

**SOFIA
Reference Manual**

Edition Number	:	1.0
Edition Date	:	22.10.02
Status	:	Released Issue
Intended for	:	General Public

DOCUMENT CHARACTERISTICS

TITLE		
SOFIA Reference Manual		
EATMP Infocentre Reference:		
Document Identifier	Edition Number:	1.0
	Edition Date:	22.10.02
Abstract		
Keywords		
Occurrence Investigation Incident Accident HEIDI	ATM specific event HERA ESARR 2	
Contact Person(s)	Tel	Unit
Tzvetomir BLAJEV	3965	SQS

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		Intended for		Accessible via	
Working Draft	<input type="checkbox"/>	General Public	<input checked="" type="checkbox"/>	Intranet	<input checked="" type="checkbox"/>
Draft	<input type="checkbox"/>	EATMP Stakeholders	<input type="checkbox"/>	Extranet	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/>	Restricted Audience	<input type="checkbox"/>	Internet (www.eurocontrol.int)	<input checked="" type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>	<i>Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)</i>			

ELECTRONIC SOURCE		
P:\SRC\WORK PROGRAMME\safety occurrence reporting\TOKAI\SOFIG		
Host System	Software	Size
Windows_NT	Microsoft Word 8.0b	879 Kb

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51

Fax: +32 (0)2 729 99 84

E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Safety Group Chairman	J. BEAUFAYS	22/10/2002

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	05/02/2001		Creation of the Working Draft	All
0.2	12/03/2001		Draft proposed to SQS for comments	All
0.3	12/03/2001		Draft proposed to Safety Group for comments	All
0.4	06/05/2002		Draft incorporating comments	All
1.0	22/10/2002		Released Issue	All

CONTENTS

DOCUMENT CHARACTERISTICS	ii
DOCUMENT APPROVAL	iii
DOCUMENT CHANGE RECORD	iv
Executive Summary.....	1
Chapter 1 INTRODUCTION.....	2
1.1 Purpose	2
1.2 SOFIA as a systemic methodology	3
1.3 What are the benefits from using SOFIA.....	10
Chapter 2 SOFIA Work Sheet.....	11
Chapter 3 SOFIA Symbols	13
Chapter 4 Factual information gathering – bottom-up process	14
4.1 What is Factual Information Gathering?.....	14
4.2 How SOFIA supports Factual Information Gathering?.....	15
Chapter 5 Event Reconstruction – top-down process.....	18
5.1 What is Event Reconstruction?	18
5.2 How SOFIA supports Event Reconstruction?	18
Chapter 6 Event Analysis.....	29
6.1 What is Event Analysis?	29
6.2 How SOFIA supports Event Analysis?	30
6.3 Human Error Analysis.....	30
Chapter 7 Issuing Recommendations.....	32
7.1 What is the process of Issuing Recommendations?	32
7.2 How SOFIA supports Issuing the Recommendations?	33
Annex A – All the golden rules at ones.....	34

©2002 The European Organisation for the Safety of Air Navigation (EUROCONTROL). All rights reserved. This document is published by EUROCONTROL in the interests of the exchange of information.

EUROCONTROL makes no warranty, either implied or express, for the information contained in this document, neither does it assume any legal liability or responsibility for the accuracy, completeness, usefulness and/or fitness for a particular purpose of this information.

The information contained in this document may be copied and reproduced by whatever means, provided that the above copyright notice and disclaimer are duly reproduced.

The information contained in this document may not be changed or modified without the prior permission of EUROCONTROL.

Executive Summary

SOFIA stands for **S**equentially **O**utlining and **F**ollow-up **I**ntegrated **A**nalysis.

SOFIA is a graphical-analytical tool supporting the process of ATM Safety Occurrence Investigation, which was developed to be compliant with ESARR 2 -The EUROCONTROL Safety Regulatory Requirement – Reporting and Assessment of Safety Occurrences in ATM.

SOFIA is recommended for use in the following phases of the investigation process:

- Factual information gathering;
- Event reconstruction;
- Event Analysis;
- Issuing Recommendations.

