# Incident Investigation in SMS and FRMS

*S. Stewart, F. Koornneef, R. Akselsson, J. Kingston, D. Stewart*

EARLY DRAFT of HILAS Book Chapter

## Table of contents PAGE

**1 INCIDENT INVESTIGATION PROCESS ........ 3**

1.1 PURPOSE ........ 3

1.2 BACKGROUND ........ 3

1.3 ANALYTICAL TOOLS THAT SUPPORT AN INVESTIGATION PROCESS ........ 4

1.4 CHOOSING ANALYTICAL TOOLS TO ASSIST INVESTIGATION OF RISK ........ 6

1.5 AN INVESTIGATION 'ENGINE' FRAMEWORK TO FOR AN RMS ........ 8

1.6 HILAS AIRLINE INVESTIGATION PROCESS IN SIRA RMS ........ 11

1.7 CORE TOOLS DESCRIPTION ........ 18

*1.7.1 Description of ECFA+ ........ 18*

*1.7.2 Control Change Cause Analysis – 3CA ........ 19*

REFERENCES ........ 22

# 1 Incident Investigation Process

## 1.1 Purpose

The objective of the HILAS SMS working group is to develop an incident investigation method that was capable of delivering a user friendly (can be used by any Safety Officer), time efficient, reliable, procedural, repeatable, scalable, diagnostic and comprehensive investigative methodology for any member of an airline safety department to use as an investigative tool for any incident that may arise within flight, ground and/or engineering operations.

## 1.2 Background

The purpose of an investigation into an incident or accident is to determine what happened, why it happened, and what needs to be done to prevent a reoccurrence (Sklet, 2002). This process fits well with the concept of organisational learning (systemic risk detection, notification, inquiry and organisational adjustment) supported by organisational memory (directives, protocols, manuals, training programs) (Koornneef & Hale, 2004). The investigation process sequences into the Risk Management System (RMS) of an airline SMS. The investigation process can be represented by the steps of an industry validated investigation framework (DOE., 1999) and include the following evidence gathering (collect, preserve and verify); data integration organisation and analysis (facts and evidence) to determine causal factors, evaluation of causal factors in a system context, conclusions and recommendations (judgements of need); conduct a requirements verification analysis on the system and presentation of a structured report.

The findings of the investigation process identify direct cause, contributory factors and root causes (DOE, 1999). These findings need to be assessed for systemic risk implications (identification, evaluation and analysis) before risk reduction (decision making, implementation and monitoring) activity can occur (Figure 1, International Electrotechnical Commission (IEC), 1995). An application of risk assessment in an airline RMS, supported by an investigation process is to satisfy existing regulatory requirement or to support an evidenced based derogations from safety certification standards (Stewart & Abboud, 2005; Harvey, 1985).

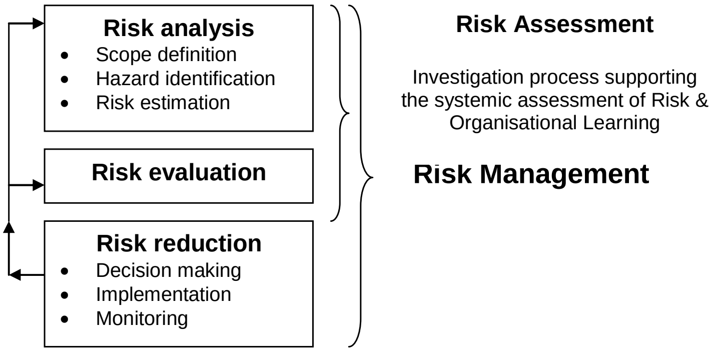


**Figure 1**. Risk Management Process (IEC, 1995)

This concept is embodied within the Systems Integrated Risk Assessment (SIRA) (Stewart et al, 2008 & Stewart et al, 2009a) Risk Management System (RMS) 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. 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 and analytical capability can be directed at risk analysis and systemic evaluation of these signals. The role of the investigator supported by analytical investigation tools (or toolset) and data management and confidentiality protocols (refer Chapter X, Resilient Safety Culture) 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.

The binding concept that establishes the role of risk investigation in risk management activity is (organisational) LEARNING. 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).

## 1.3 Analytical tools that support an investigation process

There are a number of capable incident and accident investigation models developed and verified within the Marine, Nuclear, Rail, and Aviation industries. There exist a suite of different methods in investigation literature for the analysis of evidence and facts and these can consist of sequencing methods, root cause analysis and methods of hypothesis generation (Sklet, 2002; Frei et al, 2003). The SINTEF 5 step model of accident causation (Arbeidsmiljosenteret, 2001-as cited in Sklet (2002) p23) gives an example of the application domains of where investigative tools can be applied in context of an investigation framework. The model starts with the identification of event sequences before the accident (application of sequencing tools) followed by the next step that identifies deviations and failures that lead to the accident (analytical tools). Steps 3 to 5 identify weakness and defects in management systems, top management of the company and lastly possible deficiencies in regulation and laws. Each domain has a different context for the application of tools to support the efficiency and effectiveness of the investigation (Frei et al, 2003).

The application of these sequencing processes and analysis techniques provides the foundation to the investigation approach and the tool selection is adapted to the context of the event investigation requirement. Sequencing processes provide a proceduralised, systematic and structured framework to provide context to the incident or accident event. Commonly employed techniques (summarised in Livingston et al (2001), HSE Root Cause Analysis Review 325/2001 (HSE, 2001) and ROSS 2002.08 (NTSU) Sklet (2002)) consist of Events and Causal Factors Charting (ECFC), Management Oversight Risk Tree (MORT)(Knox & Eicher, 1992), Sequenced Timed Events Plotting Procedure (STEP); Multi linear events sequencing (Hendrick & Benner, 1987) and Events and Conditional Factors Analysis (DOE, 1999). These sequencing techniques can be used in conjunction with analysis techniques that can be employed to ascertain the direct and contributory causes around critical events. Commonly employed techniques include Barrier Analysis (Kingston and Koornneef, 2004; DOE, 1999), Change Analysis (DOE, 1999), Event trees, Fault Tree Analysis and Control Change Analysis (Kingston, 2007). These techniques are considered to be the foundation or building blocks of the investigation process. The combination of these techniques provides a capability to determine root causes in an objective, structured and systematic manner but fall short on providing guidance on how to correct the system (Basynat et al, 2005).

The relationship of the investigation 'toolbox' to the risk management process can be demonstrated (Figure 2) where analytical tools applied in context by investigators to a particular task to support the effectiveness of safety investigation and risk management activity. The next step is to facilitate the investigator in the selection and application of suitable tools to support the quality, scope and depth of inquiry within operational time constraints.

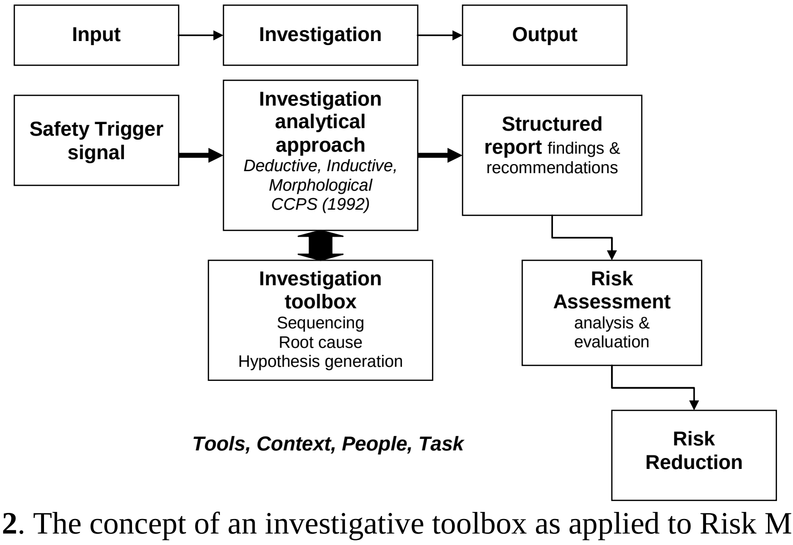


**Figure 2**. The concept of an investigative toolbox as applied to Risk Management (adapted from Frei et al, 2003)

## 1.4 Choosing analytical tools to assist investigation of risk

This section describes a rationale for selecting analytical tools for incident/accident investigation. The section is written with the investigation programme manager in mind, the person who has to provide a corporate toolkit for the investigators in their organisation. The rationale starts with the basic choice between proprietary tools and those in the public domain; the proprietary tools are not discussed thereafter. The rationale continues by considering investigative context, then the type of task to be performed and concludes with a discussion of individual preferences and the need to accommodate these.

