

# **Operational Risk Management System for SMS and FRMS**

S. Stewart, F. Koornneef, R. Akselsson

EARLY DRAFT of HILAS Book Chapter

<b>Table of contents</b>	<b>PAGE</b>
<b>1.0 INTRODUCTION.....</b>	<b>3</b>
1.1 ICAO MODEL OF A SAFETY MANAGEMENT SYSTEM (SMS) .....	5
1.2 SMS PROCESSES .....	6
1.3 WHAT ARE THE CONSIDERATIONS FOR IMPLEMENTING AN SMS? .....	6
1.4 THE ROLE OF HILAS IN RISK AND SAFETY MANAGEMENT.....	9
1.5 SYSTEMIC RISK.....	9
<b>2.0 EASYJET-HILAS SYSTEMS INTEGRATED RISK ASSESSMENT MODEL     (SIRA) .....</b>	<b>18</b>
<b>3.0 SUMMARY .....</b>	<b>34</b>
<b>REFERENCES.....</b>	<b>36</b>

## 1.0 Introduction

Safety and reliability of High Reliability Organisations requires the detection, measurement and evaluation of risks to the safe functioning of system component processes. Safety management is the process through which an airline is capable of delivering safe, reliable and predictable performance within prescribed criteria. It involves a systematic and integrated approach to risk management in flight, ground and engineering areas. The setting of acceptable safety criteria provides a measure for the determination of a system risk boundary. This process can be supported through the establishment of a Safety Management System (SMS) framework based on scientific evidenced-based toolsets. The focus of the SMS activity is to maintain airline operational readiness to meet risk and change as well as supporting continuous systemic improvement.

Airlines tend to have Safety Management Systems that are primarily reactive: that is, they respond after incidents have occurred. Reactive analysis of past events provides useful information on how and why an event took place (in order to understand how to prevent re-occurrence), but it is a limited source of evidence of overall system performance. The ICAO approach to risk management is essentially a technical model based on an engineering process viewpoint and is more applicable in concept to stable systems, such as chemical and nuclear industries. If airlines are to manage fatigue-related risks and other risks in a proactive manner they need to apply risk detection tools that provide real time and continuous systems oversight.

This chapter describes a systems approach applied to the development and implementation of a dynamic Safety Management System (SMS) in a major airline in Europe with a focus on management of Fatigue-related Risks. This work has been realised as a part of the in the EU Commission HILAS project. The SMS comprises both Risk Management System (RMS) and a Safety Assurance processes and the SMS working group adhered to the principles of Organisational Learning (Argyris & Schön (1974), Koornneef (2004)) and Resilient Safety Culture (Reason (1997; 2008), Weick & Suttcliffe (2007), Akselsson et al (2009)) in the development of the HILAS RMS. As a result, the RMS is conceived as an aspect system with functions, actors, supporting processes and connecting data streams. The RMS is supported by an Investigation Process (Chapter x, Stewart et al, 2009) that is invoked by the RMS when needed. The Investigation Process may trigger a 'culpability' process to elicit sensitive operational information from operators who have acted in violation with rules. Selection from options is supported by Decision Making processes through which interests between different stakeholders is being balanced and the acceptance of choices is mutual.

The key issues in the airline's SMS will be discussed in more detail in this and subsequent chapters inclusive of:

## Operational Risk Management System for SMS and FRMS

- a) A safety Sensory Network with data streaming in for reactive / proactive learning into the Aviation Quality Database<sup>1</sup> (AQD) and initially reviewed by a competent Safety Data Team
- b) A dynamic Risk Management System (RMS) process where a range of safety toolsets (Audits, safety reports, investigations, safety performance indicators, Flight Data Monitoring) that form part of a multilayer framework delivering safety trigger signals based on risk logics supporting proactive, exploratory as well as reactive and evaluatory capabilities.
- c) The role of the investigator supported by analytical investigation tools (or toolset) and data management and confidentiality determines root cause and contributory factors and makes recommendations from the assessment of risk (refer chapter x, Stewart et al, 2009).
- d) The processing of safety signals (weak and strong) filtered from the background system noise so that limited risk investigation resource and analytical capability can be directed at risk analysis and systemic evaluation of these signals.
- e) A Just Culture Management Protocol that governs the 'culpability' process to enhance intra-organisational learning and for which the notion of Resilient Safety Culture becomes very relevant and concrete (refer chapter x & x, Akselsson et al, 2009 & Stewart et al, 2009).
- f) The concept that establishes the role of organisational learning in risk investigation and risk management activity. Where learning exists, in order to restore system functioning as usual (or proactively to change in order to stay in business) to maintain system viability. Learning needs to be an organised process in the Safety Management System (consisting of RMS and Safety Assurance) (refer Chapter X, Koornneef et al, 2009).
- g) The development of a fatigue-related risk management model that draws from the HILAS Risk Management System concept. This performance model forms the basic framework for the implementation of an operational airline Fatigue Risk Management System (FRMS) (Stewart et al, 2009 HILAS Chapter x)

The principled development and implementation of the SMS has also led to the development of risk data sharing processes between the airline and a main service provider, allowing inter-organisational learning, amplification of weak risk signals and faster risk communication between different players in the sector (Chapter x, Stewart et al, 2009)

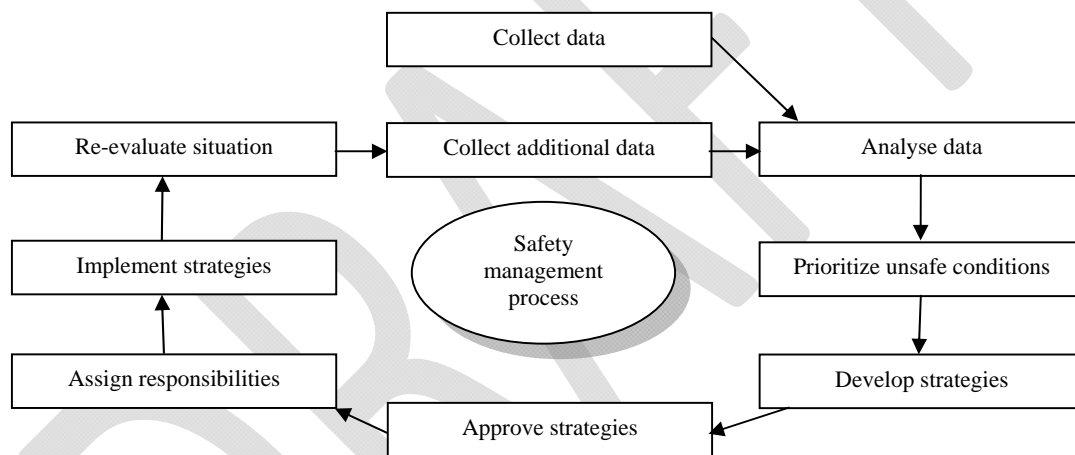
The work in progress demonstrates that integrating humans in processes of risk management leads to bridging domains of expertise and improved control of business as well as safety risks. We will begin by reviewing the ICAO SMS framework and the role of HILAS supporting innovation toward next generation SMS capability.

---

<sup>1</sup> AQD is an integrated safety and quality management system, covering functions from hazard identification, accident/incident reporting, analysis and investigation tracking through to auditing and corrective action tracking. It has been developed by aviation software specialists and has been used for over 20 years by regulatory authorities, airlines and other aviation related organisations

## 1.1 ICAO Model of a Safety Management System (SMS)

The ICAO Model of a Safety Management System (figure 1) outlines a number of coordinated process steps that form a safety cycle. The first step in the process is the collection of relevant safety data in the system concerning equipment, procedures, and humans etc to identify latent conditions. The data is analysed both qualitatively and quantitatively in order to identify safety hazards, their likelihood of occurrence and their effect. Using risk assessment, the unsafe conditions are prioritised according to seriousness and are then managed by developing appropriate strategies of e.g. elimination and mitigation. The strategies are approved by the management level in order to proceed to the next step in the safety management process of assigning responsibilities of action, allocate resources etc, and to implement strategies of action. To close the improvement cycle or loop, a re-evaluation of the safety situation is required to check the effectiveness of implementation and to check if new problems may have been introduced. This may need new information being collected and a new iteration in the safety management process.



**Figure 1.** Safety management process (from ICAO Doc 9859, 2008).

Safety and reliability of this system requires the detection, measurement and evaluation of risks to the safe functioning of system component processes. Safety management is the process through which an airline is capable of delivering safe, reliable and predictable performance within prescribed criteria. It involves a systematic and integrated approach to risk management in flight, ground and engineering areas. The setting of acceptable safety criteria provides a measure for the determination of a system risk boundary. This process can be supported through the establishment of a Safety Management System (SMS) framework based on scientific evidenced based toolsets supported by senior management and based on a ‘non-punitive’ Just safety culture that oils the functioning of the integrated processes. This program facilitates evidenced based change management where the decision making process of the management group is supported by a detailed understanding of system processes and operational risk influences. The SMS is

## Operational Risk Management System for SMS and FRMS

constructed around the company safety policy and is an essential element of the company business plan.

Definition of a Safety Management System: “A dynamic risk management system based on quality management system principles in a structure scaled appropriately to the operational risk, applied in a safety culture environment” (Stolzier et al, 2008 p19).

### **1.2 SMS processes**

States shall require a SMS from service providers that are exposed to safety risks. In the Annexes to the ICAO SMS document it is also established that the SMS shall be accepted by the state. The SMS shall, as a minimum (ICAO, 2008):

- identify safety hazards;
- ensure the implementation of remedial action necessary to maintain agreed safety performance;
- provide for continuous monitoring and regular assessment of the safety performance; and
- aim at a continuous improvement of the overall performance of the safety management system.

These minimum requirements are in fact essential processes in managing safety and found under headings such as; Safety risk management, Safety assurance and Safety promotion in the framework below. The four main components of a full SMS are identified by ICAO to be:

#### **1. Safety policy and objectives**

- 1.1. Management commitment and responsibility
- 1.2. Safety accountabilities
- 1.3. Appointment of key safety personnel
- 1.4. Coordination of emergency response planning
- 1.5. SMS documentation (most important is the SMS Manual (SMSM))

#### **2. Safety risk management**

- 2.1. Hazard identification
- 2.2. Risk assessment and mitigation

#### **3. Safety assurance**

- 3.1. Safety performance monitoring and measurement
- 3.2. The management of change
- 3.3. Continuous improvement of the SMS

#### **4. Safety promotion**

- 4.1. Training and education
- 4.2. Safety communication

### **1.3 What are the considerations for implementing an SMS?**

1. Planning of a safety management system

## Operational Risk Management System for SMS and FRMS

Safety management begins with careful planning. Existing procedures for investigation of incidents, hazard identification, safety monitoring, etc, should be reviewed and maybe modified for inclusion in the SMS. Appoint key line managers and a person designated as the organisation's safety manager to conduct the planning phase.

### 2. Application of scientifically-based risk management methods

Care has to be taken when selecting a risk management strategy in order to avoid introducing new risks.

### 3. Senior management's commitment to the management of safety

Flin (2003) concludes that one of the major factors in the managing of an organisation's safety is the degree of management commitment to safety and how the workforce perceives it. O'Toole (2002) concludes that there is a relation between the management's leadership and approach to safety, the employees' perception of safety management, and accident/injury rates. Thompson et al. (1998) found that the management plays an important role in promoting a safe workplace, but that managers and supervisors do so in different ways. Managers influence safety (indirectly) by affecting the politics of communication (or the work climate), and supervisors influence (directly) by the fairness by which they interact with employees. Rundmo and Hale (2003) analysed the relations between managers' safety attitudes, behavioural intentions and their self-reported behaviour. They found that safety attitudes might be an important causal factor for managers' behavioural intentions and behaviour. What seemed to be ideal attitudes for managers to display were high management safety commitment, low fatalism, low tolerance of rule violations, high worry and emotion, low powerlessness, high safety priority, high mastery and high risk awareness (Rundmo and Hale, 2003).

