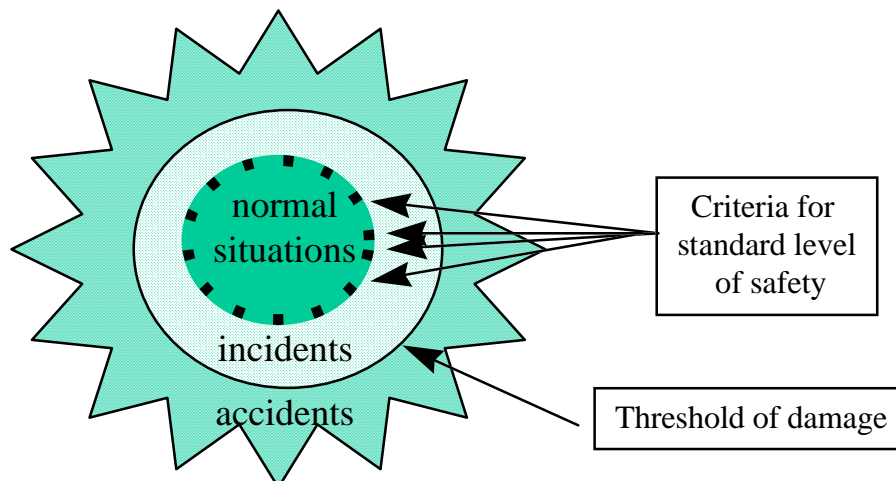
### 3.2.2 Difficulties in the concept of incident

The meaning of the expression 'jeopardise the safety' in the ICAO definition is blurred. The definition is therefore complemented in Annex 13 with a reference to an explicit list of types of incidents of particular interest for the prevention of accidents. That list does not pretend to be an exhaustive one, so part of the decision to consider a specific event as an incident is left to expert judgement (the reporter's, the analyst's,..). Is it possible to go further and assist that kind of judgement with a more accurate interpretation of 'jeopardising safety' ?

A first approach can be to consider that safety is jeopardised when the probability of an accident has increased from the 'standard' level by more than an acceptable increment. It would be the rational approach. Unfortunately, such a probability cannot be estimated, except perhaps for serious incidents, as defined above, i.e. quasi accidents. Furthermore, the 'standard' probability of an accident is hard to define, as it actually varies continuously from one flight to another, an even within one flight, with many parameters such as flight profile, flight phase, weather conditions, traffic density, crew fatigue and the like.

A second approach can be to consider that safety is jeopardised in any event where at least one of the 'objective' criteria accepted by the system as an indicator of (or a condition for) a standard level of safety has been breached. As shown at the figure below, such criteria typically include :

- adherence to critical safety procedures
- safety margins : e.g. 'X NM' or 'Y Feet' separation between two aircraft ; 'X feet' above obstacles ;
- limitations to 'normal' operation domains (speed, altitude, weight and balance, load factor...)
- availability of critical protections (e.g. stall warning, GPWS)
- minimum equipment (MEL)



Then, the definition of an incident would read : 'any event where at least one of the 'objective' safety criteria accepted by the system has been breached'. However, such a definition would be either very incomplete or very restrictive. If we stick to a very pragmatic and operational point of view, and consequently limit 'safety criteria' to the availability of residual margins or protections, it will be incomplete because many losses of control are recovered before breaching the margins, and reaching those criteria. If, on the other hand, we extend the concept of safety criteria to include all kinds of system specifications (e.g. all Standard Operational Procedures), then the definition would be very restrictive because it would tend to equal the safety of the system and the absence of any deviation. In the next paragraphs, it will be argued that the safety of a system cannot be based on the absence of deviations, and we will attempt to determine a more reasonable definition of "not jeopardising safety".

### 3.2.3 Safety through specification

A first strategy to design the safety of a system is to call on invariant functional properties of the world (environment) to elaborate relevant operational responses. The ideal achievement is then to design and specify responses which are perfectly adapted to a situation demand. These solutions are

generally crystallised in organisational charts, specified in documents in the form of rules and procedures, stored into the operator's long term memory under the format of procedural knowledge (rules and skills), and implemented according to the situation.

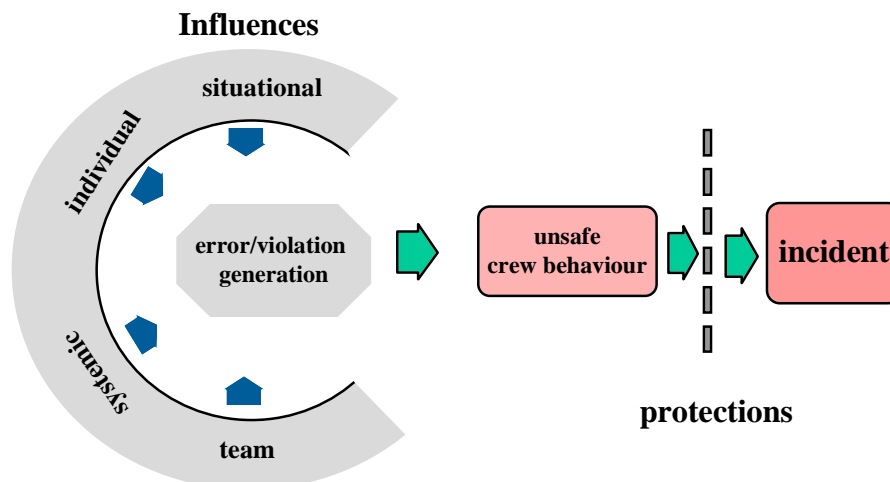
The main safety problem is then to remain within the frame of a known situation, and to stick to the proven solutions. In this approach, safety is impaired when the environment varies (de-adaptation), when the technology fails, or when the standard solution is not adhered to (errors will inevitably be committed by humans, violations are expected not to be committed).

It follows that the main strategies for safety are, first the *prevention of deviations*, mainly through the correction of deviation prone conditions, the development of a 'professional' culture respectful towards procedures, or the threat of punishment on the deviants, and secondly the *protection against the consequences of deviations*.

Consequently, the corresponding incident (occurrence of an unsafe situation) models, which actually serve as the background reference for most of the current OIRAS, more or less share the following structure :

- an error (unintentional) or violation (intentional) *production* engine. The engine is fuelled by influences (contributing/triggering factors) at the individual, team, situational or systemic level.
- errors and or violations then combine with circumstances into 'unsafe' operator behaviour
- protections designed into the system, or provided by positive human operator's behaviour, or provided by luck, prevent the 'unsafe' potential of the behaviour from leading to an accident.

This incident model is represented schematically at the diagram below :



### 3.2.4 Safety through adaptation

It can be argued that such 'normative' approaches to safety, seeking a reduction of variety and variations within the system, are based on a simplistic metaphor of socio-technical systems, seen as linear deterministic machines. They are also inherently reactive : they are based on a design-fly-crash-fix (or at least design-fly-fail-fix) loop, which is external to real time dynamic production processes. While they have been the keystone of safety improvements during the last twenty years or more, and have widely contributed to reach the current safety thresholds in aviation, they are unlikely to improve the system past the current ratio ( $0.5 \cdot 10^{-6}$ ), as currently displayed by the best operators.

Beyond such a safety level, the potential for improvement is so thin that merely pushing further the normative approach would not provide the expected results. Negative collateral effects (due to impeding natural human risk management mechanisms) would no longer be of second order compared to the benefits of the normative strategy. A more realistic conceptualisation of the human-technology interaction is needed. A contemporary alternative is a shift of the metaphor of systemic models from 'Machines' to 'Ecologies'.

The 'Ecology' metaphor suggests that systems are not totally stable, and cannot be entirely specified. They are adaptable and are constantly adapting, at the local/individual/real time level of front line operators as well as at the global/collective/long term level. A fundamental difference is that *deviations* are not considered abnormal events but rather the normal situation because :

- the production process is rarely a linear sequence of actions as described in the procedure: there are very often several competing processes, leading to mutual interruptions, and requiring prioritising;
- errors will inevitably be committed by humans; indeed, humans take actions upon the real world in which they are immersed (their environment) in reaction to their representation of that real world. Representations are never true to reality : they are schematic, distorted, anticipatory (i.e., partially driven by themselves, and independent from sensorial feedback loops). Actions are rough, imperfectly controlled, subject to lapses. Sensorial feed back is a very limited and oriented filtering process.
- the technical equipment is rarely standard : modifications will progressively particularise individual aircraft or equipment, minimum equipment list will allow flights with unserviceable equipment, failures will occur during the flight, etc.
- voluntary deviations will also occur, most of the time linked to prioritisation due to the constraints discussed above ;
- unanticipated events, abnormal contexts will also occur, with no anticipated 'standard' solutions ;

Seen from an ecological perspective, errors and deviations are not failures, but the expression of adaptability. They provide the necessary internal variety, as a source of adaptation to external uncertainty, as suggested as early as 1956 by Ashby's<sup>1</sup> Law of Requisite Variety. Operational responses are permanently imperfect, because they must include latent, open solutions to different and unforeseen situations. They are also the expression of operators' ability to learn from experience. Furthermore, they provide a means to find out where the (blurred) limits of a system are, in order to flag them and respect them.