Analytical tools can support accident investigation. These tools are sets of rules and procedures for creating descriptions of accidents from particular points of view. Physical tools exploit principles such as mechanical leverage, whereas analytical tools use principles drawn from logic and from theories of accident causation. Like their mechanical counterparts, analytical tools have little in-built protection from misuse: decision-makers must take care when equipping a corporate toolbox, just as investigators must when selecting and applying particular tools.

There are many reasons for using tools but, in general, using a tool confers some advantage on the user by making their work possible, or easier, or by improving the quality of the finished product. This logic applies to analytical tools as well; if the user is not getting much advantage from using a tool, they will prefer to use something else, or nothing at all.

However, there are arguments for using tools other than the advantages to the investigator who uses them. These include, promoting: efficacy in an investigation; consistency across investigations; transparency of reasoning; thoroughness of search; communication within the investigation team and with others. These reasons are often more appealing to the manager than to the user, and organisations who want to secure these advantages need to recognise this.

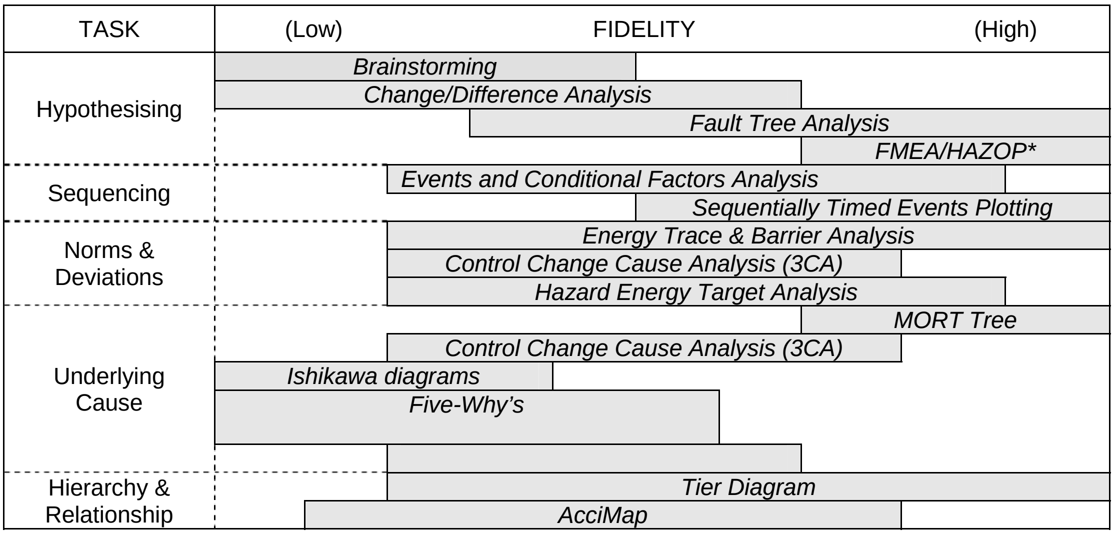
When equipping a corporate analytical investigation toolbox, the first decision is whether to pay for tools or use those available for free in the public domain. Proprietary tools often come as ready-made toolboxes and frequently achieving integration of the constituent tools via software implementation. The software aspect is a strong selling-point, and very few analytical tools in the public domain are computerised. So, in effect, the choice here is between automated and manual tools. Although software has many attractions, these have to be balanced against four main drawbacks. First, it is difficult to know quite how complete the toolbox is. Second, the user may have only limited control over the logic and process used by the tool. Third, the superficial quality, the gloss as-it-were, of automated output can sometimes obscure poor quality input: GiGo applies; garbage in, garbage out. Fourth, software may also discourage the user from developing a deep insight into how the tools work, the assumptions made by their designers and the limitations these entail. Without this insight, there is a danger that the tool becomes the master, not the servant.

The choice of analytical tools needs also to accommodate the degree of confidence needed in the findings of the investigation. By and large, confidence correlates with potential severity: the more serious the accident, the greater will be the appetite to invest resources in an investigation[1]. This idea of "degree of confidence" might be expressed more easily as fidelity. High-fidelity tools are designed for use in meticulous investigations of high-consequence events. It is still possible to use high-fidelity tools in investigations of low-risk events, but there would have to be an exceptional reason for using a heavy tool on a light task. Similarly, low-fidelity tools, which are designed to provide quick, meaningful labelling of low-risk events, have little to offer in investigation of a major accident. However, these are the extremes and some tools are sufficiently flexible to allow them to be useful across a range, although not the full spectrum; one tool does not fit all.

The two selection processes mentioned (public domain or proprietary, low- or high-fidelity) effectively define the type of analytical toolbox. The next decision is about selecting a tool from the toolbox to fit the task in hand. Frei et al. (2003) suggest that there are four types of analytical task: (i) forming hypotheses; (ii) organising information sequentially; (iii) identifying norms and deviations, and; (iv) identifying underlying cause.

For each of these tasks, a selection of tools exists in the public domain. In table 1 these are laid out in order of relative fidelity, estimated from the author's experience of use and theoretical knowledge.

**Table 1.** Analytical tools available for free in the public domain by type of task and fidelity (estimated).



| TASK | (Low) FIDELITY (High) |
|---|---|
| Hypothesising | Brainstorming |
| | Change/Difference Analysis |
| | Fault Tree Analysis |
| | FMEA/HAZOP* |
| Sequencing | Events and Conditional Factors Analysis |
| | Sequentially Timed Events Plotting |
| Norms & Deviations | Energy Trace & Barrier Analysis |
| | Control Change Cause Analysis (3CA) |
| | Hazard Energy Target Analysis |
| Underlying Cause | MORT Tree |
| | Control Change Cause Analysis (3CA) |
| | Ishikawa diagrams |
| | Five-Why's |
| | |
| Hierarchy & Relationship | Tier Diagram |
| | AcciMap |

FMEA = failure Modes & Effect Analysis
HAZOP = Hazard and Operability study
MORT = Management Oversight & Risk Tree analysis

[1] There are exceptions to this rule; high-reliability organisations share a "pre-occupation with failure" even when these failures are small, and they have "a reluctance to accept simplifications" (Weick and Sutcliffe, 2007; pages 9-10).

* Note: FMEA (Failure Modes and Effects Analysis, and HAZOP (Hazard and Operability studies) are limited to use in particular technical contexts, the other tools in this category are truly general).

The implication of table 1 is that at most levels of fidelity there exists more than one tool that can do the task. The width of the grey bars represents the author's estimate of the range of fidelity in practice (e.g. the reliability of the tool given different users and contexts). This is something of a simplification: the tasks described have nuances and these will reflect in the choice of the tool. For example, in relation to hypothesis formation, Change Analysis is good at producing insight into obscure causes (i.e. things the investigator is unaware of) in a way that FTA (Fault Tree Analysis) is not. On the other hand, FTA is good for generating different scenarios for evaluation when the available evidence is not clear; something that Change Analysis does not do.

Once the nuances of the task are understood, any choice remaining depends on the preferences of the people who equip the corporate investigative toolbox and the preferences of the investigators - the users - themselves. For example, there can be an overlap between investigative tools in terms of their fidelity as tools to assist analysis of underlying causes. However, the tools are very different and evoke very different reactions from would-be users. Some users like the structure provided by a checklist-driven method, as for others, this is a laborious burden. Some users like the focus given by an event-driven method like 3CA, others can find this too confining and prefer to think holistically and to reach insights intuitively.