SOFIA makes use of the following investigation concepts:

- Barrier Analysis;
- Root Cause Analysis;
- Change Analysis;
- Time Sequence Analysis;
- Probabilistic and Deterministic Causation;
- Human Error Analysis;
- Event and Condition types of contributing factors;
- Contributing and Reductive correlation;
- Parallel Processes representation;
- Alternative Scenarios representation;
- Investigation in the Context of the system environment.

All these contemporary investigation concepts are combined implicitly in a user-friendly methodology in SOFIA, the user benefits from them just by applying simple so called “golden rules”.

Chapter 1

INTRODUCTION

1.1 Purpose

***SOFIA stands for
Sequentially
Outlining and
Follow-up
Integrated
Aalysis.***

SOFIA is a graphical-analytical tool supporting the process of ATM safety occurrence investigation and developed to be compliant with ESARR 2 -The EUROCONTROL Safety Regulatory Requirement – Reporting and Assessment of Safety Occurrences in ATM.

***SOFIA is recommended
for use in the following
phases of the
investigation process.***

-
- Factual information gathering;
 - Event reconstruction;
 - Event Analysis;
 - Issuing Recommendations.
-

SOFIA is designed to be ESARR 2 compliant.

Main milestones of SOFIA compliance to ESARR 2 are:

- ESARR 2 terminology;
 - ESARR 2 concepts – HEIDI based tool;
 - ESARR 2 Event Types;
 - ESARR 2 Contributors types – Direct and Indirect Contributors to the safety occurrence;
 - Applicability to Aviation Incidents/Accidents as well as ATM Specific Occurrences.
-

1.2 **SOFIA as a systemic methodology**

This is achieved by using the following three simple concepts:

1. **Three generic Barriers to the occurrence:**

- **Prevention** of potential conflicts, like airspace design, flow management, procedural de-conflicting of the routes;
- **Resolution** of potential conflicts, like ATCO instructions;
- **Recovery** from actual conflicts, like ACAS supported avoiding action;

2. **Two types of causal contribution:**

- **Direct** – removal of which could **deterministically** have prevented the safety occurrence;
- **Indirect** - removal of which could **probabilistically** have reduced the safety occurrence likelihood.

3. **Three layers of contributing factors to the efficiency of the Barriers:**

- **Actions** – events immediately close to the incident scenario;
 - **Job factors** – procedural, design and training issues influencing the **Actions**;
 - **Organisational factors** – **Root Causes** deeply in the organisational conditions.
-

SOFIA is a systematic methodology, addressing safety occurrence reconstruction and analysis.