The ecology metaphor suggests a flexible and learning approach to safety. The key issue is keeping control on deviations, through an adequate balance between stability and adaptability, between specifications and intelligence. The deviation management process includes a monitoring of random or unforeseen variations, both externally in the environment, and internally in the operational responses (failures, errors and deviations). Deviations and unanticipated/random events are detected by 'virtuous' loops. Deviated actions generate unexpected representations which generate deviation & risk assessment, in which the nature and intensity of the potential threat introduced by a deviation is assessed. It is important to understand that, by far, not all deviations should be corrected. Some errors or abnormal events can be ignored without risk. A correction of the representation will be achieved and/or correcting actions will be taken (mitigation of deviation consequences), only if it is felt to be a need according to the risk assessment<sup>2</sup>.

The deviation management process also includes a self monitoring of the efficiency of the monitoring process. So it stands as a self-referencing system, with a stability of a dynamic nature. A stable mode occurs when the reactions of the operators to their representations generate a reality consistent with

---

<sup>1</sup> Ashby, W.R. (1956). Introduction to Cybernetics. John Wiley, New York.

<sup>2</sup> In a process similar to biological immunity, defences are created and developed in response to pathogens recognition (hence they need aggressors to develop).

those representations. There are bifurcation points where virtuous loops suddenly shift into vicious loops : deviated representations generate deviated actions which generate a reality which is more and more inconsistent with representations, without any perception of such a shift.

In summary , the safety of an operation ultimately results from a permanent ongoing adaptive risk control process. This risk management process relies **both** on :

- a normative prescription (a music score) which describes the potential situations (nominal, abnormal, emergency), defines and plans for the relevant actions, assigns the roles, the task sharing, defines the human/machine and the human/human co-operation ;
- a dynamic, real-time implementation of the above prescription (the intelligent interpretation of the music score), which includes:
  - a permanent deviation management process : monitoring, self-monitoring, detection, prioritisation, correction of deviations (not all of them); the anticipation and/or recognition of abnormal (up to emergency) situations and their management ; and also
  - a meta-management process: resource management, external and internal (cognitive compromise) risk management;

More than deviations, what must be prevented is the loss of control of the risk management process on the situation hence an incident can be broadly defined as the failure of the risk management process. From this perspective, we can learn from both risk management failures (including incidents) and risk management successes. Therefore **an OIRAS should be designed so as to allow the analysis of both risk management failures and risk management successes.**

### 3.3 Analytic approaches

With risk management included in an incident model, three levels of analysis are possible and necessary. The first is the *Narrative* or 'descriptive level'. This places the event in its context - the facts, circumstances, and physical parameters of the event. To the extent possible, it is a matching of the report to the physical reality of the event with minimal interpretation. It highlights the need to understand the context (the same event can be considered normal in one context, and highly abnormal in another).

The next level is the *Explanative* or 'causal level'. Here the analyst is interested in the deviations - the errors and violations production process - and also the defences which failed. All possible influences and contributions are considered to help explain the cause of the event: individual (personality, attitudes, skills); team (synergy, team norms, habits, shift hand-over,...); systemic (training, procedures, man/machine interface, time pressure, culture, ...); and situational (circumstances, luck, chance).

The third level addresses *Risk monitoring*. Here the analyst can ask several questions to determine the apparent failure of the risk monitoring process:

- What was the danger (risk)?
- What was the risk management strategy that was supposed to be used ? (safety principle)
- What was the actual risk management strategy that was used ? How well did it work ? How did it fail ?
- What is the lesson ?
- What are the potential corrective actions ? What is the action selected to be taken ? Why ?
- Who should know about this? (do we need to change mental representations about this risk)
- What is the next check on the efficiency of the action taken?

The three levels of analysis together will render a complete understanding of the event. More importantly, they will go beyond the individual event to render information about the organisation's risk monitoring processes by highlighting broader weaknesses. This integrated approach will also

explicate and challenge different safety assumptions, as will be seen in Section 4, 'Functional Specifications'. Further details about the tracking and evaluation of the organisational response to the event can also be found in Section 5, 'The Role of the Safety Office'.

### 3.4 Risk management monitoring throughout the 'system'

What has been called 'the system' in the previous part of this document must now be clarified.

An obviously relevant 'system' is formed by the front line operators at work. At this level, front line operators interact in real time with the real world, maintaining, refuelling, flying real aircraft. The 'system' is the coupling of teams and/or individual human operators with their technological, physical and social, local environment. Individual behaviour as well as team behaviour are typical relevant safety issues at this level, which are covered by the traditional 'Human Factors' approach, including man/machine interaction, environmental influences, ergonomics, traditional CRM (team dynamics), cognitive processes, and the like. We will refer to this level as the '*Front Line Operator*' level. It will include not only pilots and cabin crew, who are the sharp edge operators, as they are 'at the scene' and directly interact with the flight all along, but also maintenance personnel, dispatch personnel, ramp staff, Air Traffic Controllers, and other 'operational' people, who may be at least partially removed from the real time flight scene, but directly influence it by their actions and decisions.

But we know that the environment in which front line operators actually perform their tasks is determined by management decisions, structures, organisational processes, and cultures. Indeed, selection, training, procedures, cockpit design, work conditions, company culture, professional (sub)cultures govern individual or team behaviours. Management decisions and organisation processes also determine the extent to which work contexts are prone to error and violation, or facilitate deviation management and risk management processes. If we consider OIRAS as a risk monitoring tool, then it must also address the (operational) organisational level, not just the front-line operational level. That organisational level typically includes airlines, with their different departments (flight, maintenance, ..). It also includes Air Traffic Management organisations, Airport operations. We will refer to this level as the '*Organisations*' level in the next part of the report.

But again we can broaden the perspective, and realise that airlines and other operational organisations are not isolated and autonomous components, floating in a vacuum. Airlines inherit from aircraft manufacturers specific cockpit design, operation manuals, maintenance procedures, training philosophies. They are bound by economic competition, political and social constraints, national and international regulations. So the relevant 'system' would ultimately be the global civil aviation industry, including all the airlines, manufacturers, authorities, unions, international bodies, and the like.. At this level, what we have is a macro-system, and safety issues are more political, economic, and cultural than 'technical'. For instance, deregulation generates more competition which generates economic strains which generate pressures for under-staffing and for lower wages, which generates higher turnover and loss of skilled manpower, and so on. However, currently, aviation safety is not really managed through executive decisions at this global level. What takes place at this level is more of an harmonisation of what takes place at lower levels. To some extent, airlines discuss their philosophy and exchange their practices through organisations like IATA, manufacturers communicate with their customers, civil aviation authorities develop and reinforce national and international regulations. But there is no unified theory and language to address safety issues at that level, nor does a global united body exist to handle it. Therefore, for the time being, we suggest to incorporate only two aspects of the macro-system level into the A-OIRAS: aircraft manufacturers, and civil aviation authorities.

Aircraft manufacturers have a pivotal situation. Many of their decisions have downstream impact on the actual operation of their aircraft and strongly influence safety: design decisions, operation



procedures design, associated training philosophy . We will refer to this level as the '*Manufacturer*' level in the next part of the report.

National and international regulation (e.g. FAR, JAR) regulations dictate shared references for the safety principles of the system. The national civil aviation level is currently relevant because national regulations (or the national instantiation of international ones), national cultures, economics and political issues interact to really shape the reality of air operations, and make them different from those of the neighbourhood. In the next part of this report, we will call this level the '*Authority*' level.

Safety assumptions exist at all four levels - it is these assumptions which need to be explicated, monitored, and challenged with the appropriate OIRAS. Consequently, an OIRAS should allow such an explicating, monitoring and challenging process, with reference to reported events, at all four levels.

## 4. An improved OIRAS: Functional Specifications

This section will describe the functionality that should be provided by an advanced OIRAS (A-OIRAS) in order to make it a risk management monitoring tool. It will start with higher level functions intended for the analysts or the other users of the system, and then work backwards and describe how the OIRAS should be organised in order to support the higher level functions.

### 4.1 Basic features of the proposed system

The following features are intended to provide acceptable responses to the challenges described earlier, to take advantage of the potential resources brought by new technology, and to be a first step towards a broader conception of a safety reporting process as a component of an 'organisational learning process'.

- The OIRAS will be 'conceptually top-down' (from safety assumptions to events), and forward-oriented ('*risk management oriented*'), instead of bottom-up (from events to safety lessons), backward-oriented ('*causality oriented*'). In other words, the ultimate goal of the reporting and analysis process is not to analyse the causes of incidents, but to improve the system's understanding and management of its own risks.