The challenge for managers of investigation programmes, the corporate providers of tools and toolboxes, is to accommodate the range of investigative contexts, the variety of investigative tasks and the diversity of investigators. It is generally wise to leave some flexibility to the investigator, simply because the creativity and insightfulness of the analyst is valuable and easily discouraged by insisting on a tool which, from the user's point of view, does not fit. Managers have understandable qualms about reliability; they want the outcomes of an investigation to be contingent on the facts, not on the characteristics of the investigator. However, whilst tools can help provide some degree of consistency they can only ever be servants.

## 1.5 An investigation 'engine' framework to for an RMS

The HILAS SMS working group have reviewed and examined current incident methods to identify if any aspects of those methods could be combined to create a new incident analysis technique suitable for application by an 'average' safety officer. It has been established that a 'one-size-fits-all' approach to incident investigation may not be adequate and that a combination of analysis methods is necessary to ensure that all aspects of an incident are investigated and analysed fully.

The incident investigation process comprises a set of standardised steps, sequenced into the RMS (SIRA steps 5 to 7) that are designed to guide the investigator through the analysis to aid in the identification of applicable contributing factors. A framework was developed based on the concept demonstrated in Figure 2 that consists of a selection of core sequencing and analysis techniques (of sufficient fidelity and ease of application by an airline safety officer) integrated into a representational and classification process to suit an airline requirement (Figure 3). The Incident investigation process baseline capability uses complementary steps from Case Based Reasoning (Aamodt & Plaza 1994), Event and Conditional Factors Analysis (ECFA+)(Kingston et al, 2006) and Control Change Cause Analysis (3CA) (Kingston, 2007) techniques sequenced with representation via the Bowtie model and integrated (codification) into the Human Factors Aviation Classification System (Weigmann & Shappell, 2001) creating a combined method of analysis.

The Case Based Reasoning (CBR) (Aamdt & Plaza 1994) process 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. The investigator is not constrained to the employment of the baseline capability to every investigation. Where required, a scalable or alternate investigation 'toolset' capability can be selected to suit the context of the investigation and this stage is facilitated by access to an investigation toolbox of context related analytical tools such as: Investigative interviews, Predictive Fatigue Modelling programs, System Fatigue performance metrics, Sleep diary's/actigraphy, Fatigue questionnaires, Fatigue performance testing, Fault tree analysis, Barrier analysis, Change analysis; Why-be-cause-analysis (WBA); Management Oversight Risk Tree (MORT) etc..). This tool selection and application process employs the tool/context/people/task/ouput concept from Frei et al (2003). The toolbox includes a users guide as to the application of analytical capability in context and depth, sensitivity and degree of resolution required to support the investigation (note this capability is dependent on operational readiness and training). The concept of tool resolution to task supporting system resilience and operationl readiness to respond is established by the fact that weak safety rigger signals require a 'mindful' organisation and investigative capability (Weick & Sutcliffe "Managing the Unexpected", 2$^{nd}$ edition, 2007). Weick & Sutcliffe stress that a 'mindful' infrastructure continually a) tracks small failures (weak signals), b) resist oversimplification, c) is sensitive to operations, d) maintains capabilities for resilience, and e) takes advantage of shifting locations of expertise. Resilience then comes in as a notion that is linked with containment of the emerging problem and return to normal operation.

At the completion of the investigation results (structured report) are encoded within the Aviation Quality Database to support system safety stewardship through datamining (case based reasoning and event trending) and the notification, tracking and assignation of actions/responsibility to accountable management levels. Particular emphasis needs to be placed on the report format, content and structure. Good investigations are wasted on badly written reports and the purpose of the investigation to prevent reoccurrence of an incident can be compromised (Hendrick and Benner, 1987). The process facilitates investigating officer's access to risk solutions from other system investigations under the CBR process. This process links the investigation to business context into the risk management cycle for the operation. The investigation sponsor reports back to the business (process owner) at each stage of the investigation process to maintain feedback and open communication.

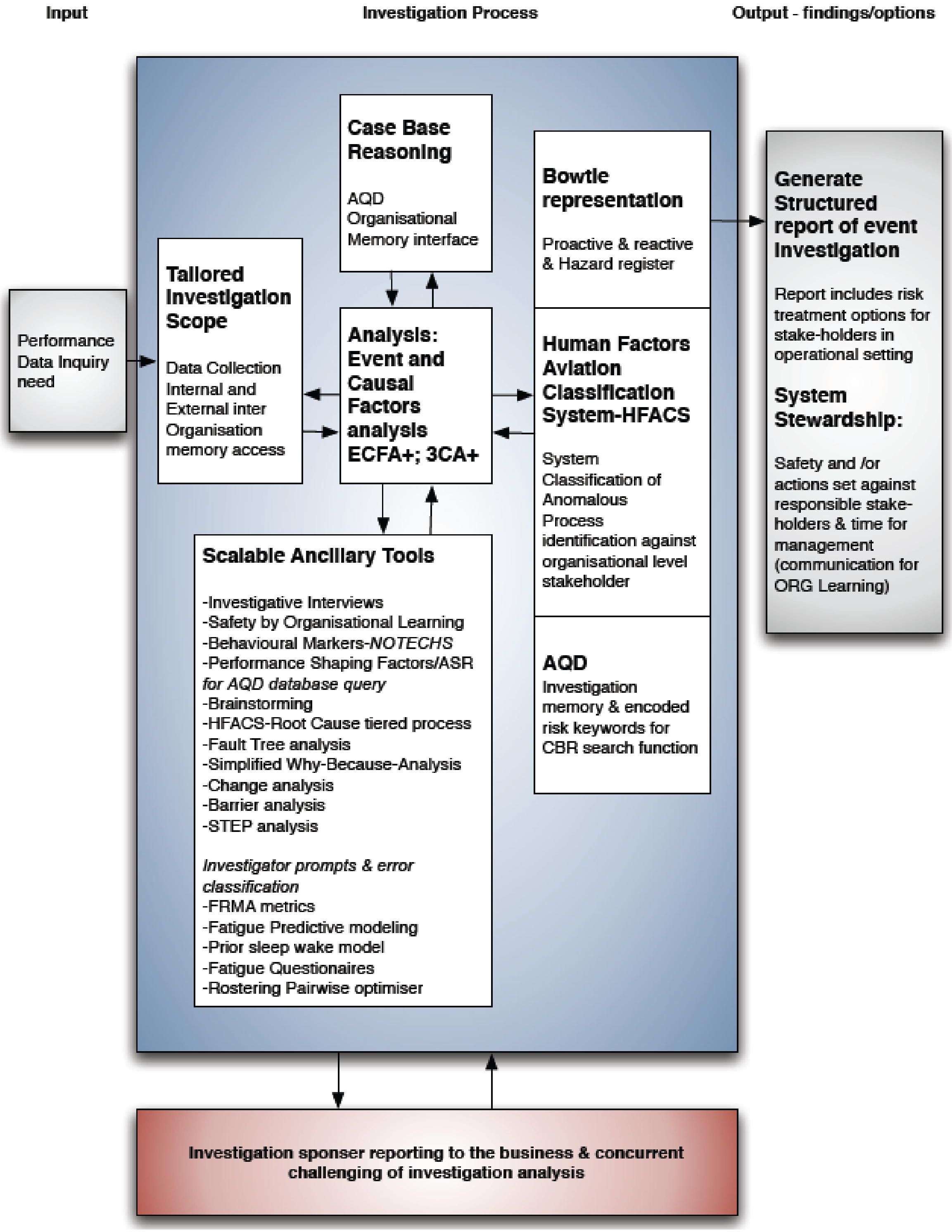

Input
Investigation Process
Output - findings/options
Performance Data Inquiry need
Tailored Investigation Scope
Data Collection Internal and External inter Organisation memory access
Case Base Reasoning
AQD Organisational Memory interface
Analysis: Event and Causal Factors analysis ECFA+; 3CA+
Bowtie representation
Proactive & reactive & Hazard register
Human Factors Aviation Classification System-HFACS
System Classification of Anomalous Process identification against organisational level stakeholder
AQD
Investigation memory & encoded risk keywords for CBR search function
Scalable Ancillary Tools
-Investigative Interviews
-Safety by Organisational Learning
-Behavioural Markers-NOTECHS
-Performance Shaping Factors/ASR
for AQD database query
-Brainstorming
-HFACS-Root Cause tiered process
-Fault Tree analysis
-Simplified Why-Because-Analysis
-Change analysis
-Barrier analysis
-STEP analysis
Investigator prompts & error classification
-FRMA metrics
-Fatigue Predictive modeling
-Prior sleep wake model
-Fatigue Questionaires
-Rostering Pairwise optimiser
Generate Structured report of event Investigation
Report includes risk treatment options for stake-holders in operational setting
System Stewardship:
Safety and /or actions set against responsible stake-holders & time for management (communication for ORG Learning)
Investigation sponser reporting to the business & concurrent challenging of investigation analysis