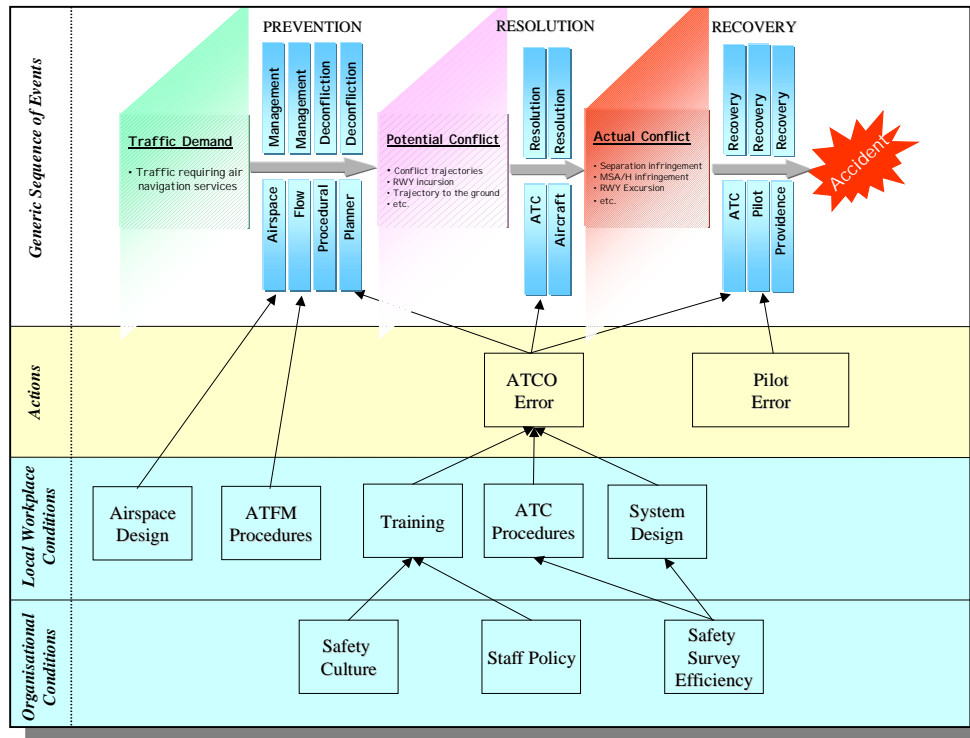


Figure 1

SOFIA combines a representation of the generic sequence of events (potential conflict, actual conflict, safety occurrence), leading to the safety occurrence, together with some example of the causal factors groups (contributors) from the previously defined 3 layers.

Barriers against accidents – Barrier Analysis

The generic sequence of events, leading to an accident could be stopped by any of the barriers:

- ➔ **Preventing** the potential conflict;
- ➔ **Resolving** the potential conflict;
- ➔ **Recovering** from the actual conflict.

The example in Figure 1 shows a diagrammatic view of SOFIA outcome.

Accident sequence is divided by the important events (potential conflict, actual conflict) into phases with different controllability of the situation.

Controllability is defined in terms of the ability of ATM to recover to a normal situation. Controllability is an aviation system function, but is often defined by the extent and ease with which the human operators (controllers, pilots) can contribute to the safety goals. Controllability is directly related to the accident risk – the less controllable the situation the higher the risk.

Prevention of potential conflict is a phase with real time controllability unimpaired.

Design and procedural actions could prevent the potential conflict in advance of real time flight operations – de-conflicted air routes, procedural de-conflicting. Uncertainty of the outcome in case of preventive actions is low.

Resolution of potential conflict is a phase, characterised by controllability being slightly impaired.

Timely actions are needed to restore the normal “equilibrium” – solve the potential conflict by changes to the flight parameters (profile, speed etc.). The rate of development of the situation is such that available reaction time is adequate to consider multiple alternatives. There is no need for evasive action. In case of timely intervention uncertainty of the outcome is low.

Recovery from actual conflict is the phase requiring immediate actions to restore the “equilibrium” or at least to confine the hazard.

It is usually said that the “***situation is unbalanced***”. Small changes in the way aircraft operations are performed could determine the outcome of the situation – recovery or accident. The speed at which the situation develops is such that available reaction time is minimal. There is a need for evasive action. Even in the case of intervention uncertainty of the outcome is high.

If Safety Principles are applied it can help the prevention, resolution or recovery. For example ***Resolving*** the potential conflicts could be decomposed into the following four Safety Principles:

- ***Detection*** of the potential conflict;
- ***Develop*** some plan to solve the potential conflict;
- ***Deliver*** the instruction to the crew;
- ***Execute*** - crew to implement the actions required by the instruction;

Each barrier could be decomposed layer after layer into safety principles.

Each Safety Principle could be decomposed again into the next level Safety Principles. For example ***Detection*** needs:

- ***Anticipate*** the potential conflict;
- ***Sensor*** the distinguishing characteristic of the potential conflict;
- ***Recognise*** the pattern of the potential conflict;

The Safety Principles as described above are functional. For each investigation they should be elaborated with the specific details – how human, equipment and procedures in the given environment of operations achieve the functions. For example Detection of potential conflict of two aircraft in the air can be facilitated or not by the Medium Term Conflict Detection system. The same holds true for the Delivery – via verbal or data link communications.

Following the ICAO definition, causes can be broadly interpreted to include actions, omissions, events, conditions, or a combination thereof, that lead to an accident or incident.