### 4. Safety culture

A corporate safety culture that fosters safe practices, encourages safety communications and actively manages safety with the same attention to results as financial management.

### 5. Hazard identification and risk management

Hazard identification programmes are vital for the systematic identification of hazards that can affect the operative work in an organisation. Through risk management, criteria are established for assessing and thereafter eliminating or mitigating risks.

### 6. A non-punitive environment to foster effective incident and hazard reporting

Reason (1997) suggests that a safety culture is an informed culture where fear is minimized generating good reporting of incidents, and where the organisation has updated knowledge about human, technological, organisational and environmental factors that determine the safety in the system or organisation.

### 7. System to collect, analyse and share safety-related data arising from normal operations

Learning is a process of deliberate questioning of the adequacy of current practice and of continuously and systematically searching for deficiencies and vulnerabilities in the organisation. Organisations with 'good' safety management have mechanisms in place to gather safety-related information, measure safety performance, and bring people together to learn how to work more safely.

## Operational Risk Management System for SMS and FRMS

8. Competent investigation of accidents and serious incidents identifying systemic safety deficiencies (rather than just targets for blame)

9. Effective implementation of standard operating procedures (SOPs), including the use of checklists and briefings

10. Integration of safety training (including Human Factors) for operational personnel

An example of the importance of safety training is from a study at the Swedish air traffic control organisation (Ek, Akselsson, Arvidsson and Johansson, 2007). The study revealed that large groups (both air traffic controllers and administrators) at all three study locations thought that they had not received enough training in how the communication should function in emergency situations. A similar result was found in Hilburn and Flynn (2001), where over 70% of air traffic controllers reported needing more training in unusual situations, such as handling emergencies. In principle, such results can be interpreted in different ways, e.g. that the training is clearly insufficient, that the respondents' ambition concerning safety is very high, or a combination of both factors. Hilburn and Flynn (2001) concluded in their study that a lesson learnt was that training opportunities seem to serve a dual purpose: they educate the ultimate users of the system, but they also send a signal to the staff that the management is willing to invest in them.

11. Sharing safety lessons learned and best practices through the active exchange of safety information (among companies and States)

Two characteristics that can be found in successful reporting systems are the application of quick feedback to the reporter and the compilation of incident reports. These compilations are sent to organisations within and outside the company, describing safety measures taken and forwards improvements made as a result of the reporting. This active exchange of safety information is vital for the development of safety and good safety practices within an industry branch. However, this exchange of safety information can be difficult to create channels for, partly depending on the structure of the system, branch or organisation. An example can be found from a study in the maritime domain (Ek and Akselsson, 2005) where no organised exchange of information or learning took place between vessels within the same shipping company concerning, for example, experiences of incidents and quality of equipment. In contrast, this kind of exchange of information existed in a more informal way when seamen changed vessels within the same shipping company.

12. Systematic safety oversight and performance monitoring aimed at assessing safety performance and reducing or eliminating emerging problem areas

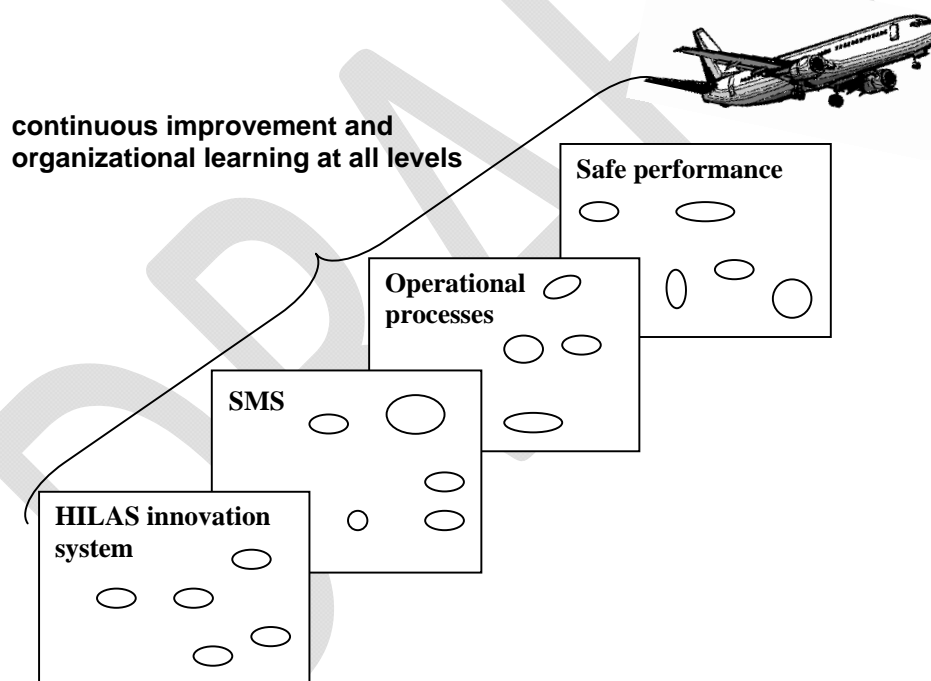
Safety oversight refers to the activities of a State (under its safety programme) and the performance monitoring refers to the activities of an operator or service provider (under its SMS) (ICAO, 2008). A formal system for safety oversight provides the means to verify how well the aviation industry is fulfilling its safety objectives. It includes elements such as comprehensive audit systems, system for analysing flight recorder data, and systematic review and assimilation of best safety practices from other operations. It also includes determining relevant safety performance indicators. These are needed in the safety management process, which is a closed loop, for providing feedback information on safety levels in order to perform necessary adjustments.

## 1.4 The role of HILAS in Risk and Safety Management

The HILAS safety model builds on the assumption that human-well being and overall system performance are interdependent and includes improved efficiency, quality and safety. HILAS has concluded that relevant and valued human factors in aviation systems are included in the identified key processes for the overall system performance improvement process:

- performance management
- risk management
- change management
- organisational learning

Within in these concepts knowledge of human factors are built in and becomes explicit in understanding the HILAS approach for these key processes and concepts.



**Figure 2a:** HILAS Variation on the theme in contrast to Reason

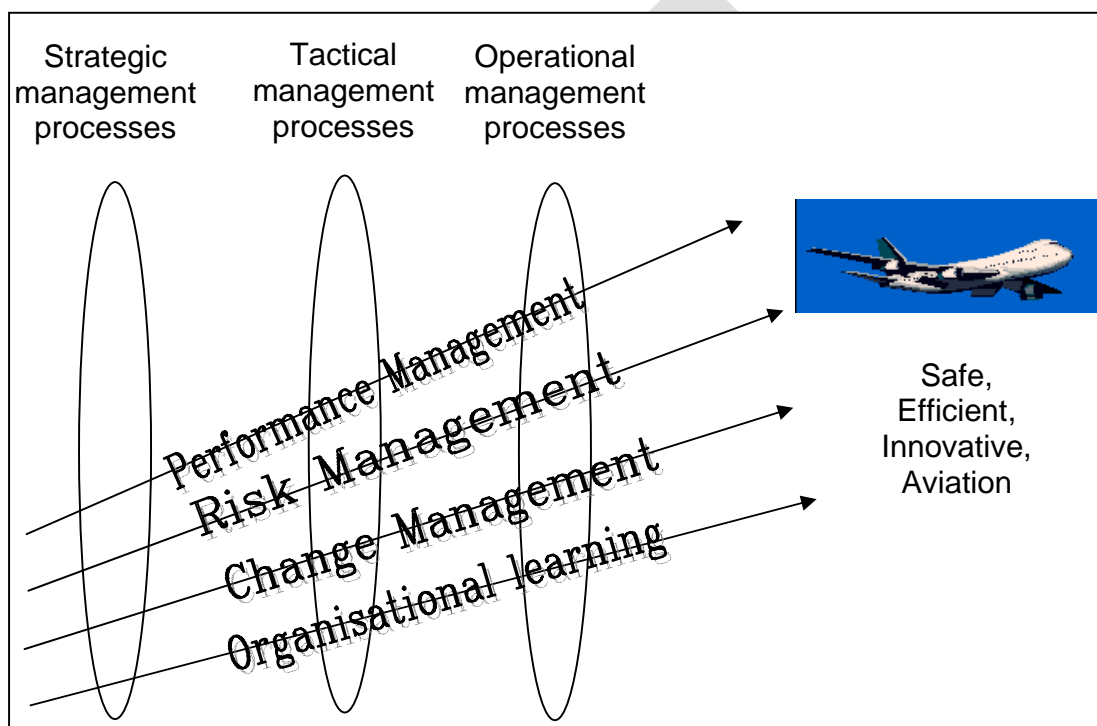
## 1.5 Systemic risk

In the HILAS model of systemic risk both quality (process efficiency and effectiveness) and financial performance may be relevant for safety performance measurement. Decisions for any change may ultimately affect safety and the risk may have financial, qualitative or safety attributes and possibly a combination of all three.

## Operational Risk Management System for SMS and FRMS

The systemic risk model combined with a system model of strategic, tactical and operational management processes gives a more comprehensive picture of risk management going on in an organisation. The five risk logics gives flexibility and allows for time-critical, short term and long term risk management processes applied in appropriate management processes dependent on performance data and change characteristics. These are called evaluatory, exploratory, prospective, retrospective and Time-critical risk logic.

In contrast to Reason's accident model of barriers with holes that enable a trajectory towards an organisational accident; the HILAS safety model could perhaps be seen as several enabling trajectories towards high system performance including safety, see Figures 2a and 2b.