**Figure 3.** Investigation core capability framework

The investigation process sequences between steps 5 and 10 of the General Incident Management process and further specification is required from the investigator as to the tool directory content and the risk representation process. This also sequences into the steps 5 to 7 of the SIRA risk management process. The aim is to articulate backwards from the abstract to the evidence (data). This ensures the investigating officers are servants to the process and avoid 'tick-box Chinese dictionary' investigation practices.

## 1.6 HILAS Airline Investigation Process in SIRA RMS

Steps 6 and 7 in the Risk Management process of the SMS described in Chapter X (RMS) are the entry points for investigation if the need is indicated. This section describes the steps in such an investigation process as is has been developed and implemented in an airline, and has been depicted in Figure 4

1. Event detection from the system sensory network incorporating capability within the four-risk logic domains – reactive, proactive, exploratory and evaluatory. SMS detection capability extends from safety reports of incidents, surveillance audits, process audits (internal quality control & external quality assurance), confidential reports, FOQA data, process performance monitoring metrics and exploratory hazard investigations of systematic factors that alter the balance between safety and performance criteria. Access will also be made to external databases to identify risk solutions or trends that may support the investigation process, i.e. US FAA ASIAS program. This process demonstrates access to inter-organisational memory. The investigation process will also incorporate random event investigations so as not to demonstrate dependence on the detection capability generated against known risk.

2. The Safety Data Team (SDT) collates 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. LOSA and Survey reports including hazard ID are forwarded to respective manager. The information management system (IMS) 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. Information sources comprise: FOQA, training records, schedule information, flight plans, technical records, ATC radar and voice tapes, witness interviews, confidential reports, human resources (personal records), FRMS and external databases (ASIAS, GAIN, STEADES etc).

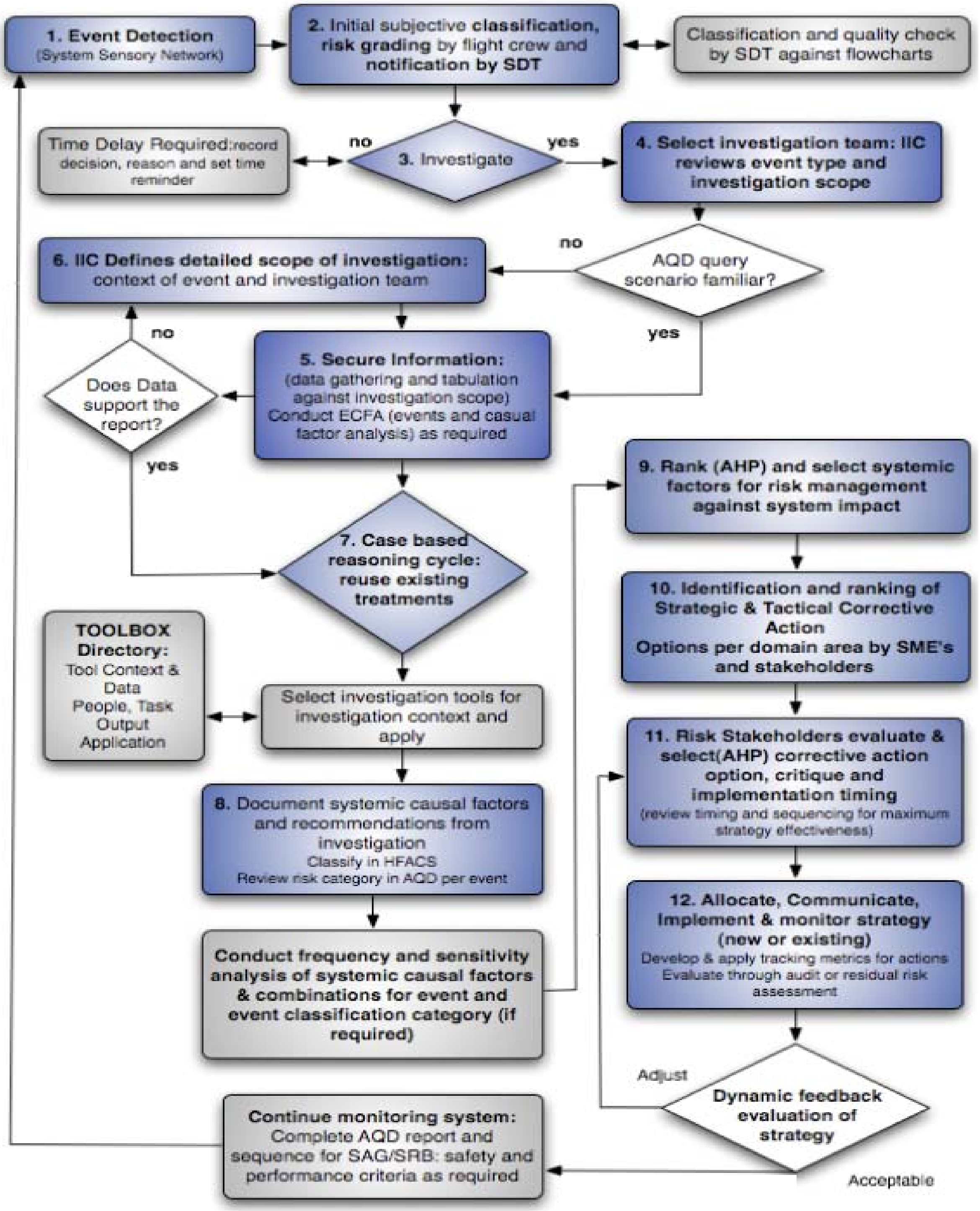
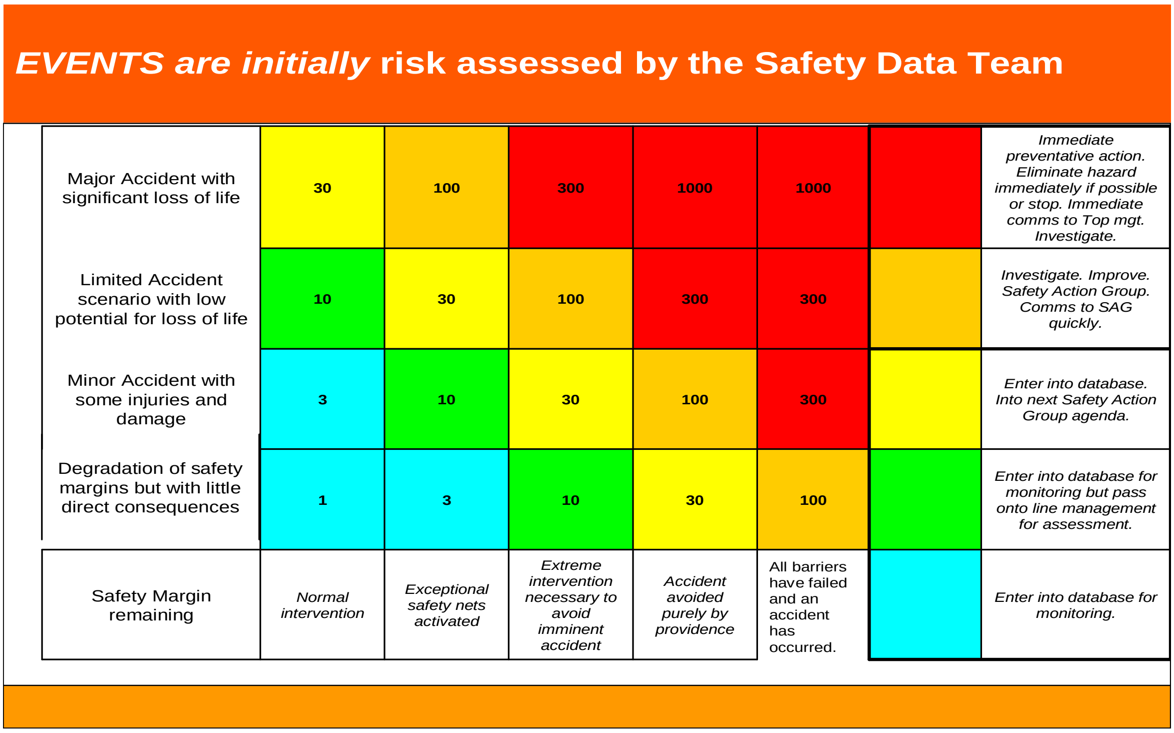