An occurrence is usually the result of a sequence of events. All causes together form the necessary and sufficient adverse events or conditions for a particular occurrence. However, the findings of any analysis may focus on some of these necessary conditions that may, in the future, combine with other factors to cause similar but not identical incidents.

Any analytical technique must enable investigators to identify the ATM system contribution to these causal events. It is possible to distinguish between a number of different ways in which the ATM system can contribute to an occurrence. For example, ESARR2 recognises the following distinctions:

SOFIA supports investigators to distinguish between the causes of an occurrence.

Direct involvement. At least one ATM event was judged to be directly in the causal chain of events leading to an accident or incident. Without that ATM event (or if there was a different order of events), the occurrence would not have happened. A direct contribution that starts an adverse event flow is called a root cause. Without such an ATM event, the accident or incident would not have happened.

Indirect involvement. No ATM event was judged to be directly in the causal chain of events leading to an accident or incident. However, at least one ATM event contributed to the level of risk or played a role in the emergence of the occurrence. Without such an ATM event, the accident or incident could still have happened.

No involvement. No ATM event was in the causal chain leading to an occurrence, nor did any ATM event play a role in the emergence of an occurrence. This covers situations where the ground elements of the ATM system had nothing to do with the safety occurrence.

The event or condition building blocks can be placed on a timeline to show how an occurrence develops over time. They are further linked with the arrow corresponding to the type of causal contribution mentioned before – direct and indirect. This leads to the development of a causal network, used in the next phases of the investigation process. Actors have been extended to incorporate James Reason’s model (the so-called “Swiss cheese” model):

Factors contributing to the barrier efficiency.

“Actors’ events/conditions” - including the active failures immediately in the course of the safety occurrence. In this layer is the main chain of chronological events leading to the undesired safety occurrence;

“Local workplace triggering conditions” – conditions, or lack of conditions and associated events that allowed the events/conditions from the first layer to happen. These conditions are also sometimes called “Job Factors”;

“Organisational conditions” – systemic organisational factors, underlying the first two layers. Within this layer are the Root Causes. Root Causes are the fundamental underlying causes, which address classes of similar occurrences, rather than single problems.

Within these three layers of actors it is possible to identify classes of factors that contributed or mitigated the occurrence:

-
1. ATM service personnel.
 2. ATM services personnel operating procedures and instructions.
 3. Interfaces between ATM service units.
 4. ATM service infrastructure/facilities and technical systems.
 5. Airspace structure.
 6. Staffing and supervision.
 7. Company structure and management policy.
 8. Regulatory activities.

The previous list provides generic distinctions between causal factors. Any particular occurrence investigation should, of course, take place at a far more detailed level and should look at the particular local circumstances that influenced the course of an incident. It should also be stressed that any causal analysis should identify not only the exact way in which an occurrence occurred but should also consider any alternative ways in which the barriers that protect a system might also have failed.

ATM service personnel.

The analysis should determine whether physical/physiological and psychosocial factors were involved in the events leading to an occurrence. It should also consider the human-system interface, the controllers working environment and the operational task demands. This analysis requires the ability to analyse the effects both of normal working practices but also any unusual or transient factors that may have adversely affected operator performance. Did the personnel follow the procedures? Were there any factors, which may have affected personnel performance, e.g. workload, fatigue, illness, personal problems, stress, experience, vigilance, situational awareness, communication, attention, automation etc.?

ATM services personnel operating procedures and instructions.

The analysis should determine whether any operational ATM procedures contributed to an occurrence or conversely whether they helped to mitigate the consequences of an occurrence. Equally importantly for some occurrences, the analysis should consider whether engineering and maintenance procedures contributed to adverse events. Were the procedures applicable in the context of the occurrence? Were the procedures applied, correct for the situation? Was the correct phraseology and communication procedures used?

Interface between ATM service units

The analysis should consider whether communications failed technically, procedurally or in a social sense between the different individuals who should co-ordinate during ATM procedures. The analysis should also consider whether any individual or organisational factors contributed to the failure, e.g., had the personnel received TRM (Team Resource management) training?