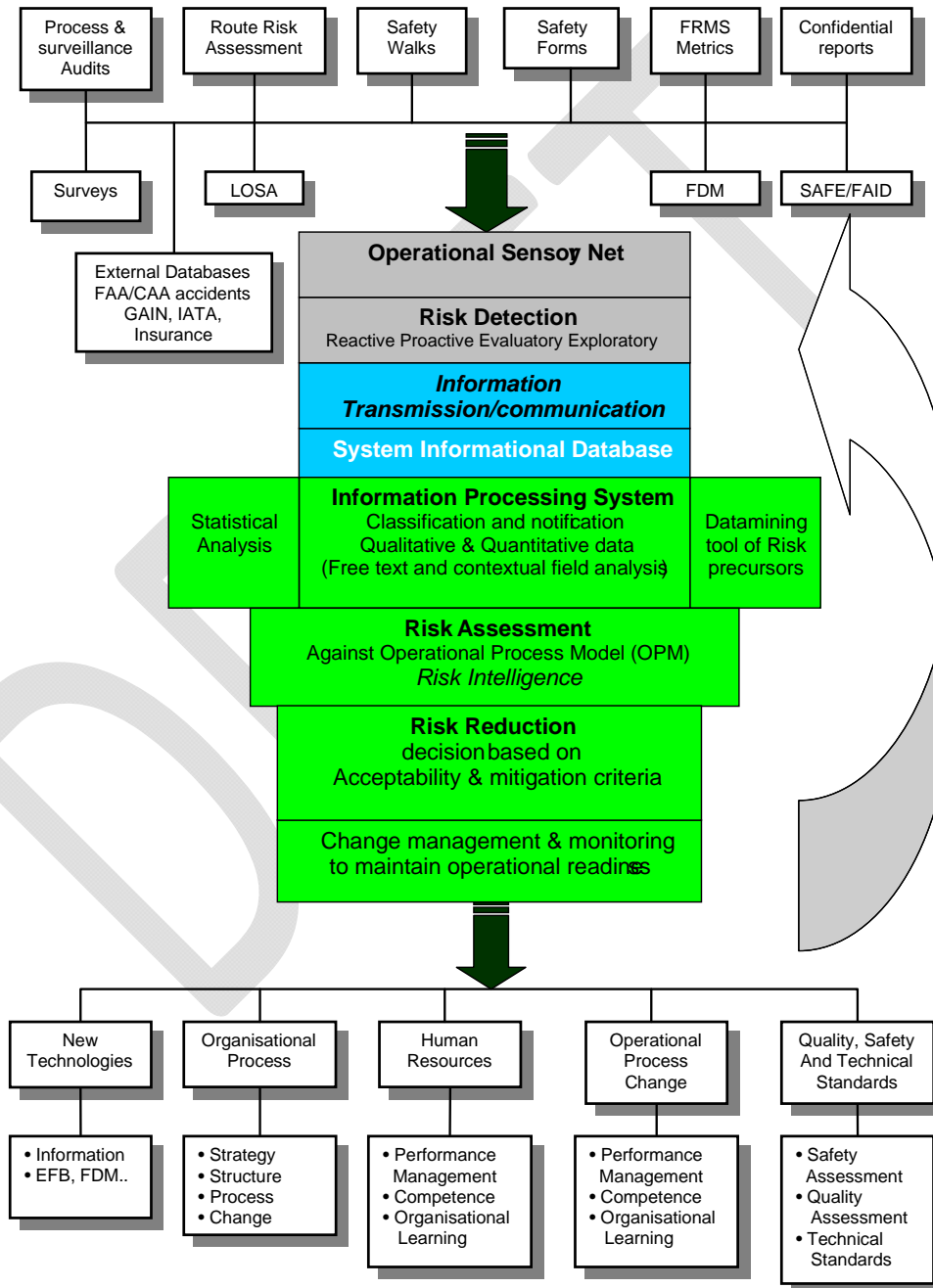


**Figure 2b.** HILAS initiative towards overall high system performance including safety.

The application of this can be extended into a concept of a dynamic Risk Management System (RMS) which is at the heart of an airline SMS (Figure 3). This concept is based on the premise that the inputs to the risk management system form part of a sensory network for the airline collating intra and inter-organisational safety signals. The RMS is supported by a range of safety toolsets (Audits, safety reports, investigations, safety performance indicators, Flight Data Monitoring) that form part of a multilayer framework based on risk logics supporting proactive, exploratory as well as reactive and evaluatory capabilities. This safety information needs to be collated, treated and classified within an Information Management System (IMS) supported by statistical and data-mining capabilities. The processed safety signals (weak and strong) can then be filtered from the background system noise so that limited risk investigation resource can be directed at risk

## Operational Risk Management System for SMS and FRMS

analysis and systemic evaluation of these signals. The role of the investigator supported by data management and confidentiality protocols determines root cause and contributory factors and makes recommendations from the assessment of risk. Risk reduction activity occurs with accountable management who decide from risk treatment options (acceptability or mitigation) that can lead to systemic change management or continued systemic monitoring through the sensory network (feedback loop). The focus of the SMS activity is to maintain airline operational readiness to meet risk and change as well as supporting continuous systemic improvement.



**Figure 3.** Risk Management System concept

## 1.6 Limitations of current airline SMS

*This is the summary of a Risk Management System review conducted from participant airlines in HILAS SMS workshop series.*

### Risk measurement tools lack development to risk needs of operating environment

The airlines reviewed generally did not provide feedback for the refinement or development of their risk detection tools. Performance tracking was limited to medium and high risk events due resource restrictions (weak signals not effectively considered). The Flight Data Monitoring (FDM) software was considered the **primary** safety tool for the airline operation (outcome based performance indicator). It was cited as the **only** SMS tool that provides a contextual based overview of events informing the SMS of 'what' is actually occurring in the operation.

### Manual safety information processing and risk assessment

Safety data management within the airlines was principally a labour intensive manual process that was not scalable against any operators' expansion requirements (without increasing headcount), and the risk assessment training and domain knowledge was limited amongst the staff. Typically, a 165 aircraft LCC operators fleet would generate safety reports in the region of >1200/month and the FDM trace analysis requirements would be >24,000/month. LCC operators have growth expansion plans typically at 10-15% pa, therefore based on the current reporting rate it will necessitate a significant increase in the Safety Data and FDM teams' workforce if digitisation and automation capability is not implemented.

### The investigation process is highly subjective and lacks formal methodology

Risk assessment in an airlines' investigation process depends on the training and human factors analysis techniques employed by an airlines' flight operations department. The risk resides in the operational process which is identified by investigated safety risk. That process must be analyzed using a validated tool to elicit knowledge about the performance of the process.

Within the HILAS airline's, analysis of safety risk was largely unsupported by an analytical capability, even though it is currently been assessed by expert judgement. Some operators appear to be using Reasons' 'Swiss Cheese' model generic framework which has been applied to operators' high risk investigations by their investigative team. The model indicates the area of organisational deficiency however it does not provide the investigator with guidance as to how to analyse a process or improve its functionality.

Airline incident investigations, in general appear to be carried out by highly experienced and motivated investigators who can be a mixture of Training Captains and/or Technical pilots however most investigators lack formalised standardised training and any investigation methodology tools (i.e. event and cause diagrams, change analysis techniques, barrier analysis, root cause analysis). Data-base warehousing platforms, such as AQD, do have an investigation process, however, it only provides a general overview

## Operational Risk Management System for SMS and FRMS

of information flow for an investigation with no reference to investigation technique or analytical tools to support the process.

### Investigations are reactive and limited to mainly high risk events

Airlines have limited resources that focus on reactive high risk events investigation (potentially top 5-10%) with limited analysis of remaining safety data information (potentially 90%). Results from detailed reactive analysis of high risk events are resource intensive and cannot be projected across the entire airline operation as an indication of safety performance. Incident investigations within airline operations provide reactive analysis of past events on what, how and why an event happened (*in order to understand how to prevent future incident re-occurrence*) but it is a limited source of evidence for an operators' system performance. Any investigated risk that is evaluated against its operational process, will elicit an inaccurate or deficient performance result, due to the lack of a developed system model (process mapping).

The SMS requires detection tools that provide a real time and continuous picture of the operation and a capability to apply and integrate the knowledge gained from this process into the organisational system. Operators need a proactive risk strategy that uses all informational resources to detect system risk to protect their business model.

### Risk management practice and decision making is not standardised

Based on the classification schemes employed, events may fall into several classification categories with only one selected and the perception of risk being different depending on the investigating department. There appears to be, within the airline industry limited communication, standardisation and integration of risk management strategy between departments (i.e. Risk assessment practices differ between departments).

There was also no definable management decision model employed against which assumptions, plans; options and consequences; implementation costs and residual risk are reviewed.

### Risk representation is not associated with organisational process

Accountable managers within all levels of the airline organisational structure need to have an appreciation of the risks they own. Risk representation that is not transparent and easily assimilated causes managers to defer to individual investigations to understand the nature of the risk exposure;

The aim of the main safety group meetings is to represent operational process risk in context for the Operations Director. The Management Board Meeting is a platform that balances organisational process risk against the CEO's commercial strategy.

### Safety Management and Quality processes were effectively separate entities within SMS

An airlines quality programme should represent a proactive element of Safety Management. The audit schedule should follow a risk based approach where safety risk against process analysis guides the scope of future audit schedules whilst maintaining the

## Operational Risk Management System for SMS and FRMS

mandatory regulatory minimums. Airlines current schedule appears to be maintained against compliance with regulatory requirements; however, flight operational safety risks are not overlaid against a risk based approach to commissioned audits.

*The SMS supports multiple tools for safety assessment however they are not integrated*

Airlines have multiple sources of safety information within their SMS, which are collected across individual departments, however, they are not effectively integrated into a Knowledge Management System (KMS). Airline investigators and FDM analysts appear to be manually extracting information from the aircrew management system, Flight documentation (flight plans, weather, journey logs) and/or crew training records. Safety Reports do not appear to be linked into FDM. FRMS investigations appear to be standalone. Some airlines may have a statistical analysis tool SPSS installed, however, it appears data will have to be extracted manually and then re-entered into this program to enable limited proactive analysis of safety information. In addition, Safety reports and audit reports appear to be managed separately within the safety data-base platform.

### **1.6.1 External Regulator Review of current airline industry risk assessment capability**

A review of the risk assessment capability of airlines was conducted by the CAA in 2007 (easyJet was a member of this project team). The findings against SMS risk assessment capability and management of the airline industry were as follows:

- *Risk assessments tend to apply to isolated areas, processes and procedures (e.g. new destination evaluation);*
- *They tend to be the responsibility of a small specialist team or individual and rarely cross organisational boundaries;*
- *They are not conducted according to a common philosophy or using common tools or methodology;*
- *They tend to be conducted only when needed for particular operational reasons;*
- *Safety risks are handled in a different way to business risks;*
- *Risks incurred by changes are rarely identified and managed systematically;*
- *Focus tends to be either on proactive or reactive risk management, not both; and*
- *The lessons learned are not systematically recorded or spread across the organisation.*

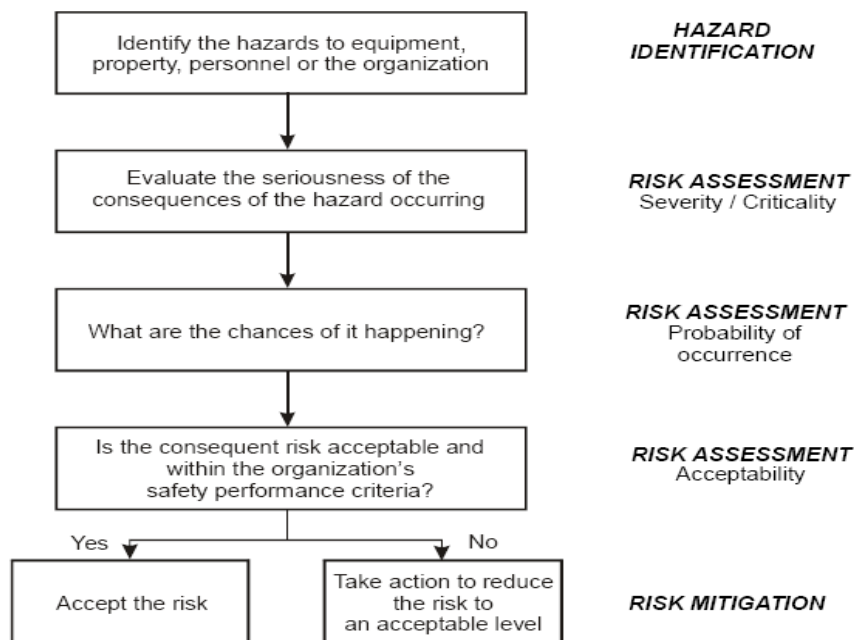
*CAA Risk assessment and regulation (draft) project report 2007*

## **1.7 ICAO Risk Management Process**

The risk management process seeks to identify, analyse, assess and control the risks incurred in airline operations so that the highest standard of operational integrity can be achieved and maintained. This standard of operational integrity can only be delivered through safety practices which identify risks. It must be accepted that absolute safety is unachievable, but reasonable safety can be achieved across the spectrum of the operation.