1. Event Detection
(System Sensory Network)
2. Initial subjective classification, risk grading by flight crew and notification by SDT
Classification and quality check by SDT against flowcharts
Time Delay Required: record decision, reason and set time reminder
no
3. Investigate
yes
4. Select investigation team: IIC reviews event type and investigation scope
no
6. IIC Defines detailed scope of investigation: context of event and investigation team
AQD query scenario familiar?
yes
no
Does Data support the report?
5. Secure Information:
(data gathering and tabulation against investigation scope)
Conduct ECFA (events and casual factor analysis) as required
yes
9. Rank (AHP) and select systemic factors for risk management against system impact
7. Case based reasoning cycle: reuse existing treatments
10. Identification and ranking of Strategic & Tactical Corrective Action
Options per domain area by SME's and stakeholders
TOOLBOX Directory:
Tool Context & Data
People, Task Output
Application
Select investigation tools for investigation context and apply
11. Risk Stakeholders evaluate & select(AHP) corrective action option, critique and implementation timing
(review timing and sequencing for maximum strategy effectiveness)
8. Document systemic causal factors and recommendations from investigation
Classify in HFACS
Review risk category in AQD per event
12. Allocate, Communicate, Implement & monitor strategy (new or existing)
Develop & apply tracking metrics for actions
Evaluate through audit or residual risk assessment
Conduct frequency and sensitivity analysis of systemic causal factors & combinations for event and event classification category (if required)
Adjust
Dynamic feedback evaluation of strategy
Continue monitoring system:
Complete AQD report and sequence for SAG/SRB: safety and performance criteria as required
Acceptable

**Figure 4.** Airline Investigation Process

Incoming reports are risk classified by the reporter through a 4x4 matrix based on severity and defences/barriers breached (figure 5). This is then reviewed by the safety data team with domain experts through application of 70 event process flowcharts updated monthly within flight, ground and engineering areas (Figure 6 as part of the triage step. Domain experts assist the safety data team (SDT) in the initial risk assessment phase before the reports are disseminated to respective managers for the decision to investigate. A tool to facilitate the initial risk assessment is critical incident technique within the business process model to determine which events/hazards are linked to critical business processes. Investigations can be triggered through identified hazards from LOSA, FRMS and FOQA data where no safety report has been filed. Such an investigation may require the completion of a safety report by the responsible individuals/crew where applicable.

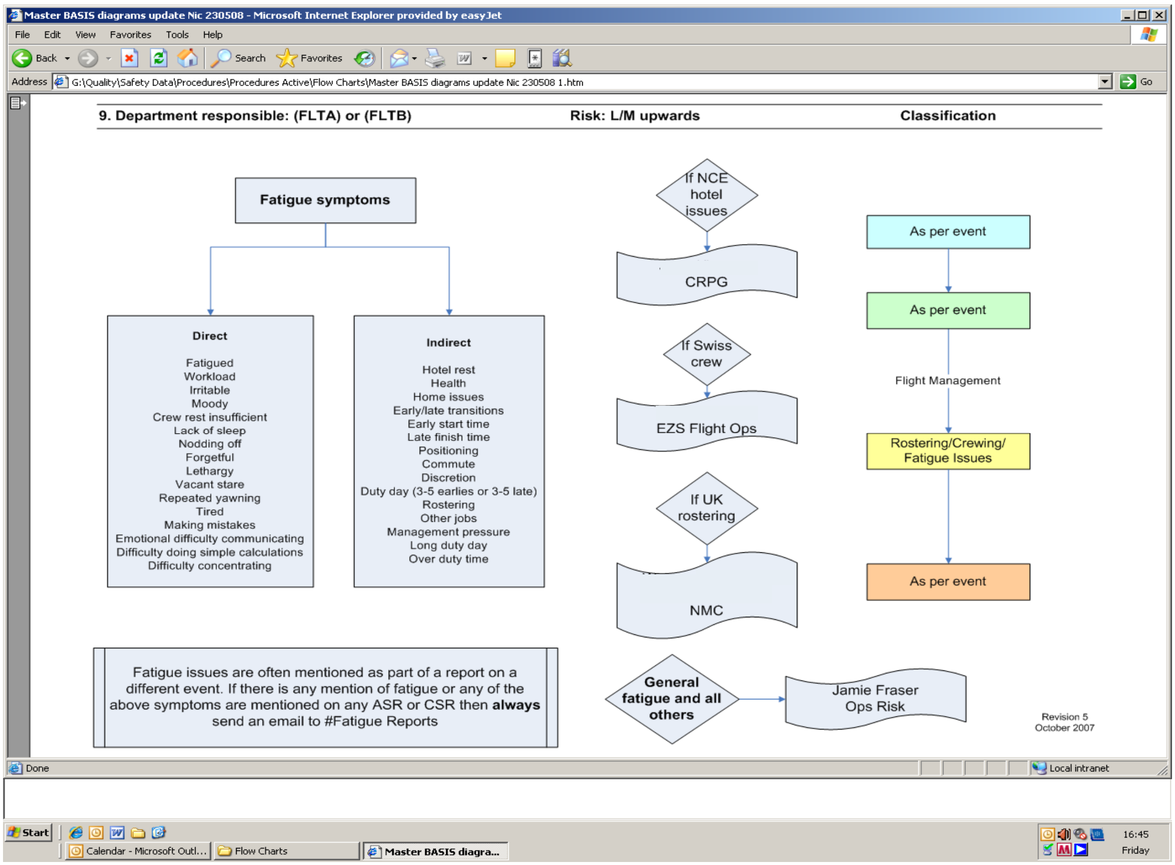


*EVENTS are initially* **risk assessed by the Safety Data Team**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Major Accident with significant loss of life | 🟨 30 | 🟧 100 | 🟥 300 | 🟥 1000 | 🟥 1000 | 🟥 | *Immediate preventative action. Eliminate hazard immediately if possible or stop. Immediate comms to Top mgt. Investigate.* |
| Limited Accident scenario with low potential for loss of life | 🟩 10 | 🟨 30 | 🟧 100 | 🟥 300 | 🟥 300 | 🟧 | *Investigate. Improve. Safety Action Group. Comms to SAG quickly.* |
| Minor Accident with some injuries and damage | 🟦 3 | 🟩 10 | 🟨 30 | 🟧 100 | 🟥 300 | 🟨 | *Enter into database. Into next Safety Action Group agenda.* |
| Degradation of safety margins but with little direct consequences | 🟦 1 | 🟦 3 | 🟩 10 | 🟨 30 | 🟧 100 | 🟩 | *Enter into database for monitoring but pass onto line management for assessment.* |
| Safety Margin remaining | *Normal intervention* | *Exceptional safety nets activated* | *Extreme intervention necessary to avoid imminent accident* | *Accident avoided purely by providence* | All barriers have failed and an accident has occurred. | 🟦 | *Enter into database for monitoring.* |