ATM service infrastructure/facilities and technical systems

The analysis should consider whether hardware or software problems contributed to an occurrence. Very often these issues do not relate simply to component failure but to design and integration problems. For example, changes in the presentation and format of data can prevent controllers from performing necessary tasks using particular software interfaces. The analysis should also consider particular characteristics of aerodrome layout and its associated infrastructure.

Airspace structure.

The analysis should take into account route structure and capacity as well as the sectorisation of ATS airspace. For instance, many ATM providers report that occurrences often occur during the transition from periods of heavy loading to more quiescent intervals. Such informal observations should be backed-up by analyses that consider whether or not such changes were a factor in particular occurrences.

Staffing and supervision

The analysis should consider whether the personnel were familiar with the operational environment before assuming the responsibility for ATC. Adequacy of staffing level in relation to the work demand, relief and rest schemes and adequacy should be considered as well. Was the level of supervision satisfactory?

Company structure and management policy.

The analysis should consider the contribution of operational line management. They should also consider any successes or failures in safety management systems. The analysis should include institutional arrangements before, during and immediately after an occurrence. This may also lead analysts to consider the impact of management and personnel policy on the events leading up to an occurrence.

Regulatory activities

The analysis should also consider whether any regulatory activities, regulation and approval processes failed to prevent an occurrence and whether appropriate changes might be requested in the light of an occurrence.

1.3 **What are the benefits from using SOFIA**

SOFIA provides following benefits for the Safety Occurrence Investigation Process:

- Providing a **complete methodology** for performing the factual information gathering, event reconstruction, analysis and recommendations elaboration;
 - Ensuring the **systematic investigation** in a user friendly environment, where the contemporary investigation concepts are implicitly included in the simple to use “golden rules”;
 - Illustrating and validating the **sequence (or network) of events** leading to the safety occurrence;
 - **Depicting the relationships** between the immediately relevant contributors and deep job and organisation factors;
 - **Promoting a multiple causality** understanding of safety occurrences;
 - Providing a **structured method** for factual information gathering, pointing to the gaps in the reconstructed safety occurrence and directing the progression of additional data collection;
 - Providing a means to combine **probabilistic and deterministic causation** in the analysis and elaboration of recommendations;
 - **Validating the outcomes** of the other investigation and analysis methods and techniques;
 - **Visualising** factual and analysis information;
 - **Quality assurance** for the incident investigation process;
 - Serve as a means of **lessons learned** and exchange;
-

Chapter 2

SOFIA Work Sheet

The SOFIA work sheet (Figure 2) is a two-dimensional co-ordinate system representing:

- Important moments in time - on the horizontal axis;
- Relevant “Actors”, playing a role in the investigated occurrence - on the vertical axis.

Actor(s) can be any representative player in the occurrence:

- Crew;
- Individual pilot;
- ATCO;
- Airport vehicle drivers;
- Separation;
- Weather etc.

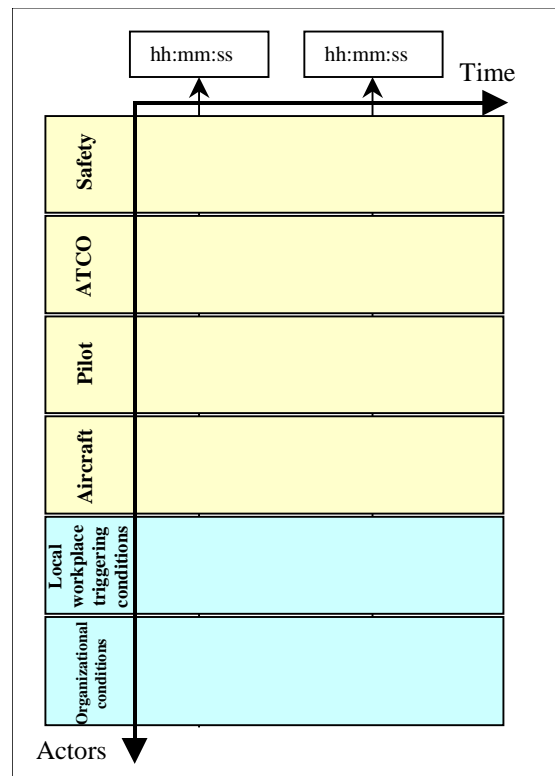


Figure 2

Actor can be a person but also an aircraft, an aircraft system, and/or an ATM system.