## Operational Risk Management System for SMS and FRMS

Airlines tend to have SMSs that are primarily reactive: that is, they respond after incidents have occurred. Reactive analysis of past events provides useful information on how and why an event took place (in order to understand how to prevent re-occurrence), but it is a limited source of evidence of overall system performance. The ICAO approach to risk management (figure 4) is essentially technical model based on an engineering process viewpoint and is more applicable in concept to stable systems such as chemical and nuclear industries.



**Figure 4.** ICAO Risk Management Process (*source SMM 9859 pp6-2 2006*)

If airlines are to manage fatigue and other risks in a proactive manner they need to apply risk detection tools that provide real time and continuous systems oversight.

### 1.8 Functionality of National Aviation Authority Oversight

Traditionally under the auspices of the Air Navigation Order (ANO), the CAA developed a system of compliance auditing looking at defined areas using checklist based tools. The areas encompassed the Flight Time Limitations (FTL), Flight and Aircraft Checks and Training Records. This worked well with small to medium sized companies with limited levels of management structure, as any process deficiencies would expose specific weaknesses in the company structure. Overall management competence and structure was not the focus of the auditing team.

With the advent of EUOPS and the growth in company size the focus of auditing has had to shift towards the organisation and structures of companies. The situation that the CAA must address is how to develop processes that will address these areas and there appears to have been some difficulty in developing these techniques and control mechanisms. At the same time there has been a downsizing of the CAA and a reduction in inspecting staff. More reliance is being placed on the Inspecting Officers in conducting these audits.

## Operational Risk Management System for SMS and FRMS

These officers are well trained in auditing techniques but do not have extensive experience gained from working within aviation companies. They have the facility to call on pilot resources within the CAA, should they feel that is required, and at present are operating under the direction of a qualified flight operations inspector. The eventual intention is to rely on company internal auditing, which will be checked by the inspecting officers.

This concept of operation will only be achievable if an airlines' quality department is well resourced and have complete autonomy of the mainstream organisational structure. However for this auditing to work efficiently there must be a defined structure against which to audit. Historically, it has been necessary for the inspector to develop a close working relationship with the company in order to become aware of the day to day processes of the various departments which he can then examine. Should this time consuming relationship not be in place auditing becomes a chance process as the inspector endeavours to decide where his limited resources should be concentrated. The inspector has to rely on Mandatory Occurrence Report's (MORs), FTL breaches and information from complainants to the authority to identify inefficiencies of the company and possible areas of weakness.

A strong internal company audit process (internal governance), that utilises an approved schedule and able to react instantly to changes in the company processes can inform the CAA against an examination schedule already in place. This will highlight weaknesses which could be discussed prior to an audit and used to target areas for the CAA to look at more deeply, thus enabling concentration of scarce resource directly to the needy areas. This would require regular assessments of an airlines' quality departments by qualified CAA personnel.

### **1.9 Management awareness and exposure to operational risk**

Currently, airline safety departments do not have a comprehensive appreciation of the level of risk to which the accountable manager is exposed due to the inability to measure the risk. An FAA (Von Thaden & Wiegmann, 2004) research paper demonstrated that deficiencies in many of the SMS components contribute to the development of accidents and serious incidents. Implementation of new analytical tools or processes in an attempt to transition away from reactive only analysis of events can be difficult as safety management performance metrics cannot be easily quantified under a financial business case Performa (cost benefit analysis of *not* having an accident). Safety is not the only risk priority to a business model and resourcing must compete with other business projects.

Similar limitations and mitigative influences have been reported against the current approach to safety management in airlines (Dijkstra, 2006) that support the findings presented here. The Hampton report (2005) highlights a requirement that comprehensive risk assessment should be the foundation of all regulatory enforcement with the emphasis being on operator self governance. Regulatory oversight of operators should reflect the level of risk represented by the operatoCorporation recognises that the preventive approach of safety management system can represent in an organisation a 15% to 50% of

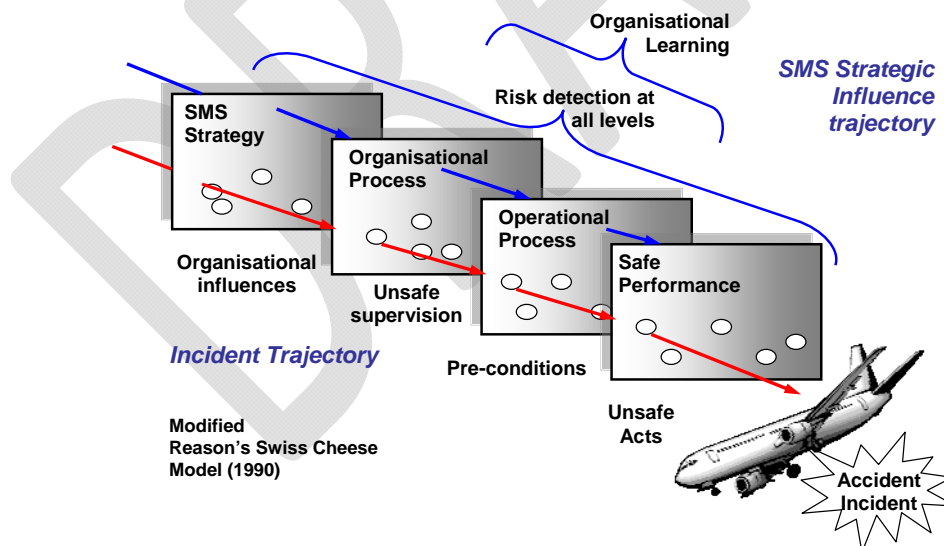
## Operational Risk Management System for SMS and FRMS

saving in operational costs, 30% in optimisation and efficiencies, and additional 5% within HSE (Shell, 2007).

Airlines need to develop a Risk Management System that embraces an *evidence-based Safety Management System that proactively and continuously delivers safety effectiveness and operational integrity within a risk controlled environment*. This airline strategy should be institutionalised and integrated across departments to deliver a **lean** system embracing optimization and efficiencies), **controlled** (self-governance embracing management process mapping, risk-based decision-making, competence, and training) and **dynamic** system (flexible risk tolerant business model with technological innovation and organisational learning).

An airline safety policy should embody safety objectives (risk elements) that have the ability to generate:

- *An effective and timely **reactive response** to incidents;*
- *A comprehensive **proactive analysis** of risk using all available information sources to maintain system integrity;*
- *A **risk trending capacity** that effectively evaluates implemented control strategies;*
- *An ability to **explore future risks** within the system due to organisational and/or business strategy changes; and*
- *An ability to effectively **represent in a clear and transparent manner** the system dynamic risk state to all management levels in a standardised format.*



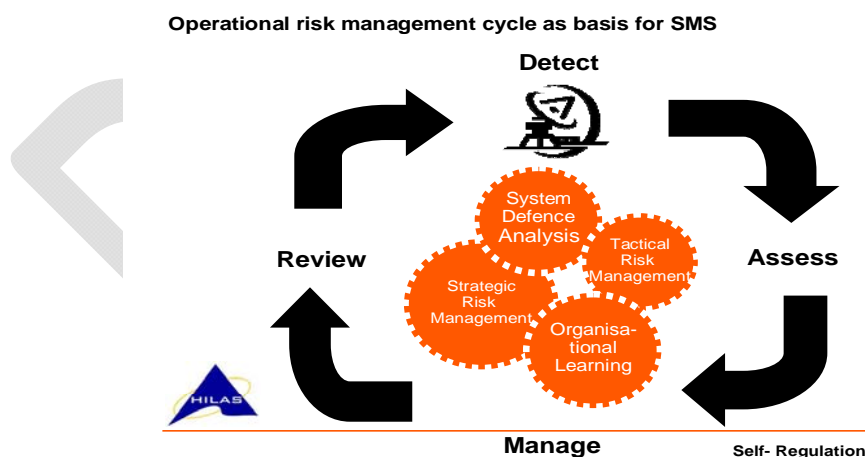
**Figure 5.** Strategy, process to risk detection capability

Reason's Model (1990) tells us that every incident trajectory has an unsafe act where associated latent failures within the organisation has contributed to this event. The "modified Reason Model" states a safe performance is achieved when an integrated SMS strategy is implemented detecting risks at all levels of the organisation, mitigating these

risks (Reactive Proactive Evaluatory Exploratory processes) then coalesce this applied knowledge into Organisational Learning and store it for later (re-)use into Organisational Memory (see also OL/OM chapter in Book 1)

## 2.0 easyJet-HILAS Systems Integrated Risk Assessment model (SIRA)

easyJet and HILAS have developed a risk management framework to suit an aviation SMS known as SIRA (Figure 6) (Stewart et al, 2006 & 2008). The process integrates safety assessment, multi-criteria decision making and organisational learning. The process is based on a risk radar approach acting as a system sensory net scanning the risk environment gathering a wide range of technical, human performance and system data. The data is managed within the company Aviation Quality Database (AQD) and an intelligence process classifies and analyses causal patterns. This drives decision-making, intervention design and monitoring against the operational system. The cycle then continues utilising feedback loop processes as a function of risk management from both strategic and tactical interventions. As a result, SIRA process embodies strategic organisational learning with a reporting stage based on a risk modelling platform and a weighted risk boundary calculation index. The tactical and strategic cycles of the model are interdependent represented by the larger strategic cog driving (and driven by) the smaller tactical cog dealing with day to day risk activity. The strategic cycle represented by the larger cog encodes whilst the tactical cycle deals with day-to-day risk activity with corresponding response speeds.



**Figure 6.** Operational Risk Management Cycle as basis for SMS

### 2.1 Operational risk in aviation and the HILAS approach to risk detection

The following are the main characteristics of the operational risk environment in aviation:

- Very low rate of serious incident (hull loss, fatality). Too low for direct computation of operator (airline, maintenance company) risk index.

## Operational Risk Management System for SMS and FRMS

- High frequency of discrete operational units (flights, aircraft checks)
- High acceptance of normal operational performance monitoring enables the generation of large amounts of data on normal operational performance (both human and technical)
- Strong institutional and regulatory requirements for reporting occurrences and other operational deviations generates both a wide range and a large number of reports on relatively minor failure (in terms of consequences)
- Rapidly increasing IT integration across the organisation, including operational areas, enables the linking of a wide range of data sources (including planning, technical, human resources, operations, quality and safety).

All these factors combine to create the possibility of an integrated assessment of risk which has the following characteristics:

- It links data representing the state of the system to data representing a variety of outcomes of operational activity. This is the basic requirement for the analysis of risk.
- No single metric of system failure is possible. Rather it is necessary to construct a composite metric compiled from different types of outcome. These will include technical, operational and human performance indices which relate to different degrees of severity of outcome (from normal operational success to mandatory reportable occurrence).
- A wide variety of different data sources (again representing human, technical and operational factors) are relevant to defining relevant states of the system which potentially are probabilistically related to the composite of outcome metrics outlined above.
- The risk metric is therefore based on a complex process of statistical data analyses, driven by reasoned judgement, which constructs a balanced analysis that integrates all relevant information in a composite overview.