**Figure 5.** Crew self classification/SDT Triage risk matrix based on consequences and system defences (*ECAST Committee, 2008*)

3. The report once treated by the SDT is communicated to the relevant department manager responsible for the domain area for a decision on whether to investigate the incident or not. The manager then compares the reported event against threshold levels specified for Safety Performance Indicator's (SPI) as Safety Perofmance Targets SPT (based on event frequency and rolling year average risk level – event frequency/no. of flights – and this figure is compared to the SPT safety performance target). For example, Safety Performance Indicators trended at the SAG and SRB will have threshold levels set as



Fatigue issues are often mentioned as part of a report on a different event. If there is any mention of fatigue or any of the above symptoms are mentioned on any ASR or CSR then **always** send an email to #Fatigue Reports

**Figure 6.** Fatigue Classification flowchart in AQD

safety performance targets per domain that trigger investigations as a combination of event frequency and/or severity to the operation. The purpose of this step is to detect practical drift where an event may be increasing in frequency on the network over a period of time but this is not detected at SAG meetings as they focus on monthly SPI trends. If the manager is currently overloaded or resource restricted and the investigation can be deferred in their judgement then this is entered into the IMS and a notification period allocated. If the decision is made not to investigate then the accountable manager enters this into the IMS with their authorisation and feedback is provided to the reporter.

4. If the decision is made to investigate then the manager assigns an investigator/team (Investigator in charge -IIC and investigators per domain) to initiate the process with an initial investigation scope from the report. The first step is to determine from the IMS whether an event of this type has previously occurred and what information sources were analysed. This step applies an automation aspect to the investigation process so that the business does not repeat investigations at significant cost. This will take the form of a quick query process within AQD where investigation scenarios are accompanied by risk keywords per event.

5. If the scenario has been investigated before the investigating officer can quickly source the information required to commence the process of setting the scene rather than reviewing all information sources. A tool at this stage depending on the complexity of the investigation would be application of Event and Conditional Factors Analysis (plus) (Kingston et al, 2007).

6. If upon reviewing the data collected in step 6 there seems to be a disparity between the safety report and the information gathered then the investigator may redefine the scope of the investigation and the depth and capability of the investigation team. Prior research at easyJet/Imperial College London (Stewart et al, 2006 unpub)has shown that the higher the risk of the event the less accurate is the safety report or total absence of one.

7. Once all information is collated a more detailed assessment of the event scenario database for the event category is made using a case based reasoning approach (CBR) (Aamdt & Plaza 1994). The CBR (figure 7) cyclical learning approach uses the investigator domain knowledge and the retained knowledge of previously investigated events to facilitate problem solving. This saves time and cost in the investigation process and encodes organisational learning. This stage identifies whether the hazards within this event have been successfully treated previously through strategic and tactical actions. CBR facilitates the reuse of previous successful risk management strategies retained in the AQD database (in context where the organisation has learned) from previously experienced events. If there is a perfect match or simple adaptation of existing employed risk strategies against previous investigated events then the investigator can move to the risk management stage (step 11). If there is a partial or incomplete match then analytical tools are sequenced by the SME against the context of the investigation. This assists the domain expert/investigator to ascertain systematic causal factors (tools, context, people, task (Frei et al, 2003)).

8. The investigation is then completed and documented with the root cause, direct cause and contributory causes identified. The Human Factors Aviation Classification system (HFACS) Wiegmann & Shappell (2003) can be applied to identify active and latent failures against organisational levels of the business model. The next stage represents the interface from the investigation output into the risk management process. A frequency analysis of causal factors and combination of factors against the event category in the MCM is conducted. This is to detect if there exists a common causal thread between events within the category to assist the hazard analysis and ranking process. This analysis must be sequenced against risk management initiatives previously conducted within the event category. Conduct frequency and sensitivity analysis (factor criticality and relevance) of systemic causal factors & combinations for event and event classification category (if required).

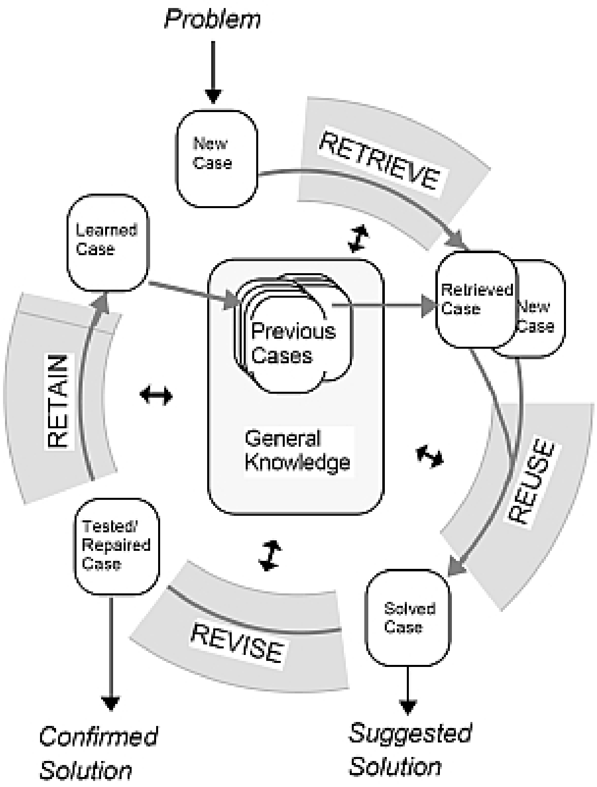


**Figure 7.** The CBR Cycle (*Aamodt and Plaza, 1994*)

9. A systematic causal factor table is developed at this stage: (factor, consequences, cost to operation, enablers (solutions), impact (+/-), cost savings, time to implement, accountability). The risk stakeholder group then rank - using a simple Analytical Hierarchical Process to facilitate - selected systemic factors for risk management against system impact.

10. The investigator and domain manager then identify strategic and tactical risk treatment options and 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. 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 double loop learning activity. Strategic options will all be associated with subsequent tactical management activity.

11. Risk stakeholders will then select a risk treatment option by consensus for positive impact against the system. The stakeholder group will review previous risk treatment activity against the risk scenario considering the impact of current control measures and the cost. The purpose of this activity is to determine if a

*known* system risk has increased in frequency against an Safety Performance Targets (threshold). An incident  may be categorised initially as low risk but it may require a more comprehensive risk management solution if the frequency of common influence increases against an event category. Risk reduction activity is focussed on the causal factors to undesirable process performance (this stage differs from step 3). An example of this would be using frequency of unstabilised approaches as a SPT, but determining that over 60s crew performance is a significant risk behind multiple unstabilised events. A strategic risk management action from the investigation process would be the requirement for the development of a new policy regarding over 60s crew recruitment. They will consider the timing and scope of the risk treatment requirement for tactical action and/or strategic action. The current scenario may be containable within the risk boundary/threshold until a strategic solution can be implemented. The stakeholder group may utilise the AHP process at this stage for strategic management. Tactical strategy selection can be facilitated using the Cohen et al (1996) Recognition/metacognition model (R/M) (figure 8). 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 to remain flexible for new novel situations. This model complements the CBR approach of problem solving and learning.

12. 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). 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. (Figure 2. shows the expanded process). 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. Should the strategy not be effective a new adapted strategy can be implemented represented by the feedback loop to risk treat options identification. If the strategy performance is acceptable  then monitoring activity occurs with a feedback loop returns to the sensory network stage. The report is documented in the IMS and information is prepared and trended for the Safety Action Group and Safety Review Board by the department postholder. An adjustment 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 to step 6 and redefines the scope of the investigation.