The information processing will therefore be driven by the following pattern :

- what kind of operational risk is that event (family of event) connected to ?
  - is that operational risk domain already considered a risk monitoring priority ? If not, should it become a risk monitoring priority ?
  - What are the risk management strategies (the safety principles) associated with that risk domain?
  - Which of them were actually triggered during the event ?
  - Which of them were successful ?
  - Which of them failed ?
- The OIRAS will be company/organisation oriented instead of 'safety specialist' oriented. Information processing will be *distributed* through the organisation.
    - The Safety Office within airlines, manufacturers, ATM organisations, Civil Aviation Authorities, will mainly act as a dispatcher of information, a catalyst of safety questioning, a facilitator of feed back information. (See Section 5 for more details within an airline environment)
    - The Safety Office will act as a safety network manager : part of the analyses will be conducted by the different specialist organisations (e.g. within an airline : Operations, Maintenance, Training departments. The Safety Office can also ask a series of CRM workshops to discuss a specific safety issue and report their conclusions.)
    - The analysis process will include the manufacturer as necessary to clarify technical or operational issues, design philosophy, ...
  - The OIRAS will not be limited to incidents : it will include all 'safety relevant events' where a successful recovery process took place.
  - The output of the OIRAS will not be limited to a causal analysis and recommendations for the modification of the system. It will also include :

- ‘anecdotal’ feed back : reporting what happened to the front line operators to improve their representations about the risks, and risk management strategies
- connections to the training system : to feed the training system (CRM workshops, simulators, ..) with scenarios, case studies, ...
- Adaptive keywords
  - Recognising the evolutionary nature of an OIRAS as an organisational learning tool, certain keyword groups will be 'living lists' which will expand as more data is received from operators, and as analysts challenge and expand their own thinking.
  - Namely, the lists of safety principles, failure modes, recovery modes, and corrective actions (see § 4.3.3) will grow with the diversity of reports.
- The OIRAS will be organised as a multi-layer analysis tool and a network connecting several levels of organisation: Front Line Operators, both individuals and teams ; operational Organisations (e.g. airlines), Manufacturers, Authorities.
- The design of the OIRAS computer system will allow for a multimedia recording, storage, and information processing provision. Indeed the expansion of new information technology will quickly allow for the reporting of events through different media : sound, video, digital data. Future cockpits will probably incorporate simplified data transfer systems allowing for a download of CVR, DFDR, Video (this should also facilitate the development of self-debriefing tools providing the crews with an immediate reconstruction of the flight, as an immediate feed-back ).

## 4.2 The functional outputs of the system

The system shall be capable of the following:

- allow authorised persons to access the database through an identification password, and further complement and modify the data
- store and retrieve information related to individual events with provision for multi-media formats
- resist multiple input of the same event
- discriminate between established factual data, and assumptions
- discriminate between descriptive data, and causal interpretations brought up by the clinical analysis of individual events
- further discriminate between the different origins of information : the reporter, the analyst(s), the airline operational departments, the manufacturer...
- allow individual events to be back up to risk management strategies
- allow individual events to be back up to failure modes
- allow individual events to be back up to recovery strategies
- allow individual events to be back up to follow up actions
- retrieve a set of events sharing a common combination of features
- show potential patterns of contributing factors behind a designated set of events
- show potential patterns of deviation (error, violations, failures, unexpected events) management behaviour (prevention, detection, recovery) behind a designated set of events
- filter and format the information related to individual events in order to communicate them to third parties with a format appropriate to the potential receivers: Authorities, Manufacturer, other Airlines.
- display automated ‘flag’ warnings about the realisation of pre-programmed ‘abnormal’ conditions (event frequency range, specific combination of factors, ...)
- store anticipated results expected from the follow up actions, and means to assess the actual effects of these actions

## 4.3 OIRAS Format

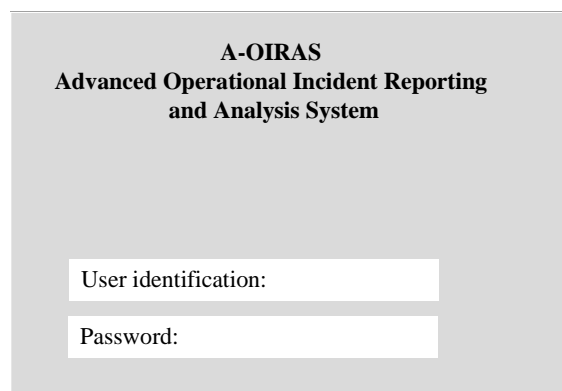
### 4.3.1 Objectives

This section will describe the functional layout of the Advanced Operational Incident Reporting and Analysis System (A-OIRAS). As stated above, the fundamental difference between A-OIRAS and current OIRAS is that it is 'risk management oriented' instead of 'incident analysis' oriented. The focus is not incident description and causality, but risk management. Consequently the traditional approach is inverted. The traditional approach is to seek risk management strategies through an aggregation of incident reports. The proposed approach is to look at incident reports through pre-established risk management strategies. An incident is then analysed in relation to the organisation's existing risk management strategies.

In order to facilitate that description, it will be presented in the following paragraphs in the form of a computer interface mock-up. However, this is not intended to mean that this interface would be the most appropriate one to meet the functional requirements established in the previous paragraphs. This interface should only be considered a presentation tool, in other words a metaphor, of the functionality expected from the A-OIRAS.

### 4.3.2 Overall structure

The A- OIRAS is a computer software program accessible by anyone in the organisation with an identity and a password giving relevant rights to access, retrieve and edit the data.

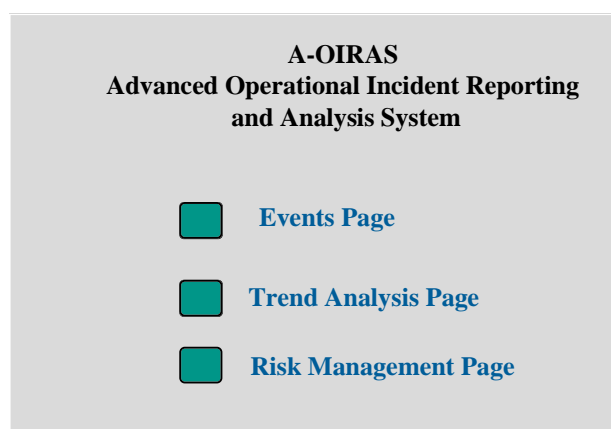


A-OIRAS  
Advanced Operational Incident Reporting  
and Analysis System

User identification:

Password:

Next access is to a menu of three items :



A-OIRAS  
Advanced Operational Incident Reporting  
and Analysis System

- [Events Page](#)
- [Trend Analysis Page](#)
- [Risk Management Page](#)

- The *Events Page* gives authorised persons access to a list of stored events, designated by a reference number, a date, a title.

File	Edit	Description	Sort	Trend
<b>Events Page</b>				
Event Reference	Date	Aircraft	Title	

This list can be edited (a new event can be added to the list).

A double click on any individual event, or pulling the Description menu gives access to an Individual Event Description Page.

File	Edit	Events	Sort	Trend
<b>Individual Event Description Page</b>				
Reference	Date	Aircraft	Title	
<b>Descriptive Factors</b>				
<b>Narrative</b>				
<b>Interpreted causal factors</b>				

This page allows the entry of data concerning a new event, or the modification of existing data. The Individual Event Description Page is the interface used by the analyst to 'code' a new event into the event data base. Data concerning an event includes both, and clearly discriminates between, two categories of data :

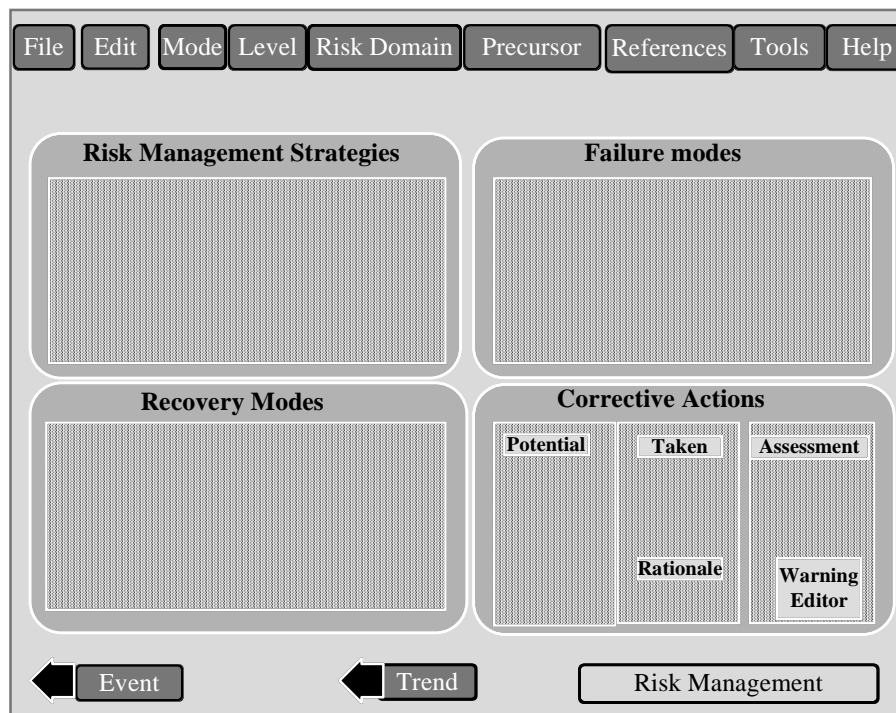
- a set of objective and factual descriptive factors (date, type of aircraft, phase of flight, proven scenario ....) and
  - a set of subjective explanatory factors as established by the safety analyst if a 'causal analysis' has been conducted ;
- the *Trend Analysis Page* gives access to a traditional trend analysis tool. The trend analysis tool clearly discriminates between :
    - conclusions and causal assumptions inferred from 'statistics' on descriptive data (e.g. 80% of reported destabilised ILS approaches shared the following features : short haul flights & cavok weather conditions & heavy ATM traffic reported; this has been shown to be statistically significant ; a reasonable interpretation is that flight repetition and ATM pressure influence approach stabilisation) ; and