In order to manage and make sense of this complexity in range and types of data, it is necessary to have a model of the operational system. It is a truism of systems engineering that without a model of a system it is impossible to understand the functional relations within a system. Without understanding these functional relationships, it is impossible to derive requirements for how to change the system to improve its functioning. In the current context, such a model enables one to link the systems variables together in a coherent manner and the outcome variables together in a coherent manner. Such a model should also recognise that operational outcomes are the result of long sequences of process activity (leading from planning and supply to the operational process itself). Therefore outcomes at any particular stage of the process become inputs (states of the system) for subsequent stages on the process. Such a model also needs to be hierarchically organised (micro to macro) in order to address the complex ways in which human performance influences system outcomes. Within an operational risk management framework the role of a model is to:

- Represent current system states, dependencies, and necessary resources, thus providing a coherent framework for linking variables indicative of both system states and system outcomes.

## Operational Risk Management System for SMS and FRMS

- Help identify underlying causal mechanisms
- Help analyse requirements for system change

The following scenarios are integrated into the 'sensory network' of an aviation risk management system to illustrate the way in which such a risk management process might work. They concern primarily the role of a risk analyst and his or her task in deriving risk analyses through processing the data in the system. Beyond reporting to senior or strategic management, these scenarios do not directly address how these risk analyses are used in the organisation (or even between organisations).

### 2.2 Five Risk Logics

The systemic risk model combined with a system model of strategic, tactical and operational management processes gives a more comprehensive picture of risk management going on in an organisation. The five risk logics gives flexibility and allows for time-critical, short term and long term risk management processes applied in appropriate management processes dependent on performance data and change characteristics.

*Reactive mode*, is a post-hoc process by where the SMS reviews data that indicates a variance or disturbance from the 'normal' safety state. Events or incidents and accidents fall into this category where the system safety barriers and controls have been breached as a negative outcome for the incident to have occurred. The incident is reported into the SMS through a safety reporting process such as a Air Safety report or Fatigue report for that captures descriptive contextual information around the incident and universal free narrative. Incident reports are encoded into the event method classification database in the airline and prioritised for investigation per operational domain. Incidents are broken into sequence of events and significant factors analysed by subject matter experts against the required performance specifications per organisational level of the system (safety barriers and controls). Approved corrective actions linked to accountable personnel are implemented, tracked and monitored for effectiveness as part of the quality assurance function to ensure stable normative functioning of system processes.

#### *Pre-emptive risk detection capability*

*Proactive mode* is a forward looking capability within the SMS that reviews potential risk precursors to the system processes and controls, investigates and develops safeguards for implementation. This capability extends to a reactive-proactive process where existing safety databases are mined (quantitative analysis) for risk indicators within the system and sub-processes. An example of this is the review of existing investigations where contributory risk precursors to an undesirable system outcome may have impact beyond the context of the investigation and be common to other incident categories. e.g. Air Traffic Control language issues may be responsible for both unstabilised approaches and level busts on certain company routes. The proactive capability extends to the commissioning of network surveys to determine system subjective feedback on risk related issues and the application of Line Operations Safety Audit (LOSA) observations.

*Exploratory risk mode* is also proactive but is applied where there is little direct evidence (knowledge of domain safety experts) where new systems or processes are to be implemented as part of strategic change or renewal. They may also be triggered due to the limitations of existing hazard detection tools and where risk signals have been received from a review of external data sources such as IATA STEADES or ASIAs programs.

*Evaluative mode* is the monitoring and evaluation of risk implementation strategies. This mode measures the effects of change as a function of time where metrics are encoded into the system to track the performance of new risk control processes against preset performance criteria.

These pre-emptive risk modes by their nature require that an airline operation is process mapped and effectively modelled so that the interaction and interdependency of change against system performance can be tracked and performance reported to management. The overall process is data driven so that risk treatment solutions are evidenced based and can be balanced against the company business case for the decision makers.

Time-critical risk management processes rely on a current Risk Register, often supplemented by retrospective risk analyses generated from reports of individual events. Time-critical risk management is conducted immediately prior to activity (e.g pre-flight briefing, initial check meeting) and during activity, either at predetermined points in time or when situational factors unexpectedly change. It is of use to both planning and operations staff (i.e., both for planning as well as for carrying out activities).

We will now establish the risk logics that meet and exceed the ICAO guidance for reactive, proactive and predictive capability that are integrated into the SIRA process. Firstly, an outline of the core functions of SIRA as an airline Risk Management System.

### **2.3 Core functions of SIRA**

1. Detect, measure, categorise, investigate and analyse hazards from the operation. Interface from safety risk assessment to process orientated view as part of the risk based quality management approach.
2. Prioritise strategic and tactical risk management activity around the development and implementation of controls for identified risk
3. Communicate, allocate and implement change management activity
4. Track, Monitor and residual risk assess the performance of implemented controls
5. Feedback to individuals, system and regulator as part of a continuous improvement cycle

## Operational Risk Management System for SMS and FRMS

The investigation process in the SIRA model is condensed in steps 6 and 7, see Figure 7, and links the output which identifies systemic causal factors in the context of the investigation to the risk management process. Causal factors can stand up separately from the context of an individual event investigation and have generic implications to normal system functioning. An example of this is where a systemic factor identified in the context of an event may be crew age and performance decrement. Beyond the context of the investigation crew age and performance decrement may be assessed as a system hazard and may have negative consequences against safety criteria within a number of system processes. In this way the systemic factor can have strategic risk implications for the operation beyond the context of the individual event.

### ***SIRA Model steps***

Figure 7 depicts a Risk Management Process of an airline: the SIRA model. The steps in this model are described below.

1. Stage one of SIRA considers the external signals from the operational environment and those within the organisation (intra and inter) and third party suppliers-quality control and assurance. A suitable analogy would be the aircraft crew and systems operating in the physical environment of weather/terrain/airspace/ramp etc..
2. Stage two is the detection stage where the sensory network or risk radar for the organisation encompasses capability from the five risk logics (reactive, proactive, time critical, exploratory and evaluatory) as an evolution from the primarily reactive aviation model. Information sources can be internal and external to the operation (CAA databases; IATA Steades, other airlines with which safety agreements are inforce)
3. Stage three is the data communication stage where data is treated and sent to a central repository for interpretation and encoding. The data may be in the form of scanned or digitised report forms, FOQA data, ACARS reports, audit reports etc The data represents both structured and unstructured formats.
4. Stage four is where the data is classified within a method classification model (AQD database) in preparation for domain expert triage as part of the initial risk assessment process. The Safety data team collate the SMS information from the detection system into one information management system (IMS) that facilitates data storage for safety reports, investigations and quality audit reports, surveys, losa reports and the tracking of accountability and actions implemented from the risk management process. The information management system is centred on a method classification event model with an integral statistical capability and is the information source from which system performance trends are generated. The IMS is linked into the prime data sources to facilitate incident investigations and process evaluation within safety and quality.
5. Stage five represents the initial risk assessment step facilitated by Critical Incident Technique and domain expert triage. This step represents the *inquiry need* and *notification* of investigators.
6. The risk assessment stage includes risk identification, investigation, analysis and recommendations on systemic causal factors. The investigation process is

outlined in HILAS Chapter x (Stewart et al, 2009), a short summary is provided here. The inquiry process employs Case Based Reasoning (CBR) (Aamdt & Plaza 1994) which identifies the current problem, reviews previous similar investigation risk management strategies and suggests/adapts a solution to the current risk areas identified in the report. An evaluation of the proposed solution occurs before strategy selection and system adjustment/update occurs (learning from the investigation process). The process adapts or employs knowledge based on previous learned experiences (old solution adapted to new problem). The CBR process employs a range of different techniques for organising, retrieving, utilizing and indexing the risk knowledge retained in past investigations. Where further detailed investigation is required this stage is facilitated by core analytical capability within the investigation process (toolbox of context related analytical tools, i.e. Bowtie analysis, root cause analysis, event and causal factor charting, MORT, Fault tree analysis, barrier analysis, change analysis). This tool selection and application process employs the tool/context/people/task/output concept from Frei et al (2003). The toolbox includes a users guide as to the application of analytical capability in context and depth required to support the investigation.

The feedback loop to the sensory network at this stage supports the possible requirement for more information around identified risks to support the investigation process. The investigation process is supported by a just culture management process to determine culpability around unsafe acts versus non-punitive human performance management (refer HILAS Chapter x, Stewart et al, 2009)

7. The generation of strategic and tactical risk treatment options with the pros and cons detailed then follows. This includes cost of implementation (per domain area) as well as projected risk after treatment is effected. Tactical risk management represents preliminary risk control activity. Strategic risk management activity may require further exploratory risk investigation if identified from the investigation process. For example preliminary activity may be concerned with putting out the fire whilst strategic considerations may be associated with removing the fuel source. Tactical management is associated with single loop learning whilst strategic management considers dual loop learning activity (Koorneef & Hale (2007)). Strategic options will all be associated with subsequent tactical management activity.
8. Strategic and Tactical management of systemic causal factors. This stage of SIRA reflects the tactical and strategic processes represented as system cogs. The smaller tactical cog spins faster than the larger strategic cog showing tactical management of risk being dealt with in-silo activity for day to day time critical risk decisions set against safety criteria. The strategic cog spins slower as it reviews all system inputs against a safety boundary facilitated by the Aerospace Performance Factor tool (APF) (Lintner & Smith 2008) before initiating strategic investigations and change management. The strategic process involves the risk stakeholder group and is actioned through the board safety reporting meetings both monthly and the management quality review meeting quarterly. The decision making process here is facilitated by

## Operational Risk Management System for SMS and FRMS

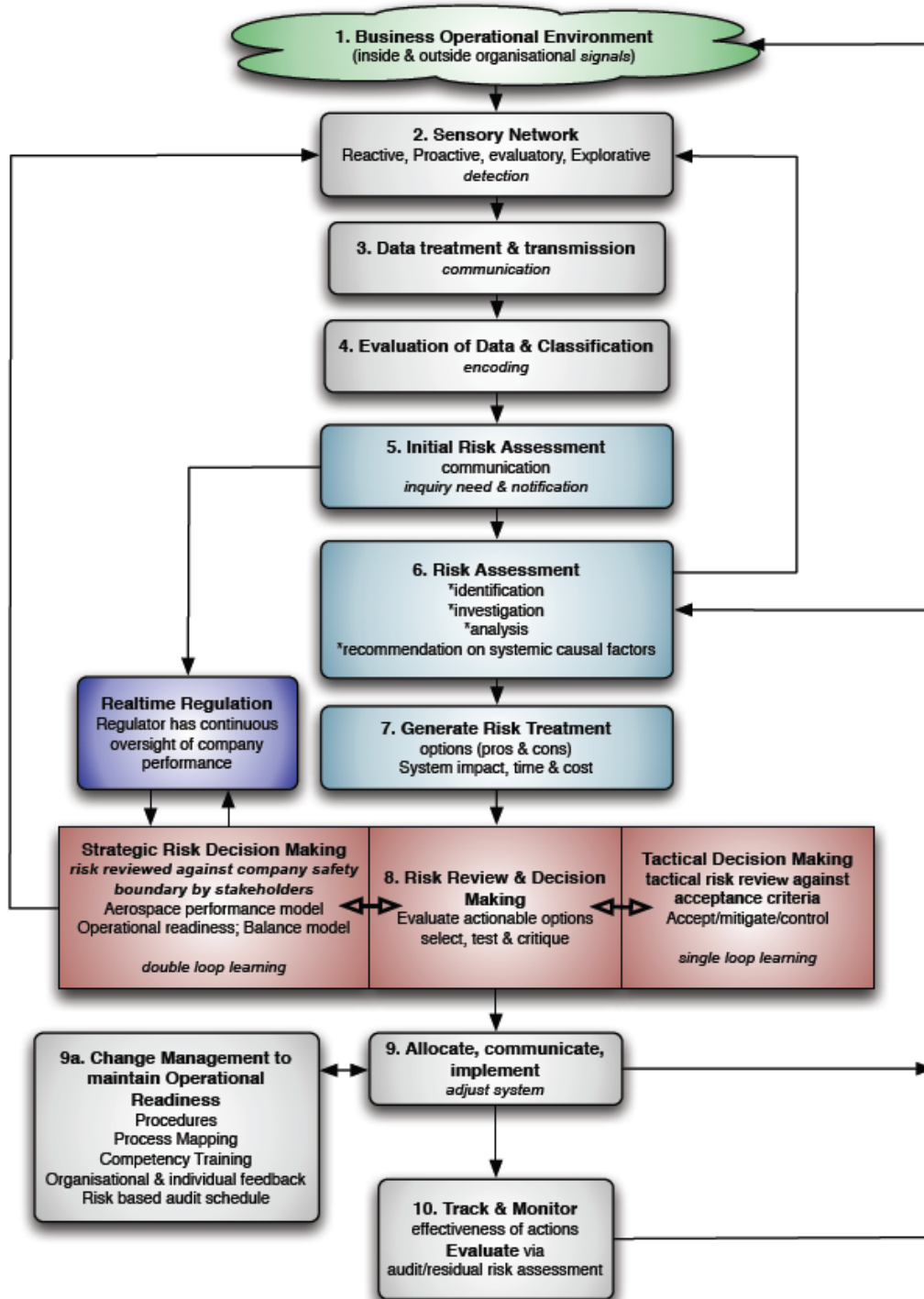
Analytical Hierarchical Process (Beauchamp (2007) to evaluate, weight, rank select and critique strategic risk options. The strategic feedback loop has the capability to tilt the sensory network to focus on strategic risk signals. Tactical strategy selection can be facilitated using the Cohen et al (1996)