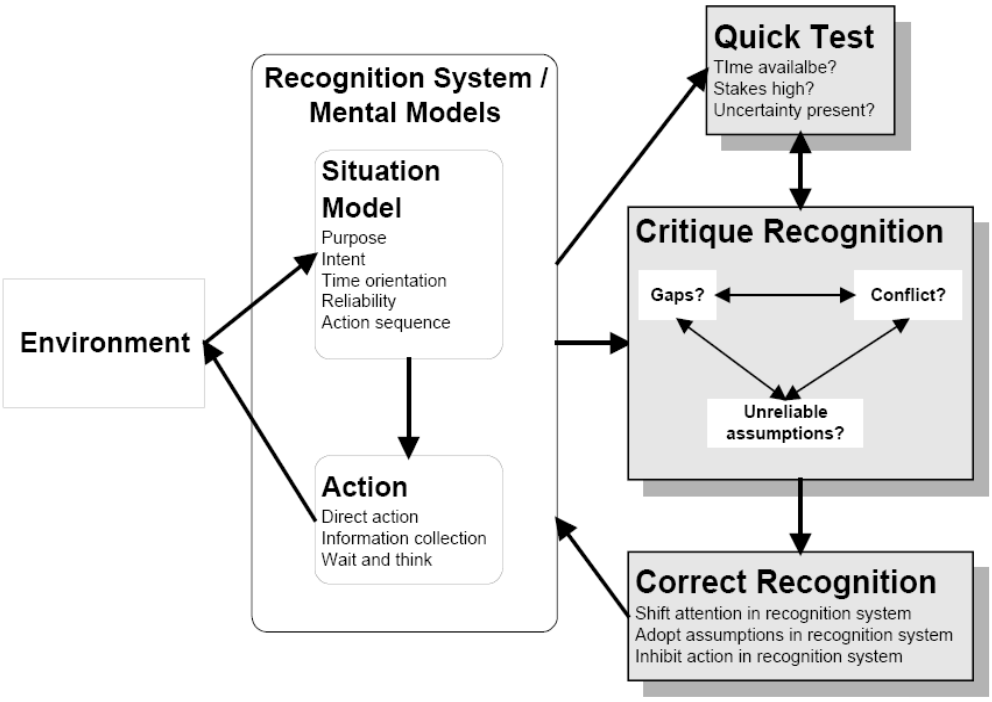


**Figure 8.** Basic components of the recognition/metacognition model (Cohen et al, 1996)

## 1.7 Core Tools description

### 1.7.1 Description of ECFA+

The "Events and Causal Factors Analysis" process (ECFA+), Kingston et al (2006) (NRI), is based on the Event and Causal Factors Analysis process: ECFA (Buys and Clark, 1995) and includes refinements of this approach that have been collected over the last decade. These refinements were arrived at through the experiences of the authors and by applying criteria and methods developed for investigation of the Fireworks Disaster in Enschede (2000) and tested again in the investigation of the Volendam Pub Fire disaster in 2001. . In order to distinguish this method from its predecessor, it is called ECFA+, Events and Conditional Factors Analysis.

The process was developed by the NRI Foundation whose aims are:

1. To help investigators produce accounts of incidents that are robust with regard to evidence and completeness;
2. To encourage stakeholders to share information about incidents;
3. To provide a reference point for practitioners (of investigation), tool developers, researchers and students.

ECFA+ is a method of producing a sequential description of an incident, which accounts for the logical relationships between the facts presented. Using witness narratives, logs and other sources of evidence, ECFA+ helps an investigator to build an account of the events that comprise an incident. Each event is stated using the present tense. These events are put into chronological order and linked together by identifying logical relationships. These links are tested to ensure that each event is explained satisfactorily. When needed, conditions are identified to ensure the completeness of these explanations. Every event, condition and logical relationship must be established to the standard of evidence required by the investigator.

ECFA+ analysis is generally an iterative process, running in parallel with other investigative activities. New information is added to the evolving ECF chart and this often raises new topics for further inquiries. If one were to add together the various iterations of work on an ECFA+ analysis, it will seldom take less than one hour for a simple incident, often two hours and sometimes more than this if the incident is complex. The fact that ECFA+ benefits from a team approach will add to opportunity cost associated using the method.

The ergonomics of ECFA+ means that it is best approached as a paper and pencil method, but this assumes that there is a sufficient physical space in which to do the work: a blind wall, four metres wide is adequate for most analyses. Experience suggests that a computer-based approach is not effective for performing ECFA+ in real time, especially when a team approach is used. If report quality materials are needed, it is normal practice to transcribe the ECFA+ chart using a flow-charting package or other vector graphics software application.

### 1.7.2 Control Change Cause Analysis – 3CA

3CA is designed to help investigators structure their inquiries into the underlying cause of incidents and to make it easy for others to review their reasoning. It is closely linked with ECFA+ as it starts from selected critical events in the ECFA+ reconstruction of an incident. The 3CA analyst may select events from the ECFA+ diagram by using various tests of relevance to the incident or accident. The analyst sets out these facts in a worksheet to form explanations and sets of questions. The result of the analysis is a concise description of the incident – seen in terms of changes and limitations in the control of changes – and a set of questions that the investigator needs answers on in order to fill gaps in the description.

*Description of Control Change Cause Analysis*

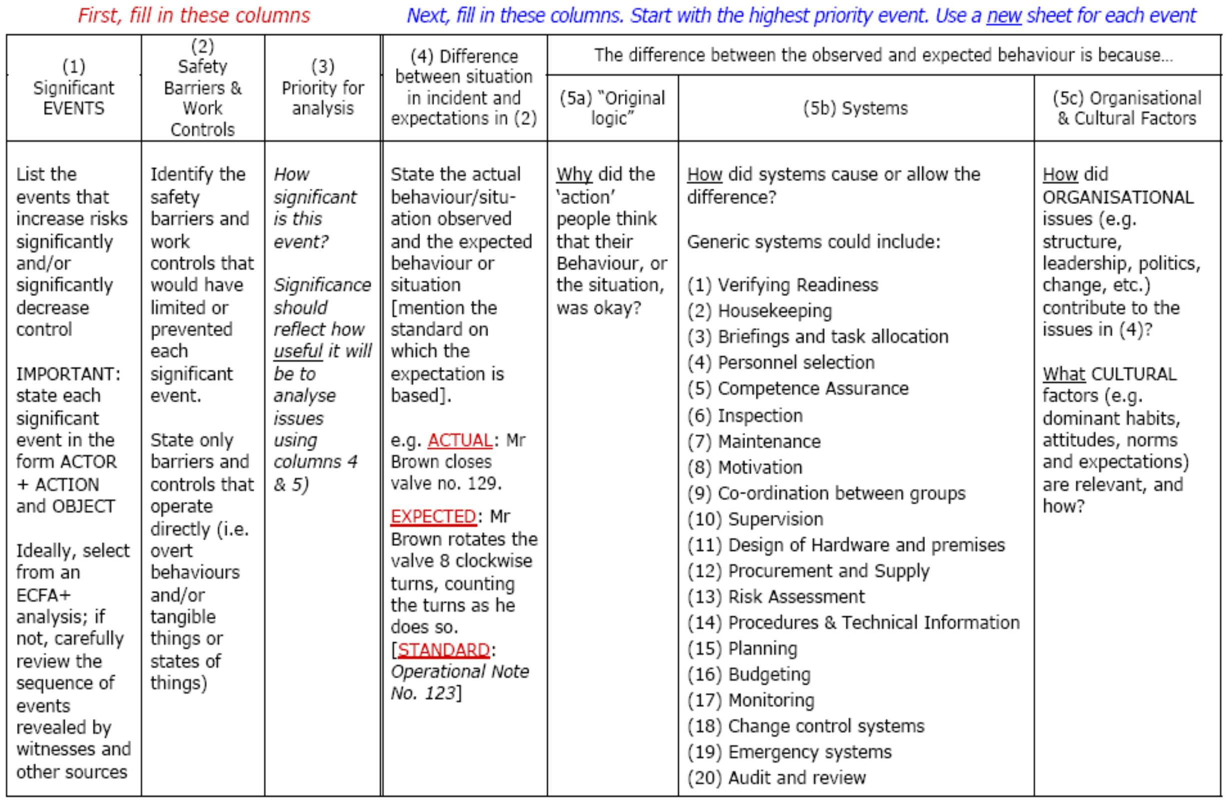
The analyst can begin the 3CA process as soon as he has the basic facts about what happened. It is best to start early because the analysis is likely to raise questions. In most investigations, the 3CA analysis will be revisited one or more times; as new facts emerge, so the analysts can answer the questions posed earlier. These answers sometimes trigger new questions.