- frequency of causal interpretations brought up by the clinical analysis of individual events by safety analysts (e.g. 80% of reported destabilised approaches have been attributed to routine and ATM pressure by the analysts).
- the *Risk Management Page* is the kernel of the system, and will be further described in the next paragraphs.

The Events Page and the Trend Analysis Page are very much similar to those provided by currently existing incident data base.

### 4.3.3 The Risk Management Page

The **Risk Management Page** gives access to a screen as shown in the following schematic :



Some menus have pre-set categories, and others are created to be amended as a function of incoming reports through the edit menu.

#### 4.3.3.1 The main menus are:

- *File* : to manipulate the file (open, close, save, format, export, import, quit)
- *Edit* : to edit some menus content : Risk Domain List, Precursor Family List, Individual event list, etc.
- *Mode* : to select one of two basic modes :
  - an Event Entry mode : allows the analyst to create links between that event (and its Individual Event Description Page) and the Risk Management Page components, as explained further

- a Risk Management mode : to use the Risk Management Page (e.g. review incidents related to a failure mode, find frequencies, etc.)
- *Risk Domain*: displays the Risk Domain List and allows for the selection of one. The Risk Domains can be thought of as potential typical accidents that have been identified by the organisation and that the organisation strives to prevent. Below is an example of such a list :

#### **Indicative list of typical accidents**

1 CFIT/ initial climb /go-around/ final approach	7 Ground collision on active runway
2 CFIT/ climb/ cruise/initial approach	8 Severe turbulence
3 Loss of control (takeoff/initial climb/final approach)	9 Uncontrolled fire in flight
4 Loss of control (climb/cruise/initial approach)	10 Uncontrolled technical failure in flight
5 High speed runway excursion (landing / take-off)	11 Crash landing
6 Mid-air collision	12 Failed emergency evacuation

That list is hierarchical : priorities (e.g. red, amber, yellow) will be allocated to the items in the list and these priorities will influence the corrective actions' decision process, particularly the cost/benefit assessment. Priorities will be attributed both from an external rationale (specificity of the operations, accident history, known weaknesses...) and an internal rationale (based on the frequency and severity of internal incidents).

- *Precursor*: for each typical accident, it displays a list of precursor scenarios and allows for the selection of one. From each typical accident in the list, the organisation builds a list of potential major precursors, which contains the main typical incidents that could eventuate in that typical accident. For example, an incident family developed from "Ground collision on active runway" would include runway incursions, landing on the wrong runway, and crossed runway simultaneous operation mishaps. Each risk domain can generate several incident families, or none.
- *Level* : allows for the selection of a level of organisation, as described at § 3.4, at which the analysis will be conducted : Front Line Operators (individuals or teams), Organisations, Manufacturer, Authority . The selection of any of the four levels will govern the content of the lists included into the four main windows (see the next paragraph). Indeed, safety assumptions, failure modes, recovery modes and corrective actions exist at all four levels, while also being (partially) specific to each level.
- *Tools* : gives access to statistical data processing tools
- *Event* : gives access to Individual Event Page.

#### **4.3.3.2 The page also includes four interactive windows with the following titles :**

- *Risk Management Strategies* : includes a list of safety principles. Identify the relevant 'safety principles' through the following question: how was the system supposed to be protected against that risk (before the incoming incident suggested it might not really be) ?
- *Failure Modes* : includes a list of failures of safety principles. Identify the 'pathogens' and analyse the system's vulnerability. What safety principle appears to be challenged? Apply a substitution test -what if I change the aircraft type, the crew, the airline, the airport,...- to assess the real extent of the failure.

- *Recovery Modes* : includes a list of the known recovery strategies, as well as known protections and defences against dangerous outcomes of failure modes.
- *Corrective Actions* : includes a list of corrective actions that could be taken ; a list of corrective actions that have been actually implemented, along with the rationale for their selection, and follow up action assessment strategies related to these corrective actions.

#### 4.3.3.3 All these four windows have a menu :

- *List* : displays the list of risk management strategies, failure modes, ... in the corresponding window
- *Edit* : allows for a modification of the list
- *Event* : gives access to individual event data sheet (link to the traditional data base layer)
- *References* : gives access to a list of relevant references that can justify or document each safety principles, the failure modes, the recovery modes, or the corrective actions. Gives hypertext access to the material itself from the list of references, either through local disk, through the organisation intranet, or through the internet.

References include but are not limited to the following

- as per safety principles : regulation, philosophy, company policy, procedures or even academic literature can be referred to ;
- as per failure modes : results from outside data bases, safety analyses, results of specific surveys, academic literature,...
- as per recovery modes : results from outside data bases, safety analyses, results of specific surveys, airmanship, academic literature,...
- as per corrective actions : identification of the authors of corrective action proposed (e.g. reporting crew, Training Department, Maintenance, Air Traffic Controllers , Accident Investigation Report Recommendations ..); identification of the decision maker for corrective action selection ; rationale for the decision ; similar actions taken in other organisations ;
- *Help* : gives access to the definition and content of the different windows, guidance material about safety concepts, as well as guidance material about the A-OIRAS functioning.

#### 4.3.4 Feeding the Risk Management Page

The first thing an analyst<sup>3</sup> should normally do when processing a new event report is to open the Risk Management Page and to match the event with an existing 'Risk Domain', and further, to a 'Precursor Family' in the corresponding sub-menu. If there is no apparent match, it may be necessary to create a new Risk Domain if the analyst thinks it is warranted. It is a feature of this A-OIRAS that new items can be added to the categories as the need arises. Matching an event with a Risk Domain and a Precursor Family will increment an event number counter, which will provide useful information concerning the ongoing updating of the prioritisation of the risk domains.

Alternately, upon reading the report, the analyst may decide to assign the report to a filing cabinet as being of no perceived interest (the report is minor, of no consequence, with nothing to be learned). The reporter would be acknowledged (it is important to encourage information from the operators) and the report would be kept for possible review at a later date. This then is the first "intelligent"

---

<sup>3</sup> In this section, we refer to 'analyst' as if it were one person. This is for convenience only. In Section 5, An Improved Safety Office, we describe the role that others in the organisation play in the analysis of the incidents.



decision to be made - an initial identification of the report in terms of its risk potential to the organisation, as identified by its proximity to the risk domains.

Once a report as been identified as belonging to a Risk Domain and a Precursor Family, it would be added to the Events list, thus being assigned a date, a reference number and a title. Although the Individual Event Page can be filled in at this step with the available data, it may be more efficient to do it later, while introducing the event into the various items of the Risk Management menu, which will suggest relevant questions and guide the event coding.

When the Risk Management menu has been opened there are four interactive windows, as described at the previous paragraph:

- Risk Management Strategy
- Failure Modes
- Recovery modes
- Corrective Actions

#### **4.3.5 Risk Management Strategies**

Within the Risk Management Strategy window, there are a list of stated protections. Creating this list for each Precursor Family is a way to explicate the safety model of the analyst (or organisation). The task is to consider all the ways in which such an event is *not* supposed to happen, all the features of the system that defend against such an occurrence. For example, in the case of runway incursions (seen as an Precursor Family arising from the Risk Domain of Ground Collisions) the following can be considered Risk Management Strategies or safety principles:

- Taxi navigation : crews (are supposed to) know where they are ;
- Runway visual protection : crews can see the runway limits, marked with standardised paintings, signs, lights,...
- ATC procedure : crews must receive a clearance before they can enter the active runway
- Phraseology : controllers will give clearances using standard phrases, messages will be read back, controllers will monitor the read back,...
- Crew visual monitoring : crews will check that final approach is clear
- Controllers monitoring : controllers will check aircraft movements visually, or with the assistance of ground surveillance radar,...