Recognition/Metacognition model (R/M). The model describes a set of critical thinking strategies that support memory/recognition of known problems/treatments. The process supports the critiquing to identify problems in the risk treatment options based on unreliability, incompleteness or conflict in the options plan. These identified issues are corrected by collecting more data, adding or dropping assumptions and/or changing scope/focus of information retrieval. The R/M model facilitates experienced decision makers to exploit their domain experience but also remain flexible for new novel situations. This model complements the CBR approach of problem solving and learning. Real-time regulation is supported by National Aviation Authority Flight Operations Inspector (FOI) access to the APF tool which provides access and risk transparency at all organisational levels. Links from the APF graphical representation extends into the company risk registers facilitating continuous risk oversight of the operation. This process allows performance based regulation instead of simple binary compliance and facilitates the regulator to design focussed audits, which benefit the airline. Where SMS performance and risk management practice is within mutually accepted tolerance levels this provides evidence for the insurance community on risk signature, evidence to the regulator for a reduction in formal oversight visits and regulating authority fees.

9. Once a course of action has been selected by the risk stakeholder group, then it must be allocated, communicated and implemented to the relevant management levels (new or existing strategies). Change management as a form of organisational learning takes the form of process change mapping, introducing new procedures, safety standards, new technology, competency training, a change in risk based audit scope and frequency for operational process risk and individual and system feedback.
10. A decision must be made on how to track and monitor the implemented actions and to assess the residual risk to the modified process and the performance of processes dependent around the implemented risk strategy. The residual risk from a modified process may have raised the system risk level by transferring the risk to other linked or dependent processes. A residual risk assessment must account for singular and system process performance against acceptable criteria. The evaluation stage of an implemented strategy usually consists of an audit of the process change. This represents a discrete assessment. A dynamic feedback capability should exist to support a continuous monitoring capability by the sensory network. Should the strategy not be fully effective a new or adapted strategy can be implemented represented by the feedback loop to risk treat options identification. If the strategy performance is acceptable or requires further monitoring then a second feedback loop returns to the sensory network stage. The report is documented in the IMS and information prepared and trended for the Safety Action Group and Safety Review Board. An adjustment

## Operational Risk Management System for SMS and FRMS

at this stage can be made, if required, of the safety and operational performance criteria as recommended from the investigation report. If the strategy is unacceptable the investigator returns and redefines the scope of the investigation.



**Figure 7.** SIRA Airline Risk Management System Model

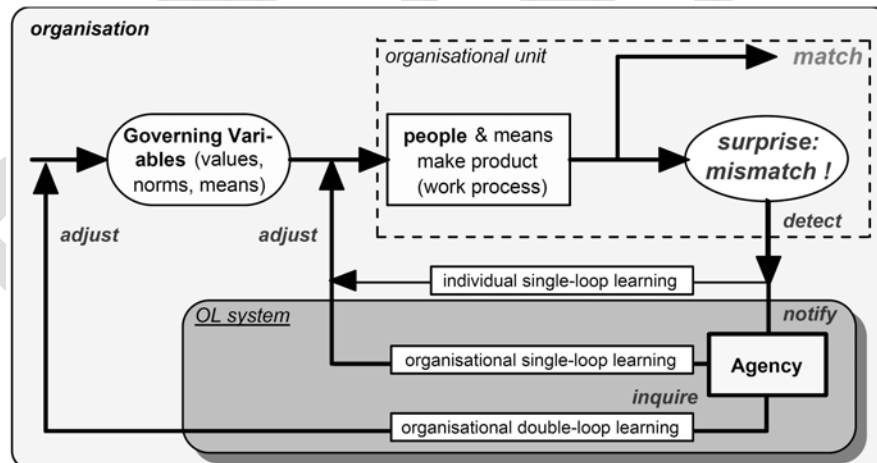
## 2.4 System of Organisational Learning in SIRA

This section describes the implementation of a System for Organisational Learning (SOL) as integrated into an airline risk management system.

The description and functioning of the SOL model has been outlined by Koornneef in the OL and M chapter (book 1). Here we will revisit the basic principles as they pertain to a risk management process.

The Key functions in organisational learning incorporated as the core of the SIRA Risk Management System are, see also Figure 8:

1. *Detect*: an abnormal condition or event [by crew safety report, by inspection or audit, by data processing system, etc.]
2. *Notify*: make known to appropriate 'elsewhere' that something unexpected has been detected [consult organisational memory for known problem and solution; trigger triage review]
3. *Inquire*: investigate what the detection signal represents: new problem, known problem, etc. and what sets of measures would resolve the problem situation [activate 'learning agency']
4. *Adjust*: implement by accountable management the selected set of measures into the work process, or modify governing variables first before changing the work process [line management, crew]



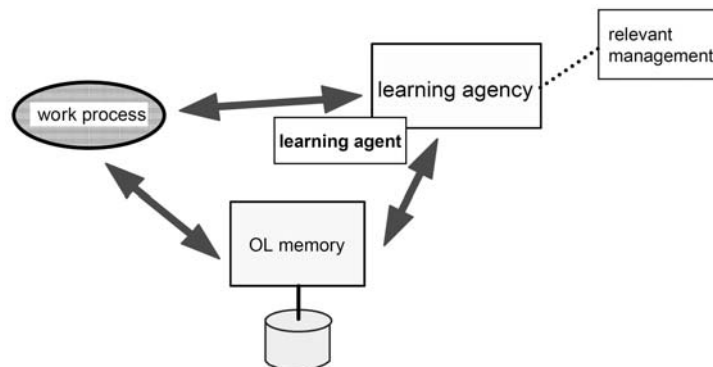
**Figure 8a.** Organisational Single- and Double Loop Learning modified after Argyris (Koornneef, 2000)

Key elements in Organisational Learning are, see also Figure 8b:

- a) the *work processes* that generate performance signals,
- b) designated persons that take on the task of learning for the organisation as a member of a '*learning agency*', and
- c) *Organisational Memory* that is accessible for storing and retrieval of lessons learned-in-context.

## Operational Risk Management System for SMS and FRMS

The SOL-model, described below, depicts key elements and interactions in organisational learning processes.



**Figure 8b.** Basic Model of a System for Organisational Learning (SOL) (Koornneef et al., 2005)

Argyris (1982) identifies 3 modes of organisational learning:

- I. Organisational Single Loop Learning (OSLL): tactical modification of the work process within the span of control of the first line manager
- II. Organisational Double Loop Learning (ODLL): modification of governing variables (resources, targets, etc.) that requires decision making by higher management or beyond
- III. Deutero-learning = learning about problems with the Organisational Learning system

The improved SIRA process described in this document is an output of a mode III organisational learning process.

In short, Organisational Double Loop Learning - mode II - requires strategic decision making at any appropriate tier higher than that of the work process that triggered the learning process. ODLL requires open-mindedness of people involved, which in turn requires a climate or culture that lowers the detection level, encourages people to activate the OL-process by notification without fear of retribution.

Organisational Single Loop Learning - mode I - often regards tactical changes in the work process that generated the learning process trigger (= detect + notify), but might transfer another work process for Organisational Learning, e.g. in another department that is more or less tightly linked with the operational process in view.

The key functions in Organisational Learning (detect, notify, inquire and adjust) are embodied by 'learning agencies' and 'organisational memory' interconnected with operations and management (Koornneef and Hale, 2004; Koornneef et al, 2008).

A Learning Agency consists of persons who take on the role to learn on behalf of the organisation and bring in their collective expertise, including tacit knowledge, about daily practice as far as relevant to the operational problem in operational context. Examples of learning agencies in an airline include organisation Safety Action Groups and Safety Review Board with members comprising risk stakeholders and accountable management.

The core function is 'inquiry' resulting in a preferred set of measures that are communicated with line management for implementation, or in identified problems that need to be solved by other stakeholders. Typically, members of a learning agency are very busy and are scarce resources. This stresses the need to store problems and outcomes from the inquiry in organisational memory that can be accessed for reuse of solutions (airline department risk registers).

Organisational Memory exists in different forms, including external regulation, directives, protocols, manuals, training programs, IT storage & retrieval systems, dedicated meetings, such as SAG meetings, and group behaviour that can be observed to read out this form of memory. Much knowledge that operators have about daily practice is tacit in nature and can be mobilised for organisational learning in the setting of a more or less formal designed 'learning agency' function.

### 2.4.1 Organisational Learning in SIRA

The SIRA process model has been redesigned and enhanced by applying principles of Organisational Learning resulting in a realignment of existing bodies and closing learning loops. To prove the claim that the SIRA process embeds an organisational learning system that meets principles of Organisational Learning, the SIRA model is annotated below.

The core business process is flying aircrafts (in case of SR Technics: maintenance of aircrafts) safely and economically sound. These prime operations are enabled by supporting processes in distinct business units or departments that are interlinked, but that focus on their own support processes. Thus, these supporting operations might be perceived as existing in *silos*. The business processes generate many signals captured through different monitoring and reporting systems.

In SIRA Step 1, the 'business operational environment' generates performance data in many different ways varying from continuous streams to event reports submitted by crews. Also, data and information about safety problems and developments in aviation become available through other communication channels.

The 'Sensory Network' in SIRA Step 2 *detects* trigger signals coming in from Step 1 in four risk mode categories: reactive – proactive – evaluative – explorative. Each category requires a dedicated process of organisational learning set up and when needed in place, with different scopes and objectives. This is reflected in the application in context of the SMS hazard detection tools that can be categorised within the risk modes. For example, a LOSA audit is an observation hazard detection tool based on threat and error management taxonomy. The summarised output of a focussed or system LOSA actioned in accordance to a risk trigger (required audit compliance schedule or an FOQA event frequency trigger) represents a proactive SMS hazard detection tool but is applied in accordance with management safety objectives, safety data protections and confidentiality, trained observers, ethical considerations from audit participants and the treatment and analysis of data.