In 3CA, the analyst treats accidents and incidents as a sequence of events in which unwanted changes occur. This sequence begins with the moment that reduces control and ends with the moment that restores control. Some of the events in the sequence are "significant" in the sense that they increase risks or reduce control in the situation, so allow further unwanted changes to occur. The first job for the 3CA analyst is to identify these significant events.

With the set of significant events established, the analyst identifies what measures could have prevented them or limited their effects. To ensure the thoroughness of this identification, the analyst describes each significant event in terms that make explicit who/what is acting, the action and who/what is acted upon. In this way, the analyst scrutinises all the elements of unwanted change from the point of view of prevention.

The analyst has to identify in what ways prevention was ineffective. In the first part of the analysis the focus is on tangible barriers and controls, those at the operational level. Next, the analyst restates the facts as differences between what was expected (based on norms such as standards and procedures) and what was true in the actual situation. The differences between the actual and expected situations provide the agenda for the rest of the analysis. The investigator seeks to account for these in terms of the reasoning used by people responsible for the barriers and controls, the systems and management arrangements that caused or allowed the difference to exist, and the organisational and cultural factors that influenced the situation.

**Table 2.** Extract from Control Change Analysis (3CA); (Kingston et al., 2007)



First, fill in these columns

Next, fill in these columns. Start with the highest priority event. Use a new sheet for each event

| (1) Significant EVENTS | (2) Safety Barriers & Work Controls | (3) Priority for analysis | (4) Difference between situation in incident and expectations in (2) | The difference between the observed and expected behaviour is because... | | |
|---|---|---|---|---|---|---|
| | | | | (5a) "Original logic" | (5b) Systems | (5c) Organisational & Cultural Factors |
| List the events that increase risks significantly and/or significantly decrease control<br>IMPORTANT: state each significant event in the form ACTOR + ACTION and OBJECT<br>Ideally, select from an ECFA+ analysis; if not, carefully review the sequence of events revealed by witnesses and other sources | Identify the safety barriers and work controls that would have limited or prevented each significant event.<br>State only barriers and controls that operate directly (i.e. overt behaviours and/or tangible things or states of things) | *How significant is this event?*<br>*Significance should reflect how useful it will be to analyse issues using columns 4 & 5)* | State the actual behaviour/situation observed and the expected behaviour or situation [mention the standard on which the expectation is based].<br>e.g. ACTUAL: Mr Brown closes valve no. 129.<br>EXPECTED: Mr Brown rotates the valve 8 clockwise turns, counting the turns as he does so.<br>[STANDARD: *Operational Note No. 123*] | Why did the 'action' people think that their Behaviour, or the situation, was okay? | How did systems cause or allow the difference?<br>Generic systems could include:<br>(1) Verifying Readiness<br>(2) Housekeeping<br>(3) Briefings and task allocation<br>(4) Personnel selection<br>(5) Competence Assurance<br>(6) Inspection<br>(7) Maintenance<br>(8) Motivation<br>(9) Co-ordination between groups<br>(10) Supervision<br>(11) Design of Hardware and premises<br>(12) Procurement and Supply<br>(13) Risk Assessment<br>(14) Procedures & Technical Information<br>(15) Planning<br>(16) Budgeting<br>(17) Monitoring<br>(18) Change control systems<br>(19) Emergency systems<br>(20) Audit and review | How did ORGANISATIONAL issues (e.g. structure, leadership, politics, change, etc.) contribute to the issues in (4)?<br>What CULTURAL factors (e.g. dominant habits, attitudes, norms and expectations) are relevant, and how? |

The analysis runs in parallel with other investigative efforts; after the initial 3CA analysis, you will likely make one or more revisions as further enquiries yield new insights and, in some cases, new questions. The initial 3CA analysis is performed in two parts in the sequence described below and indicated in Table 2.

In the first part, you complete column 1 (the significant events with identified conditional factors/hazards with identified safety barrier infringed) before completing column 2 (the barriers and controls). You finish the first part of the analysis by setting priorities in column 3; these priorities decide the sequence for the second part of the analysis. In the second part of the analysis, you complete columns 4 and 5 for one significant event at a time.

## References

Aamdt, A. & Plaza, E. (1994) Case based reasoning: foundational issues, methodological variations & system approaches. In. AICOM –Artificial Intelligence Communications Vol. 7, No1

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.

Buys, J.R. and Clark, J.L. (1995), "*Events & Causal Factors Analysis*". US Dept. of Energy. Ref. DOE 76-45/14, SSDC-14. www.jkltd.net/trac14.pdf

Cohen, Marvin S., Freeman, Jared T. and Wolf, Steve. (1996). Meta-recognition in time-stressed decision making: Recognizing, critiquing, and correcting. Journal of the Human Factors and Ergonomics Society (38,2), pp. 206-219.

DOE (1999) Conducting Accident Investigations DOE Workbook, Revision 2, May 1, 1999, US Dept of Energy, Washington DC, USA

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

Harvey, M.D. (1985) Methods for Accident Investigation. Alberta Occupational Health and Safety Division. Canada.

Hendrick, K & Benner, L. (1987) Investigating accidents with STEP. Marcel Dekker. New York.

International Electrotechnical Commission (1995) International Standard IEC 60300-3-9, Dependability management-Part 3: Application guide-Section 9: Risk analysis of technological systems. Genève.

Kingston, J., Nertney, R., Frei, R., Schallier, P. and Koornneef, F. (2004) Barrier Analysis Analysed in MORT Perspective. In Proceedings PSAM7/ESREL'04 International Conference on Probabilistic Safety Assessment and Management, Berlin, Germany, pp. 364-369.

Kingston, J., Koornneef, F., Frei, R., and Schallier, P. (2008) 3CA - Form B - Control Change Cause Analysis - Investigator's Manual. NRI5: NRI Foundation.. www.nri.eu.com.

Kingston, J., Jager, J., Koornneef, F., Frei, R., and Schallier, P. (2007) ECFA+: Events and Conditional Factors Analysis Manual. NRI-4, NRI4. NRI Foundation. www.nri.eu.com.

Knox, N.W. & Eicher, R.W. (2002) Management Oversight Risk Tree (MORT) User's Manual. SSDC-4 rev. 3. Retrievable from NRI Foundation. www.nri.eu.com.

Koornneef, F. & Hale, A. (2004) Organisational Learning: Requirements & Pitfalls. In Andriessen, J.H. and B. Fahlbruch, eds. *How to Manage Experience Sharing – from Organisational Surprises to Organisational Knowledge*. 2004, Elsevier: Amsterdam. ISBN 0 08 044349 4

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

Livingston, A.D., Jackson, G. & Priestley, K. (2001) Root Cause Analysis: Literature Review. Contract Research Report 325/2001. Health and Safety Executive (HSE).

Sklet. S. (2002) Methods for Accident Investigation. Reliability, Safety & Security Studies (ROSS). Norwegian University of Science & Technology (NTSU). Report no. 200208.

Stewart, S., Abboud, R., (2005a). Flight Crew Scheduling, Performance and Fatigue in a UK Airline Phase 1. Conference proceedings of Fatigue Management in Transportation Operations, 2005. September 11-15, Seattle. USA.

Stewart, S., Abboud, R., (2005b). Flight Crew Scheduling, Performance and Fatigue in a UK Airline Phase 2. Conference proceedings of Fatigue Management in Transportation Operations, 2005. September 11-15, Seattle. USA

Stewart, S., Koorneef, F., Akselsson, R. (2009a). *HILAS Operational Risk Management System*. HILAS Book 3 Ch. 4.

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

Weigmann, D.A. & Shappell, S.A. (2001) A human error analysis of commercial aviation accidents using the Human Factors Analysis and Classification System (HFACS). DOT/FAA/AM-01/3. Office of Aviation Medicine. Washington, DC. 20591

Weigmann, D.A. & Shappell, S.A. (2003). A human error approach to aviation accident analysis. The Human Factors Analysis and Classification System. Ashgate (2003).

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