Creating that list for every Precursor Family of every Risk Domain may seem a tedious task. Actually, it will be created through an iterative process. A first draft can be developed from scratch, and then refined and complemented from the analysis of incoming events or the evolution of the safety thinking and regulation. This process makes it a living list, capitalising on the feed back information to better reflect the safety model. Furthermore, efforts could be shared between airlines, Authorities, and Manufacturers, as they should have most of the items in the list in common.

Each time a safety principle is felt to be relevant for the reported event, clicking on that item in the list would automatically create a link with that event through its identification number. Each item on this list acts as a summary, and includes a meter of the total number of related events. Clicking on that meter will activate the list of connected events (a subset of the Events Page). By clicking on each event, the Individual Event Page would appear. Here the details of the incident can be recorded, when the full analysis is known.

#### **4.3.6 Failure Modes**

In the next window, Failure Mode, there is a list of known and or potential failures. Obviously, as more events are reported, there will be more examples of failures, and an opportunity to expand the

list. Such lists also challenge the analyst's thinking. (I didn't think X could fail... but it did.) For the runway incursion example, the possible failures include:

- Taxi navigation failure
- Communication failure
- Wrong ATC clearance
- Runway limits not perceived
- ...

Again, each time a failure mode is felt to be relevant for the reported event, the analyst clicks on the relevant failure to create a link through the event identification number, or adds another to the list. Again, each item on this list acts as a summary and includes a meter. When clicked on, the meter will activate a list of connected events. And the details of any incident can be accessed by opening the corresponding Individual Event Page. Note that the same failures can appear in multiple risk domains, so this summary technique allows the analyst to draw together events based on the system's failures, not the actual event. In a sense, this gives the analyst more distance from the data by drawing him back from the "noise" of individual events and allowing him to perceive the more important pattern of failures.

### ***4.3.7 Recovery Modes***

The Recovery Mode window will also be an open list, to be expanded as more recovery techniques are reported. This list can also feed the Risk Management Strategy window. There may be protections in the systems, not originally listed, which emerge in the recovery process. The information from the front line operators can thus alert the organisation to its weakened defences, but also its hidden strengths. These three windows help develop a true picture of the organisation's defences and weaknesses. As one list informs the other, the potential for organisational learning increases.

As discussed in §3.2.4, the key issue is keeping control on deviations. The control on deviations includes :

- a permanent deviation management process : monitoring, self-monitoring, detection, prioritisation, correction of deviations (not all of them); the anticipation and/or recognition of abnormal (up to emergency) situations and their management
- and also a meta-management process: resource management, external and internal (cognitive compromise) risk management.

### ***4.3.8 Using the organisational level menu : organising the multi-layer communication***

The 'Level' menu operates in concert with the first three windows of the Risk Management Page (Risk Management Strategies, Failure Modes, Recovery Modes). It identifies the organisational level at which the strategy, failure and recovery operated. These levels are:

- Front Line Operator - individual and team
- Organisations (airline, ..) level
- Manufacturer
- Authority

An organisation will normally run its OIRAS at its corresponding level (e.g. an airline at the front line operator + airline level, a manufacturer at the manufacturer level, ...). The communication about safety issues between organisations, within a same level or between different levels, will be facilitated by the reference to the lists of strategy, failure and recovery modes at the different levels.

It is possible that the risk management strategy was envisaged at the airline level (aircraft design), and failed, and the recovery was at the front line level. There are hierarchical links between the lists at the different levels. Many principles in the 'lower' level lists are interpretations, implementations, instantiations of principles in the upper level lists. For example an airworthiness certification principle can be addressed at several levels :

- at the Authority level, its implementation will be monitored ; it will be assessed, and possibly amended ;
- at the Manufacturer level it will be interpreted (according to Authorities' Acceptable Means of Compliance and Manufacturer's philosophy) and incorporated into design ;
- at the airline level, it will be experienced

The Risk Management windows interface will allow the analyst to record these inter-level links as well. The hierarchy will be represented into the OIRAS through the '*Reference*' menu. Indeed, safety principles will be referenced, whenever relevant, to a 'father' principle. The genealogy of safety principles will therefore be immediately apparent on request . This will drive the communication process between airlines, manufacturers, and Authorities. In further steps, the hierarchical links could be categorised more rigorously (e.g. interpretation, implementation, instantiation,...) and automated inter-layer communication protocols could be developed.

Furthermore, to a large extent, the lists of strategy, failure and recovery modes at the different levels in the local OIRAS could be harmonised between organisations of a same level (e.g. airlines), or between organisations of different levels (airlines, manufacturers, Authorities) . This would create a real 'safety exchange language' facilitating information exchange within and between the different levels.

For example, a manufacturer can say to its customer airlines : 'one of our design safety assumptions is that a pilot will never fight against the auto-pilot action, but rather click it out in case of perceived 'odd' behaviour. We suspect it is not true in all circumstances. Could you please add this assumption to your list at the front line operator level and screen the corresponding failure (falsification) modes and recovery modes and keep us informed'. Then the airline may answer : 'will do ; we fully support your suspicion, as we have the opposite statement in our list...'

### **4.3.9 Corrective Actions**

Once the analyst has decided what happened (which safety principles were called into question by the failure and subsequent recovery activities), he must decide on the appropriate corrective action. The window for Corrective Actions is a fundamental component of this OIRAS, as it tracks and evaluates the organisational responses.

First, there is a sub-menu of potential corrective actions as proposed by front line operators, safety analysts, Training Department, Maintenance, and other departments. The authors of the proposal are traced through the 'References' menu. This list will expand with the organisation's experience, and again, it will also explicate the safety models of those who contribute "solutions". Different actors in the system will be able to see the bounds of their own thinking as reflected in the solutions that they propose (e.g., always suggesting training or more procedures as the answer).

From this list of potential actions, the action(s) actually taken will be noted in the database along with the person who decided on the action, the rationale for the decision, including a cost/benefit assessment, and the group(s) upon which the action must impact.

The corrective actions taken will impact the list of risk management strategies, and should be added to the list, even if only provisionally. Questions to ask:

- Does the (provisional) corrective action impact other risk management strategies?

- Does it invalidate previous strategies?
- If so, does it invalidate a safety assumption or principle?
- If so..... ?

Finally, there must be some tracking of the actions taken, to evaluate their effectiveness. An assessment strategy must be devised, *at the same time that the action is implemented*, to determine the criteria for success and the parameters of the evaluation. This step is missing from current OIRAS, which means that these systems have no way of evaluating their own effectiveness. When a safety tool is as expensive to maintain as this can be, it is poor science and poor business to omit an evaluation mechanism. Such a mechanism closes the feedback loop for the organisation, and allows it to really monitor its adaptive processes and learning strategies, and determine a clear direction for the future.

The assessment strategy identifies the signals of success or failure of the corrective action. Here some intelligent interaction with the database is required. It is possible to translate a hypothesis into keywords, combinations, and significant frequencies. A series of "if.. then.." statements can be created and applied to the data base on a recurring automated basis. These programmed hypotheses would act as 'red flags'. Time limits should also apply - when the strategy will be introduced, when it is expected to impact the system, and when will certain incident families be affected?

#### **4.4 Feeding the Individual Event data base**

Parameters of an event (aircraft, route, altitude, etc.) and the possible outcome of causal analysis are not recorded directly in the Risk Management Page, but in the Individual Event Pages.

The purpose of the study has not been to develop a new event data sheet, with a new causal model, a new set of keywords, etc. The focus of the study has been to develop the Risk Management Page, which acts by principle as an additional interface layer between the users and the traditional layers of incident data bases, which are accessed here through the Events Page and Trend Analysis Page. As a matter of fact, although this has not been explored deeply during this research, most existing incident data base formats could probably be adapted to interface with the Risk Management Page, including formats used in different domains (pilots, maintenance, ATM, ...).

Because the study started from the AIRS (BASIS) format, and because the BASIS format is increasingly accepted among airlines for incident record and analysis, Individual Event Pages and Trend Analysis capabilities have been assumed in this study to be those provided by the BASIS format. However, another globally accepted keyword structure such as ADREP 2000 could also allow maximum transference of material between interested parties.

Also, the structure has been designed as a branching network, such that varying levels of details and causal factor related to an event can be recorded and revisited if necessary. The objective data from the event is recorded and the information can be retrieved and complemented as necessary. Coding of the individual events for causes and explanatory factors can also be performed using the data base taxonomy and keywords. However, it is very time consuming, and is not recommended for the reasons provided earlier regarding bias. Furthermore, most of the relevant information regarding causes should have been extracted through the Risk Management window when analysing the failure modes and levels. Consequently, individual events causal analysis should be limited to the highest priority risk domains, and conducted with the guidance of the questions raised when using the Risk Management window.

## 4.5 The Report Form and the reporters

### 4.5.1 *The Event Report Form*

The report form was designed with several constraints or objectives in mind.