## Operational Risk Management System for SMS and FRMS

SIRA Step 3 handles data from Steps 1 and 2 so that it can be stored in the common data repository system (e.g. AQD).

In SIRA Step 4, AQD data is analysed by the AQD team for additional triggers based on systematic data analysis. Thus, this Step also *detects* trigger signals that will be forwarded to a domain expert triage process.

In SIRA Step 5, domain experts or Subject Matter Experts (SMEs) evaluate trigger signals from Steps 2 and 4 regarding risk mode category, severity and need to inquire by a leading problem owner (*silos manager*). This 'triage' process results in a OL **notification** signal that triggers further inquiry from within a *silos*.

The OL *inquiry* process is embodied in SIRA Steps 6 and 7. Step 6 starts with a quick scan of organisational memory (focused on the AQD system becoming part of **Organisational Memory**, when possible also tapping into the individual memories of domain experts) to see whether the problem really is new or already known after all. New problems get full attention regarding analysis and - in Step 7 - risk treatment options in organisational single (tactical) and double (strategic) loop learning modes. The Safety Action Group (SAG) of the leading silos takes the role of silos-based **Learning Agency**. As the leading investigator in the inquiry process sits within a silos, it is possible that some treatment options can only be identified from the perspectives of other silos. The inter-silos SAG is in the position to assess this as an inter-silos learning agency, once the facts from the inquiry are made available by the leading silos.

The SIRA Step 8 takes the treatment options from Step 7 into decision making at appropriate management levels about tactical and strategic choice of treatment options to be implemented in SIRA Step 9. Learning Agencies in Step 8 are potentially inter-silos SAG, Safety Review Board (SRB), and PLC. Tactical decisions can be implemented by work process managers to *adjust* daily operations and, thus, establish organisational single loop learning (**OSLL**). Strategic decisions impact on governing variables of daily operations and, thus, establish organisational double loop learning (**ODLL**). On their turn, these work processes need to *adjust* their work processes accordingly. Selected treatment options will be stored into AQD memory and so will modified or new directives and protocols.

This completes and closes the organisational learning process that encompasses the whole organisation from shop floor processes generating performance data and trigger signals through learning agency functions at appropriate tiers all the way up to the PLC when needed for strategic decision making at the highest level, supported by accessible organisational memory.

## 2.5 Safety Risk Management and Safety Assurance

The function of an airline safety management system can be broken into two principle domains, that of safety assurance and safety risk management (Stolzer et al, 2008). Safety risk management activity is associated with the identification of hazards, assessment of

## Operational Risk Management System for SMS and FRMS

risk and the development of risk control strategies. Operational evaluation of these strategies determines whether they in effect control the identified risk and can then form part of the Safety Assurance function. The Safety assurance process continuously monitors operational activity ensuring that risk controls are applied effectively, are consistent and robust in that they continue to achieve intended objectives (supported by systemic safety performance indicators). These two core operational activities take place under the umbrella provided by a safety policy and safety objectives and are supported by safety promotion and feedback.

Each component is subdivided into elements, which encompass the specific sub-processes, specific tasks or specific tools that the actual management system must engage or utilise in order to conduct the management of safety as just any other core business function or organisational process.

An approach to the integration of Safety Risk Management (SRM) and Safety Assurance (SA) has been proposed by the FAA (2006, p10) that emphasizes the function of the safety assurance process as the corner stone of SMS supported by a risk management system. The FAA safety risk management process identifies hazards from a system description (based on new process elements to a system, e.g. new technology) and conducts a risk assessment (risk analysis and evaluation) to provide the accountable manager, as decision maker, with risk treatment options. Risk reduction (decision, implementation and monitoring) introduces risk controls that bring the identified risk within acceptable levels and then closes the feedback loop returning to the system description stage. The Safety Assurance loop functions to ensure that the safety controls are operating effectively (measured effectiveness) with the aim of maintaining system stability within prescribed risk threshold criteria or targets. The interface between the SRM and SA processes occurs at two stages. Firstly, when a potential new hazard or ineffective control is detected from a system assessment of safety assurance information sources (investigations, audits and continuous monitoring metrics) and second where identified risk is deemed acceptable and the process returns to overall aviation system operation. The model establishes that SRM occurs once at the system design point to establish capable system controls and then as required, if triggered by new hazards or ineffective controls (Stolzier et al, 2008).

The FAA concept essentially describes the SRM/QA function of a technical model. This is based on an engineering process viewpoint that has better application within stable plant systems, such as found in the petrochemical and nuclear industries (which undergo exhaustive generic hazard analysis of processes and systems prior implementation). The process is well suited for example, to support the introduction/integration of new plant equipment (e.g. Heat exchanger or catalytic cracker) within an oil refinery. A summary of common process methods of industry hazard identification has been collated by the European Process Safety Centre (EPSC, 2003) and includes commonly applied process industry techniques such as

- Hazard Identification (HAZID) or 'what if/What if checklist
- Hazard Operability (HAZOP)
- Fault tree analysis (FTA)
- Failure modes and effects analysis (FMEA)

## Operational Risk Management System for SMS and FRMS

- Event tree analysis (ETA)

Once generic hazard analysis and risk assessment is completed safety risk controls can be enabled overseen by the safety assurance function

ICAO (2008), however states that for SMS to function properly it requires a systematic and comprehensive hazard identification capability commensurate to the safety oversight requirements of the business model. This capability is essential within the cyclical SMS function to ensure the effective risk management function. SMS comprises a multilayer framework of tools to detect systemic hazards against the context of tasking within an airline. The ICAO (2008) Proactive Safety Strategy includes the following:

- *“Hazard and incident reporting systems that promote the identification of latent unsafe conditions*
- *Safety surveys to elicit feedback from front-line personnel about areas of dissatisfaction and unsatisfactory conditions that may have accident potential*
- *Flight data recorder analysis for identifying operational exceedances and confirming normal operating procedures*
- *Operational inspections or audits of all aspects of operations to identify vulnerable areas before accidents, incidents or minor safety events confirm a problem exists”*

The FAA’s focus has also now shifted onto a dynamic risk based approach to safety. The regulator will be looking at the effectiveness of regulations (compliance) as well as evaluating the SMS capability (safety performance) of an airline business model to meet its risk management requirements to an acceptable standard (Abbot and Bahr, 2008). The interpretation made by the EASA (EASA NPA 2009) and UK CAA as a National Aviation Authority (NAA) is for operators to focus on an SMS that is process orientated with a dynamic risk management capability. With the transition away from binary compliance operators are advised that they are directly accountable for their own risk and cannot legally defer to Safety Regulations as a form of protection. The focus within the CAA is to embrace the findings of the Hampton report (2005) such that the regulatory system as a whole should use comprehensive risk assessment to guide all aspects of regulatory lifestyle from data collection, inspection and prosecution.

This represents a paradigm shift in focus away from the traditional retrospective approach to safety management to require that operators proactively identify risk supported by application of data driven scientifically based risk management methods. A problem with current airline SMS is how hazard information, detected by multiple tools, can be commonly represented and interpreted against an operational process model. Such a model then supports Safety Risk Management and Assurance functions by facilitating an effective system assessment (identification of risk and ineffective safety controls). Also, information can be trapped within layers of bureaucracy and department silos limiting integrated functioning and organisation situational awareness and management of operational risks. A data driven approach to safety management requires that the SMS can identify factors that threaten to introduce risk to the operation and this requires a common database of information

from a variety of safety sources supported by analysis tools to elicit weak and strong safety trigger signals. This means the application of known risk scenarios and treatment, core analytical capability linked to investigation context (Frei et al 2003) and risk treatment action tracking, using safety performance metrics/indicators to support residual risk assessment (Basnyat et al 2005). The process must also support a dynamic feedback capability or performance evaluation.

Thus there is now a precedent set, by new regulatory approach to collate and integrate all SMS information sources into a single Information Management System (IMS). This IMS is supported by a comprehensive analysis capability using data-mining and statistical analysis tools to identify significant relationships within the data, indicative of risk in the system.

The relationship between safety risk management and safety assurance function in SMS should now be adapted (from the FAA (2006) approach, as cited in Stolzier et al (2008) p186) to reflect the focus on safety performance and dynamic risk assessment supporting a continuous improvement cycle.

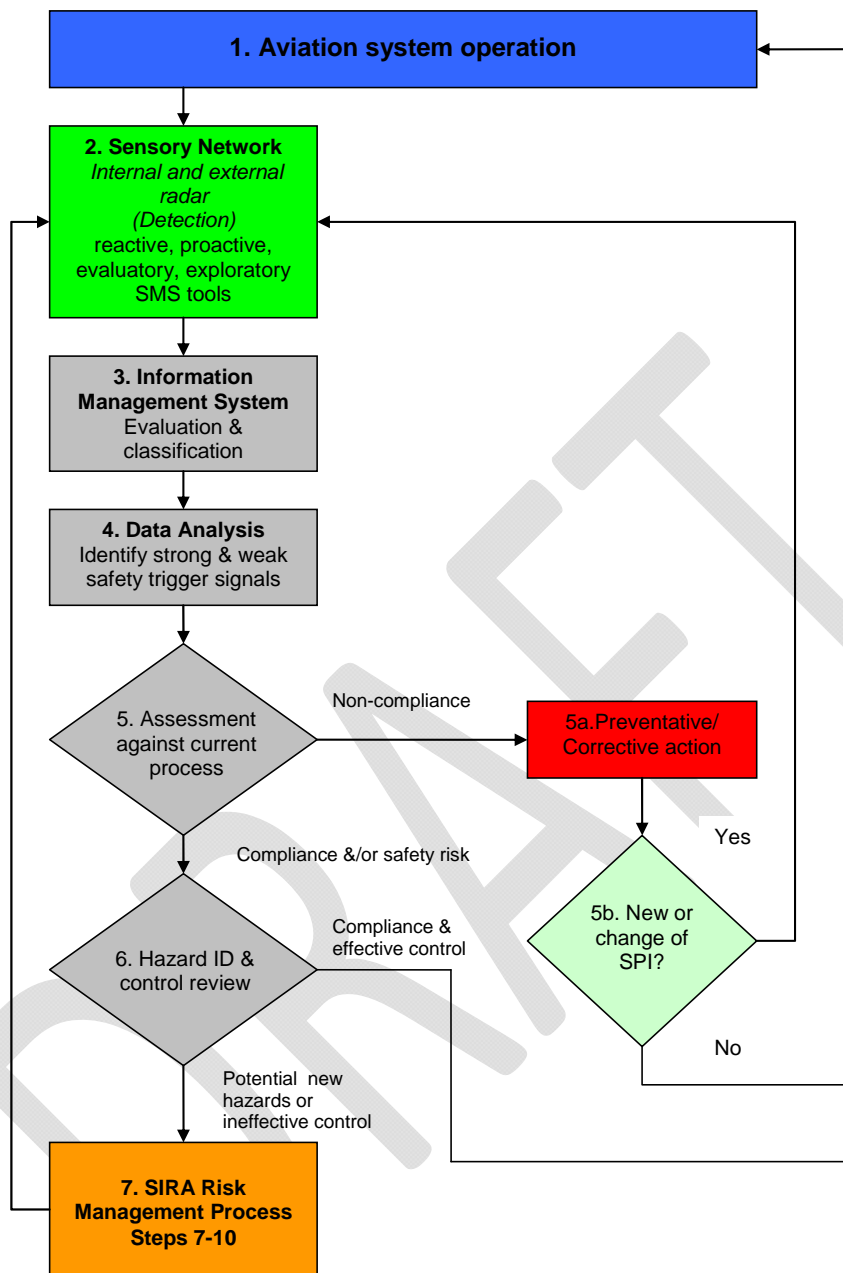
### **2.5.1 New SA/SRM conceptual process**

Figure 9 depicts the relationship between safety risk management and safety assurance for an airline operation.