Actor is also any attribute, which is important and is dynamic in the course of particular occurrence like separation.

Actors have been extended to incorporate James Reason's model (the so-called "Swiss cheese" model) - "Local workplace triggering conditions" and "Organisational conditions".

This will allow SOFIA to be used to capture the latent conditions – the hidden part of the "iceberg" that contributes to the occurrence of accidents, and incidents.

Chapter 3

SOFIA Symbols

SOFIA symbols (Figure 3) fall into 3 categories:

→ Building blocks → Contributors → System Symbols

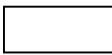


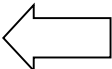

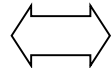









Building Blocks		Contributors		System Symbols	
	Event happened at that moment		Direct Contributor		Safety Recommendation
	Event happened before that moment		Indirect Contributor		
	Condition existing at that moment		Reductive Contributor		Link between contributors
	Event/condition happened/existed at/before that moment which is analysed that is increasing the likelihood for the final occurrence - HAZARD		Suspected but unconfirmed Direct/Indirect /Reductive Contributor		Alternative hypothesis for the contributors
					
					

Figure 3

Chapter 4

Factual information gathering – bottom-up process

Answering the questions WHAT, WHEN, WHERE, and WHO?

4.1 *What is Factual Information Gathering?*

To collect the data.

Factual information gathering is the phase of the occurrence investigation process that should deliver all the relevant information needed to explain the event. These are all the events and conditions that played a role in the process of safety occurrence generation.

4.2 How SOFIA supports Factual Information Gathering?

All identified information, relevant to the occurrence investigation is presented on the SOFIA work sheet.

The process of introducing the information is parallel to the process of investigation. Information is mainly collected during the factual information-gathering phase of the investigation. However, other phases are feeding in additional information. SOFIA allows structured information gathering by highlighting the gaps and easing quality control.

SOFIA provides a bottom-up process for information gathering. This is achieved by describing each and every relevant fact discovered during the investigation.

This is achieved by application of the “4 golden rules for factual information gathering”:

1. Enter all identified information into the Sofia work sheet, using the appropriate building blocks exemplified from ① to ④ below;
2. Assign them a relevant moment in time;
3. Add links between building blocks and appropriate HEIDI elements;
4. Check if all the relevant information is considered by answering to the question **“what was different in the system, compared to the normal operations?”** Assess these deviations (**Change Analysis – Figure 4**) for their safety significance.

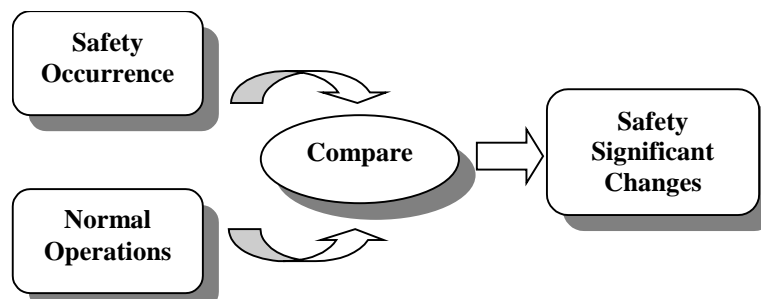


Figure 4

① Event happened at a particular moment in time

All events associated with an exact time moment are depicted like the rectangles showed in Figure 5.

For example at 10.23:39 ATCO issued an instruction to the aircraft to stop. As a consequence of this, Pilot applied heavy breaking at 10.23:45.

Each of these is an event associated with particular moments in time. Therefore, we represent them on the SOFIA work sheet as a rectangle symbol.