- Pilots are not writers, therefore we kept the form as short as possible - only two pages.
- Pilots are not sophisticated safety analysts, therefore we wrote the questions in simple, everyday language.
- We wanted to avoid leading questions as we have observed in other report forms. We chose non-directive questions (what happened? Why? How was it fixed? What should be done?) to allow the reporter to reference his own implicit model of safety.
- At the same time, we provide some prompts to encourage them to think more broadly about the system in their answer, to think about 'system failures' (how close were they to an accident), and to consider their error management strategies.
- The essential difference between an incident and an accident is the recovery process, therefore we made it the focus of one of the questions (detection and recovery).
- Finally, in keeping with the general philosophy of organisational learning, we included a question (who should be advised and what should be done?) to encourage the reporter to be part of the learning process. This question prompts the reporter to consider the safety lesson inherent in the report and how the organisation (and the aviation system) could benefit from it.
- To reinforce this thinking, the instructions for completing a report say:
  - "Report the event if you believe something can be done to avoid further or related occurrences; if other aviation professionals could learn from your story; or if you realised that the system and its protections were not as resistant as you thought".

These instructions define the reporting system and its purpose - to help avoid future occurrences, to share experience in the hope of educating others, and/or to alert the system to its true safety thresholds. Asking the right questions (open without being leading) can encourage the reporter to reflect on broader system issues as well as internal processes, inside and outside the cockpit (or work space). This is not to say that the reporters are ignorant. On the contrary, it recognises that the reporters are the only 'expert witnesses' present at the time of the incident. An educated witness, a thinking witness, will give a better (more comprehensive, less defensive) overall account of the event. An example report form is contained in Appendix A.

### 4.5.2 *Reporters - Pilots only?*

A problem with many reporting systems is that they focus on crew actions. Pilots are in a unique position to observe a great part of the system, and are therefore uniquely situated to comment on the system's health. Nonetheless an incident reporting system focused solely on pilots reinforces the idea that everything comes down to pilot error, even when other 'outside' influences are considered. If the reporting system was extended to include other departments, it would promote greater sharing of information and enhance a company-wide safety culture. It would also facilitate follow-up action within the company if all departments subscribed to an open system, and could exchange relevant reports. The potential for improvement throughout the whole system would be encouraged, rather than just focusing on pilots (where the potential for further improvement is perhaps the smallest). Pilots would be alleviated of their current roles as 'primary faulters' in a truly system-wide reporting system. Finally, given that pilots are usually perceived by other employees as privileged, it would not be fair to give pilots the opportunity to comment about other employees without also extending that opportunity to other employees (gate agents, flight attendants, ground personnel, maintenance).

The same, well-designed incident reporting form could be used in all departments.

## 5. An Improved Safety Office

### 5.1 Goals and Objectives

The goal of a Safety Office should be to promote and facilitate organisational (and global) learning about risk management and safety within the organisation.

To that end, there are several objectives:

- Co-ordinate and optimise different sources of safety monitoring (FOQA, OIRAS, operational audits and surveys).
- Evaluate costs and value of information obtained from the different sources
- Encourage and collect feedback (reports) from the operators
- Disseminate safety information to relevant others (internal and external to the airline)
- Maintain databases; make them accessible to relevant others
- Assist the local context experts with the causal and risk analyses
- Act as a clearinghouse for safety information
- Develop hypotheses based on clinical and trend analyses of the reports
- Assist other departments in the testing of hypotheses
- Assist other departments to develop corrective or adaptive interventions
- Publish and or otherwise communicate 'safety lessons' bulletins to operators
- Co-ordinate corrective actions to minimise redundancy
- Track and evaluate organisational responses
- Monitor the organisational learning

The personnel of the safety office may be most effective as *internal safety consultants* for the operational departments. Staff from the Safety Office are (or should be) relatively sophisticated thinkers about safety, but they know little of the daily operational context. Staff from the operational departments have the reverse competencies - not sophisticated safety analysts but very much aware of the full operational context. It is the operational people who will be able to 'read' a report and sense the nuances and contradictions.

The Safety Office can be most helpful by:

- guiding the analysis process for the operational staff,
- suggesting different ways to interpret the data (eg., ecological, systemic, error management),
- helping to generate hypotheses regarding failure modes and risk management strategies
- formulating the means of testing the hypotheses,
- suggesting different corrective actions
- helping to track those actions in the system.

### 5.2 Data Flow

Every incoming report should be analysed on a case by case basis. This can be done in several ways. An individual can be responsible for all the analyses (this may be the default in small companies); an individual can be responsible for the preliminary reading of the report and distribution to relevant

operational parties; or an operational team composed of individuals from different departments can meet on a regular basis to examine the reports. This last model is especially useful for complex cases which involve more than one department.

The most cost-efficient and effective method may be a combination of all three. An individual can be responsible for reading reports as they come in and then decide who should see them. When the case is relatively straightforward, eg. the responsibility of one fleet or one department only, the person can send the report to the relevant party, asking to be given feedback on the action taken. When a case is more complex, it can be assigned to a meeting of the relevant cross-departmental parties. The person who is acting as a first filter of the reports should also be the person who follows up on the action taken, and records the outcomes in the 'corrective actions' category of the data base.

The outcome of the case by case analyses can be fourfold. The first is reactive and simple, the second is a little more proactive but still relatively simple, and the third and fourth are proactive at a more systemic level.

1. A very straightforward and minor course of action, some remedial activity to correct a lapse in the system's defences as they are understood, and share the information with relevant parties;
2. A safety lesson, relatively straightforward, in that the action required seems relatively obvious. It may be to investigate a particular feature of the system in more depth as a potential problem, and share the information with relevant parties.
3. A safety doubt, which generates a testable hypothesis, and which can be answered by a proactive probe of the system. The benefit of this approach over the previous 'keywords search' of the incident database is that there is a systematic enquiry (rather than relying on incomplete, biased reports). For example, if the doubt concerns a particular route or airport or aircraft, then the question to be answered can be included with the flight papers for pilots flying that route, airport or aircraft for a trial investigation period.
4. A safety challenge. Here the course of action is not clear. The analysis guidelines should help the analyst identify a concern that is not so easily understood and can not be so easily 'fixed' (e.g. an unexpected failure bringing a risk management strategy into serious doubt). Such a challenge will be more systemic and require greater knowledge and understanding of the system. This challenge should raise a flag of anxiety (experienced at varying levels of intensity) about the system and should lead to the development of testable hypotheses (at best) or nagging hunches (that are remembered by the system for later consideration).

### **5.3 Tracking Organisational Learning: A new focus**

Current OIRAS purportedly use trend analysis to establish the effectiveness of their interventions. The absence of similar incidents in the future is considered evidence that the intervention was successful. Quite apart from the flaws in current database structures, there is a deeper, more systemic complaint with this approach.

Incidents as single events can only be considered symptoms of a system's ill-health. An intervention to prevent one type of incident may be successful in removing those incidents, but at the same time it may be responsible for creating another type of problem. (Automation is the most common example - reducing the likelihood of error in one area of flight has created new problems around complacency and ignorance of complex systems.) The disappearance of one type of incident does not guarantee an overall improvement in the system. Therefore we suggest a refocusing away from events and causal attributions toward events and organisational responses.

In such a system, the central analyst is responsible for creating a living document of organisational responses to the operators' reports. The proposed data base would record the corrective action (organisational response), cross-referenced with the report.

Periodic meetings should be arranged in order to review the actions taken.

- These meetings would serve the purpose of presenting summary response data, allowing for higher-order analyses and the detection of recurring themes.
- These summaries would highlight the range of strategies that have been tried, thereby revealing the implicit safety models on which these actions were predicated.
- Recurring themes might indicate the failure of a remedial action (a recurrence of the same strategy would indicate its partial or total failure to address the problem).
- Patterns may also emerge that are detectable only with greater distance from the data, allowing for clearer systemic thinking (e.g., one solution may be effective locally, but causing a problem elsewhere in the system).

The important distinction here is that the analysis review team is *not looking at a summary of incidents or reportable events, but rather the organisational response to perceived safety problems*. In other words, the review team is evaluating the effectiveness of the organisational learning. The questions the review team can ask are:

- Are we repeating our interventions?
- If so, does this mean they are ineffective?
- Perhaps the solution is not to do more of the same, eg., more training, more procedures, but to look for a radically different approach.
- Is there more to be learned from the response data? (There can be higher order analyses which lead to systemic interventions, rather than isolated reactions.)
- There may be more efficient strategies that are not counter-productive to each other, which only some distance from the data could reveal. Viewing the responses and their effectiveness can help the team decide on future action by generating hypotheses about what is failing and what might work.

## 5.4 Information dissemination

It is the task of the Safety Office to co-operate with other airlines and outside agencies in the global search for improvements. The topic and timing of notification to outside organisations should be linked to the perceived severity of the breach of the risk management monitoring process. For those incidents determined by the analyst to be 'very high risk', the relevant party should be notified immediately (e.g. less than 24 hours). For all other incidents, the analyst may prefer to wait for X other similar reports before notifying the relevant party. (Single incidents, unless very serious, attract little attention. But a series of medium-threat incidents all marked for the manufacturer or the regulator would make a more impressive statement). It may be possible to program the software to recognise when two (three or x) instances of the same category are listed, as a way to prompt the analyst that a pattern of similarly risk-rated incidents are developing about which the appropriate party should be notified. The actual number of reports will depend on the size of the airline and the general frequency of incidents.