The steps of the process are as follows:

1. The network of aviation system processes that describe the airline is represented by the first box.
2. The sensory network Stage two is the detection stage where the sensory network or risk radar for the organisation encompasses capability from the five risk logics (reactive, proactive, time critical, exploratory and evaluatory). The sensory network draws information sources from many system sources inclusive of surveys, Air Safety Reports (ASR), Line Operations Safety Audits (LOSA™), confidential reporting and Flight Data Monitoring (FDM).
3. The Safety data team collate the SMS information (safety and quality) from the detection system into one information management system (IMS) that facilitates data storage for safety reports, investigations and quality audit reports, surveys, losa reports and the tracking of accountability and actions implemented from the risk management process.

## Operational Risk Management System for SMS and FRMS



**Figure 9.** SIRA Safety Risk Management and Safety Assurance process

4. The information management system is centred on a method classification event model with an integral statistical capability and is the information source from which system performance trends are generated. The IMS is linked into the prime data sources to facilitate incident investigations and process evaluation within safety and quality. The data analysis produces weak and strong safety trigger signals filtered from the operational background noise.

5. The analysis and evaluation of these safety signals in the context of the operational process model is conducted by investigators to determine either non-compliance or compliance to existing processes and/or possible safety hazards. Non-compliance (5a) with prescribed criteria leads to initiation of corrective and preventative measures and where required, a review (5b) of activity and outcome based safety performance indicators to support monitoring process. The process then has a closed feedback loop to the aviation system operation.
6. The fact that compliance with existing process requirements (targets/thresholds) occurred does not ensure the effectiveness of the control. An evaluation of the control and supporting risk assessment in the OPM should be conducted to review its effectiveness and applicability in the operational environment. Compliance and identification of the controls relevance and effectiveness in the system then follows a feedback closed loop to the aviation system operation stage. Ineffective controls (e.g. organisational memory risk assessments supporting the control are no longer valid) and safety trigger signals that represent possible hazards are identified at this stage for processing through the SIRA risk management process (Risk investigation steps 5-7).
7. SIRA Risk Management Process: The output from the SIRA process will be a risk assessment supporting a new or modified system control. Risk assessments are log in organisational memory linked to the operational process model. The process feeds back into the sensory network for continuous Safety Risk Management activity.

### 3.0 Summary

This document has focused on HILAS innovation in SMS based on the introduction of a dynamic Risk Management System incorporating the principles of Organisational Learning and Memory and Resilient Safety Culture. It also presents a modified approach to the integration of safety risk management and safety assurance in SMS. The dynamic Risk Management System presented incorporates an SMS sensory network that scans the operational environment for safety trigger signals by employing a multilayer risk detection capability (reactive, proactive, exploratory, evaluatory and time critical) that expands on the ICAO (2008) approach. The RMS model demonstrates an integrated information management system supported by data-mining and statistical tools that delivers processed and ranked safety trigger signals to airline risk investigators. Risk assessment and reduction activity centres on tactical and strategic processes and change management activity supporting a continuous improvement cycle based on compliance (effective controls) and safety performance measurement. This capability builds on ICAO guidance and delivers a practicable application process to an airline SMS. It is now being implemented into a major European LCC.

It is recognized that airlines do not have the resources, manpower or time to develop system tools and processes for future SMS evolution. Academic institutions can combine

## Operational Risk Management System for SMS and FRMS

with Regulators and Operators to facilitate the development and implementation of practical processes based on sound theoretical concepts of risk assessment and management (Chien-tsung & Bos, 2007). HILAS exemplifies such a coordinated relationship. Not knowing or being unaware of the risk does not mean you are not accountable (Corporate Manslaughter and Corporate Homicide Act (c19) (2007)).

Complex systems require effective communication and control capability to facilitate resilience and adaptability to change. Airlines need to respond to market risk as a cohesive whole, with the elements of the organisational structure functioning with both autonomy and synchronicity towards strategic objectives. Airline business models represent safety-critical enterprises and require a dynamic risk management system capability such as the HILAS SIRA process to direct the operation towards achieving viability and acceptable safety (Espejo & Harnden, 1989). This requires the embodiment of the principles of self-governance, risk ownership, management by objectives, process mapping/modelling and dynamic risk representation of the company safety boundary.

The message to the industry is to focus on internal self-governance (Turnball report, 1999) where good operators can achieve earned autonomy and reduction in fees to the regulator. This is in the operators prime interest as the insurance industry now links premiums against risk signature and capability of an airline SMS to detect and manage risk. For an operator to achieve this, the SMS must be tailored to the risk needs of the business model.

Organisational failure to address these issues can result in reduced competitive capability, operational integrity, profit margin and Return-on-Equity. It is all underpinned by strategic clarity, good leadership, sound planning, operational process knowledge, innovation and correct resourcing (resource at the right place and time).

## References

Abbott, R and Bahr, N. (2008) How safety oversight can improve the aviation industry's safety record. Intl System Safety Regional Conference 2008, 23-25 April, Singapore.

Akselsson, R., Koornneef, F. Stewart, S and Ward, M. (2009) Resilient Safety Culture in Aviation organisations. HILAS Document.

Argyris, C., Schön D.A. (1974) *Theory in Practice: increasing professional Effectiveness*. Jossey-Bass, San Francisco, USA

Basnyat, S., Chozos, N., Johnson, C., and Palanque, P. (2006) Incident and Accident Investigation Techniques to Inform Model-Based Design of Safety-Critical Interactive Systems. In Interactive Systems. Springer, LNCS 3941, pp. 51-66.

Beauchamp, E. (2007) Towards integrated decision making for adaptive learning. Proceedings of ESREL 2007 Safety & Reliability Conference ISBN 978-0-415-44786-7, pp 1301-1307.

Chien-tsung, L., Bos, P. (2007) System Safety Application: constructing a comprehensive aviation system safety management model. International Journal of Applied Aviation Studies, vol 1 (2007).

Civil Aviation Authority (CAA) (2007) Risk Assessment Research Project (Draft). Flight Operations Research Centre of Excellence. Cranfield University School of Engineering. UK.

Corporate Manslaughter and Corporate Homicide Act (c19) (2007) Ministry of Justice UK.

Crawley, F. and Tyler, B. (2003) Hazard Identification Methods. European Process Safety Centre. IChemE

Dijkstra, A. (2006). Safety Management in Airlines. In Hollnagel, E., Woods, D. & Leveson, N. (eds.). *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing Ltd: Aldershot, UK.

Ek, Å. & Arvidsson, M., (2009). Proactive Identification of Work and Situational Factors That Can Affect Safety in Air Traffic Control. Proceedings of 17<sup>th</sup> World Congress on Ergonomics. International Ergonomics Association 2009, August 9-14, 2009, Beijing, China

European Aviation Safety Agency (EASA). Notice of Proposed Amendment (NPA) No 2009-02c. January 30. 2009

## Operational Risk Management System for SMS and FRMS

Espejo, R. & Harnden, R. (1989) *The viable systems model-interpretations and applications of Stafford Beer's VSM*, Wiley, Chichester.

Flin, R., 2003. *Danger men at work: Management influence on safety*. *Human Factors and Ergonomics in Manufacturing*, 13 (4), 261-268

Frei, R., Kingston, J., Koornneef, F and Schallier, P. (2003) *Investigation tools in context*. JRC/ESReDA Seminar on Safety Investigation of Accidents, Petten, Netherlands, 12-13 May.

Turnbull, N (1999): *Internal control -Guidance for directors on the combined code*. Institute of Chartered Accountants. September.

Hampton, P. (2005) *Reducing administrative burdens: effective inspection and enforcement*. HM Treasury Report

Hilburn, B., Flynn, M. (2001). *Air traffic controller and management attitudes towards automation: an empirical investigation*. 4th USA/Europe Air Traffic Management R&D Seminar, 3–7 December, Santa Fe, USA.

ICAO (2008). *Safety Management Manual (SMS)*, Second edition. International Civil Aviation Organisation. Doc 9859. Retrieved March 11, 2009, from <http://www.icao.int/icao/en/download.htm#Docs>

Koornneef, F., Hale A.R. (2004a) *Organisational Learning and Theories of Action*. In: Andriessen, J.H., Fahlbruch, B. (eds.) *How to Manage Experience Sharing - from Organisational Surprises to Organisational Knowledge*. Elsevier Science, Amsterdam.

Koornneef, F., Hale A.R. (2004b) *Organisational Memory for Learning from operational Surprises: Requirements and Pitfalls*. In: Andriessen, J.H., Fahlbruch, B. (eds.) *How to Manage Experience Sharing - from Organisational Surprises to Organisational Knowledge*. Elsevier Science, Amsterdam.

Koornneef, F., Stewart, S., Akselsson, R and Ward, M. (2009) *Organisational Learning & Organisational Memory Framework*. HILAS draft chapter.

Lintner, T. and Smith, S.D. (2008) *Future concepts for measuring aviation safety, performance and effectiveness*. Intl System Safety Regional Conference 2008, 23-25 April, Singapore.

O'Toole, M. (2002). *The relationship between employees' perceptions of safety and organisational culture*. *Journal of Safety Research* 33, 231–243.

Reason, J., (1997). *Managing the risks of organisational accidents*. Ashgate, Aldershot, UK

Reason, J. (2008). *The human contribution – unsafe acts, accidents and heroic recoveries*. Ashgate, Farnham, UK

## Operational Risk Management System for SMS and FRMS

Rundmo, T., Hale, A. (2003). Managers' attitudes towards safety and accident prevention. *Safety Science* 41, 557-574

Stewart, S., Koornneef, F., Akselsson, R., Kingston, J. and Stewart, D. (2009) Aviation Incident Investigation Process. HILAS draft chapter

Stewart, S., Holmes A., Jackson P. and R. Abboud (2006) *An integrated system for managing fatigue risk within a low cost carrier*. 59th Annual International Air Safety Seminar (IASS) October 23-26, 2006 Paris, France.

Stewart, S., Holmes, A. and McDonald, N. (2008) *An Aviation Fatigue Risk Management System*. Proc. International System Safety Regional Conference (ISSRC 2008), Singapore.

Stolzer, A.J., Halford, C.D. and Goglia, J.J. (2008) *Safety management Systems in Aviation*. Ashgate

Thompson, R. C., Hilton, T.F., Witt, L. A., (1998). Where the safety rubber meets the shop floor: a confirmatory model of management influence on workplace safety. *Journal of Safety Research* 29, 231–243.

von Thaden, T and Wiegmann, D (2004), *Measuring Organisational Factors in Airline Safety*

Weick, K.E. and Sutcliffe, K.M. (2007) *Managing the Unexpected – Resilient Performance in an Age of Uncertainty*. 2<sup>nd</sup> Edition. Jossey-Bass, San Francisco, USA.

Shell (2007) “*Find out how our 50 years' experience in optimising refineries can help improve your bottom line*”, Royal Dutch Shell Group Global Solutions web page, Top Solutions, November 26<sup>th</sup> 2007, 1200hrs