The alternative is to generate quarterly reports for distribution to the relevant parties. This method is recommended as the base system to ensure a routinised system of review and notification. Only those reports of sufficient severity or frequency would need to be sent more than quarterly, and even these should be supplemented by an automated report summary every quarter. Such an approach - quarterly summaries - will further reduce the data into meaningful categories to be sent from one analyst to another (in other departments or agencies). The adaptive lists feature will allow the analyst to detect significant patterns based on risk domains, precursor family, failure modes, etc., and the party(s) to be



notified. Quarterly reports can subsequently be summarised and reviewed as half-yearly and yearly reports. The issue here is the ability to detect trends across time using a systematic but time efficient process. Reports can be generated automatically, providing the relevant parties with a summary of the information, with the possibility of providing further information if requested. All agencies could then work efficiently to seek out trends and develop hypotheses about the system's safety.

Below is a simple but time efficient summary form for use by an airline.

<p>During the quarter _ to _, X events were filed with this office. Of those, Y events were identified as being of relevance to your area.</p> <p>The attached printout (automatically generated by selecting the right categories from the data base) provides you with the following information:</p> <ul style="list-style-type: none"><li>• A short description of the incident</li><li>• Precursor Family</li><li>• Risk Domain</li><li>• Failure modes</li><li>• Corrective action</li><li>• Any other agencies that were notified about this incident</li></ul> <p>I trust this information will be useful for your safety analyses. A more detailed report can be provided upon request. I would appreciate any feedback relevant to my organisation.</p>
---

This protocol was written with an airline pilot co-ordinator in mind. A similar report could also be designed for other agencies, eg., for the manufacturer to report to the Authority; for the Authority to report back to the airline, etc. Analysts' reports become inputs for other analysts in a multi-layer communication strata. The shared concepts will be the safety principles, the failure modes, the recovery modes. Useful information will be transmitted when a lesson learned at one level (e.g. this safety assumption- *e.g. maintenance technicians will read the procedure in the book every time before acting*- has been challenged in 80% of related incidents during last month, which is three times more than usual) can be transferred to the next level (e.g. this suggests that there may be a barrier to reading that procedure incorporated into its design or presentation). The system will work more efficiently when relevant information is shared between agencies. Again, the primary goal is to *reduce the quantity of data* being passed to others into meaningful, interpretable data that allow for trend analysis in a system that is not sure where those trends might be found.

## 6. Training Requirements

A successful OIRAS is dependent upon two major elements: getting quality information from the operators, and deriving quality information from the database. Training is suggested to address these two needs.

The qualities that make a person a credible and trustworthy confidante to his peers (and thereby selected or elected to the post of OIRAS co-ordinator) may also be the same qualities that will allow him to network successfully with Management and other departments throughout the company, as well as interview reporters about an event. These qualities, while highly favourable, are not sufficient. Co-ordinators will also be Project Managers, with resources and a budget to manage (essential to an ongoing OIRAS system). They will also need ongoing education in current safety theories and trends to broaden their perspective when considering an incident or developing hypotheses about the safety of the system. Finally, along with education in Human Factors, system co-ordinators would benefit from some education in scientific data analysis (qualitative and quantitative analysis, and data base management), to enable them to interact intelligently with the data base.

Training is envisaged as requiring at least two sessions. The first focuses on the practical issues surrounding implementation of an OIRAS in an airline; the second addresses safety analysis in more detail. We believe the first phase, establishing a credible system, is essential because experience of the last few years has shown that many airlines fail to make adequate preparations for a OIRAS. Consequently, the more theoretical work regarding analyses is relegated to the second phase, when the co-ordinator has a system in place and has begun receiving reports. The two phases can be understood as "getting quality information into an OIRAS" and "getting quality information out of an OIRAS".

These courses could be provided by the Authority to airline personnel to encourage the standardised transmittal of information to them, or as a general service to the industry.

### 6.1 Phase I: Generating quality information in OIRAS

The following is proposed as a basis for a typical four day course for Co-ordinators to meet the needs of Phase I.

#### 6.1.1 Course objectives

At the end of the course attendees will have the knowledge, skills and tools to be able to implement and maintain a OIRAS system within their airline. As OIRAS project managers, they will be able to:

- persuade peers and management of the value of an OIRAS,
- enlist support and resources for an OIRAS
- use the OIRAS system and software to analyse and encode incident reports
- maintain an active data base of incidents
- report and share the information learning (feed back and feed forward to the relevant parties)

#### 6.1.2 Course Outline

##### 1. Introduction

- Check in and get everyone's background and expectations for the course.

- Tell them that at the end of the course, everyone will present their "what I'm going to do to implement and maintain an OIRAS in my airline" checklist of activities, (the checklist to begin as soon as they return to their airline).
- Show them some report forms, and the OIRAS software installed on computers (to stimulate their curiosity)
- Explain the one constraint - learning the OIRAS software program (be realistic about the work in the course)
- Explain the style of the course as being some lecture-based, but mainly experiential with practical exercises designed to help participants brainstorm ideas for their airline. Emphasise the pragmatic aspects of the course.

## **2. Selling the concept**

*[lecture]*

This will be a presentation designed to show the value of OIRAS for enhancing safety. It will discuss the evolution of Human Factors in aviation up to the present time, and it will revolve around the idea that individuals and organisations can learn from error, hence the value of confidential reporting systems as tools for organisational learning.

This presentation will be their first "tool" to take back to their airline - it will be given to them in electronic and paper form with hidden commentary accompanying the slides. Each participant can adapt it for use in their airline, when they want to persuade peers, other departments, and or management of the value of an OIRAS program.

## **3. Barriers to Implementation**

*[group exercise]*

Following straight on from the presentation, they will do an activity in groups (or by airline depending on participant numbers). "If an OIRAS is such a good idea, as suggested by the preceding presentation, then why is it going to be difficult to implement?" Ask them to think in general terms (about commercial aviation) and more specifically (about the prevailing conditions and attitudes in their airline.) Ask them to imagine all the opposition they may encounter when they return to their airline. The more comprehensive and extreme the list, the more prepared they will be for any opposition.

## **4. What do I need to make it work in my airline?**

*[group exercise]*

Encourage them to start thinking of themselves as Project Managers. This can be a brainstorming session where they list everything (all the knowledge, skills, support and resources) that they will need to overcome the barriers listed above and successfully implement their project, an OIRAS. This should cover the theoretical issues as well as the small and practical details. Help them by signposting the different steps in the process and highlighting the underlying issues (trust and credibility in convincing peers they will not be punished, convincing Management that people should not be punished, designing a form, distributing and collecting forms, knowing how to analyse the form, and knowing how to extract and disseminate the important lessons for the organisation).

## **5. Reporting an incident**

*[individual exercise]*

Begin by asking everyone to write down an incident from their past as either instigator or co-pilot, which they will share with others in the group. Someone is likely to ask "what sort of incident do you want me to describe?" which should prompt a group discussion of what is an incident and what sort of events should be reported. The purpose of OIRAS can be revisited, highlighting that events should be reported that provide the potential for organisational learning and safety improvements.

Once they have all written something, distribute existing airline report forms, and ask them to repeat the exercise, this time answering the items on the form rather than the unstructured narrative. Then discuss and debrief the benefits and drawbacks of the 2 styles of forms (e.g., structured form elicits more information). Tell them they will be designing their own questionnaires later, when they have some more information about the type of data they will need. Hint at the confidential/anonymous distinction and the need for standard phraseology.

## **6. The need for databases**

*[lecture, video and hands-on]*

They should have computers in front of them to 'feel' this session. Discuss the need for an event data base (to get information in and out easily, to store data, to compile reports, etc.) and the need for standard phraseology.

In order to understand the database categories, the participants must have some knowledge of Human Factors, in particular the systemic and ecological approaches to understanding safety. Show an accident video. Ask them to watch the video and consider all the influences.

Debrief the video by highlighting the broad scope of the investigation. Discuss all the influences, the time period, from the immediate event back in time and away from the accident site. Introduce Reason's model and highlight the idea of failures. Discuss the adaptive features of the system. Point them to added readings in their manuals; stress the complexity of understanding an incident/accident; acknowledge they won't mount a full-scale investigation every time, but that the definition of "relevant information" is much broader than what happened in the cockpit. Remind them - the 2 essential principles to grasp are "learning from error" and the systemic and ecological approaches to safety.

## **8. Database 1**

*[lecture and hands-on]*

Start with Incident families and Risk domains. Explain the terms by going through the manual definitions with them, asking for examples when they can think of them. Distribute 2 incident reports and ask them to code them.

Once they have agreed on the appropriate categories, help them enter the report in the computer system. Walk them through the steps of starting the program, entering the report, and putting some keywords in place. Encourage curiosity with the data base at this point, and answer any questions regarding the system and its basic operation. It will help them to be confident with the system before they have to tackle some of the more difficult keywords.

## **9. Implementing an OIRAS I - Creating the system, getting the reports**

*[group exercise]*

The first of 3 sessions, this session addresses the first phase in the Project - promoting the system, building trust and credibility, getting reports, and getting them into a data base. Participants will start to work on their Implementation Checklists. Depending on the group, you can present or brainstorm the roles and responsibilities of the OIRAS Co-ordinator. The facilitator may only need to ask questions to keep the participants thinking of all the details, and the order in which they will approach them (getting the physical resources first? Network with other departments? Promote in the local publication? Decide the questionnaire items? Where to put the forms? Where they can be returned? Who's going to help me?!) This is meant to be a lively session addressing very pragmatic issues, prompting the participants to think and rethink all the steps at deeper and more detailed levels. All these activities go on the Implementation Checklist.

## **10. Database 2**

*[lecture and hands-on]*

Using the same format as above, explain the Risk Management Strategies and Recovery and Failure Modes. Revisit the 2 incidents which were coded earlier, and code them for the new categories. Update the software. Add 2 new incidents; ask them to code them, and enter them into the system. They should be very familiar with the software by now and be able to concentrate more on the corrective action.

### **11. Call-backs**

*[Exercises]*

Stress the need for relevant information in order to understand the scenario. Draw attention to the different weaknesses in reports (bias, incomplete, defensive). Stress the need for objectivity, no assumptions.

If not already discussed, highlight the benefit of confidential versus anonymous reports. Distribute incident reports that are evasive/biased or poorly detailed. Get them to brainstorm what information they will need, and from whom (may be people other than the pilots). They can review the incident reports already analysed and decide if these reports need more information also.

Though it may make some participants uncomfortable, role-playing would be useful here. They won't realise until they try it just how difficult it is to be neutral and inquiring rather than invasive and judgmental. They also have to develop some intuition about which reports would benefit from more probing and which do not. There is a basic issue of resources spent for information gained to be considered.

### **12. Database 3**

*[lecture and hands-on]*

Same format as above. Explain the Corrective Actions Categories, and emphasise the role of organisational learning. Revisit the 4 partially completely incidents and finish the analyses. Further incident reports can be given as "homework" if requested.

With all the categories and basic software mastered, they have acquired the first level of skills.

### **13. Implementing OIRAS III - It's only as good as the learning that occurs**

*[lecture and discussion]*

The most credible system and the best analysis is pointless without the follow-through. Time to discuss feedback to the crews and feed-forward to the organisation and other interested parties (manufacturer, other airlines, regulators, ATC). Discuss different types of reports, who should see and/or act on the information. Raise the issue of an operational action team within the airline. As Project Manager, they will have to demonstrate the worth of an OIRAS. Some early success will help the project, especially if the action taken is shared with all interested parties within the airline, and real change is effected.

We need to acknowledge here that these participants can not be sophisticated analysts in 4 days. It is our belief that they will come to realise "what they don't know" about Human Factors and incident analysis only through some hands-on experience with a growing data base. Rather than overwhelm them with theory which appears unrelated to their experience, we believe it is better to give them the basics, stress the goals and objectives of OIRAS, and allow them to do some learning and discovering on their own. They may start to go to safety conferences; they may start to network with other analysts. All of these activities should be encouraged. Items about how to stay informed and update their knowledge can be added to their Implementation checklists.

### **14. Presentations of the Implementation Checklists**

*[exercise]*

Revisit the "barriers to implementation" and "what do I need?" exercises to set the stage. Give class time for this; stress the more prepared they are when they return, the less they will be affected by

initial disappointment and setbacks. Anticipation and preparation will be key to a realistic implementation strategy and an early success.

Every person (or airline group) then presents their checklist. Others in the group can offer suggestions. By the time everyone has presented and shared their strategies, the group will have a very thorough, comprehensive checklist.

### **15. Conclusion**

Check in with them that they feel prepared to start the implementation process. Be sure to have all contact names and numbers ready for distribution. The list to include the Authority personnel, the other course participants, and previous participants if possible. Also a list of recommended reading material and website addresses.

Remind them that incident analysis is a skill which they will improve with practice and more learning. A final reminder: The purpose of any incident reporting system is to promote organisational learning, reduce safety threats, and improve safety.

Wish them well.

## **6.2 Phase II: Extracting quality information from OIRAS**

After Co-ordinators have had some field experience with an OIRAS, i.e., the project has been successfully implemented and reports are being received, they are ready for the next phase of training. With reports in hand, they can undergo the necessary training to develop their analytic skills.

### **6.2.1 Course objectives**

At the end of the course attendees will have the knowledge, skills and tools to be able to extract the maximum organisational learning from the OIRAS data base. As OIRAS analysts, they will be able to:

- use the OIRAS software to analyse and encode reports
- maintain an active data base of incident families and risk domains
- interact *intelligently* with the data base
- develop hypotheses based on individual and multiple events
- facilitate the testing of those hypotheses by relevant parties inside and outside the organisation
- act as a clearinghouse and communication channel for safety information
- keep a record of organisational responses
- evaluate the effectiveness of those responses

### **6.2.2 Course Outline**

This course has not been blocked in the same detail as the first course. Essentially, it will revisit the first course, and address theoretical and data base management issues in more detail. More complex case studies will be provided, and greater emphasis will be placed on communicating the results and evaluating the organisational learning.

The following topics would be covered:

- HF theory - safety through invariance and safety through adaptation
- Mental representation and Risk management monitoring
- OIRAS as organisational learning, not mini-accident investigation
- Data base management

- Hypothesis development
- Setting up organisational experiments to test hypotheses (surveys, audits)
- Extracting summary statistics
- Communicating results within the airline
- Sending information outside the airline
- Deciding the resources to be allocated to investigations
- Understanding/recognising/extracting the lesson
- The value of 'context' and inside expertise
- How to monitor and evaluate organisational responses
- Where to go for guidance (networking)

## 7. Conclusion

Acknowledging the need for a better understanding of the information that incidents can provide and how to process it, the Direction Générale de l'Aviation Civile (DGAC) funded a research study aimed at developing a methodology for Operational Incident Reporting & Analysis Systems (OIRAS). A thorough review of current operational reporting systems highlighted their limitations and constraints with regards to biased unmanageable data bases and ineffectual trend analyses, and led to the conclusion that it was not enough to simply modify error taxonomies and keywords or revise incident reporting forms. A totally different approach was needed if implicit safety models were to be surfaced, challenged and adapted. The goal of this A-OIRAS is to promote and evaluate focused organisational learning about safety-related issues.

It should be apparent from the space given the description of the Risk Management Page that we are attempting to shift the emphasis in OIRAS. To resurface an earlier metaphor, the incident reports themselves may or may not contain traces of gold. Rather than keep all the mud, as most OIRAS currently do, we are strongly suggesting an intelligent, directed filter be applied to sift out and retain the value within. This system recognises that the truly significant feature(s) of an event may only be known in hindsight, and can not be captured by predetermined keywords.

Therefore the menus, windows and sub-menus of the Risk Management Page have been designed to explicate valuable safety information. They feed each other with updating information. In line with the ecological paradigm of complex, self-referential, adaptive systems, this OIRAS contains several loops for providing feedback from one element to another. As the system matures and evolves, previously implicit safety models can be explicated, challenged, and adapted as necessary. The organisation can also learn more efficiently by monitoring and evaluating its corrective actions.

The explication of implicit safety models at different levels will also progressively create a 'safety exchange language', allowing different aviation organisations (manufacturer, Authority, airlines) to discuss safety issues from their relevant role.

To conclude, we believe that the proposed A-OIRAS can improve current safety analysis, both conceptually *and* pragmatically. To use this model, safety principles must be articulated, therefore they can be challenged, modified and updated. At the same time, the focused search for information using the sifting filter of the risk management pages will save time and money as risk-relevant trends will be more quickly and systematically detected.

\*\*\*\*\*



## **8. Appendix A. Confidential Report Form**



<p><b>WHY DID IT HAPPEN?</b> (Describe the failure(s) that allowed the incident to progress as far as it did, e.g., technical; no, wrong or poor training; no, wrong or poor procedures; regulations, crew coordination).</p>
<p><b>HOW WAS IT FIXED?</b> (Describe the steps you took, from detecting the problem up to the point when the flight was back under control. List any help you received.)</p>
<p><b>YOUR SAFETY RECOMMENDATIONS:</b> In your opinion, who should be advised about this, and what should be done? (The pilots of this fleet, The Chief Pilot, All pilots in the company, Instructors/Trainers, Line Management, Safety Office, Standards, Maintenance, Ground Ops, Cabin Crew, other airlines flying similar routes, manufacturer, ATC, airport authority, Regulators)</p>