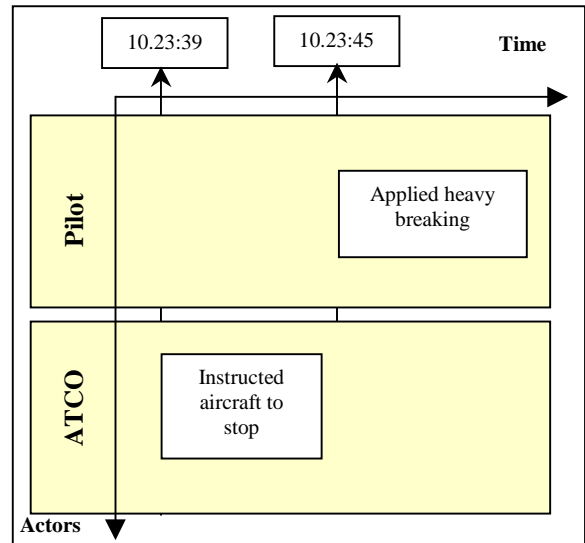


Figure 5

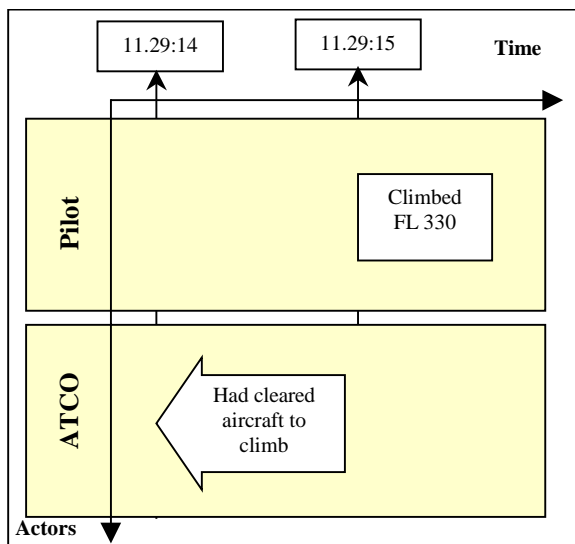


Figure 6

② Event happened before particular moment in time

All events, which happened before a certain moment, are depicted as an arrow, pointing to the left.

The example in Figure 6 describes a hypothetical event - "ATCO had cleared aircraft to climb", happened before the moment in time 11.29:14. As a result of that clearance, aircraft climbed to FL 330.

The important information here is that this clearance was present at 11.29:14, and not exactly when it had been issued.

③ Condition existing at particular moment in time

All conditions, which existed at a certain moment, are depicted as two-directional arrow.

The example in Figure 7 describes a hypothetical condition - “Inexperienced co-pilot”. This condition contributed to the reduction of the vertical separation standard.

There is no particular moment, associated with this building block – it is “floating” in time. This condition fits well the J. Reason’s model of organisational accidents/incidents.

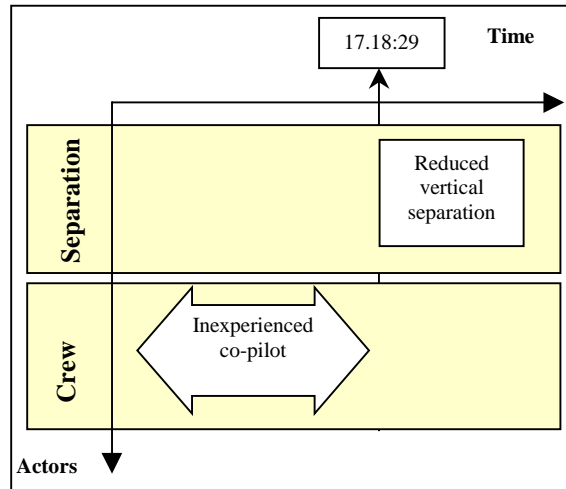


Figure 7

④ Event/Condition happened/existed at/before particular moment, which is increasing the likelihood for the Safety Occurrences (HAZARDS)

In Figure 8 “radar failure” and “ATCO training less than adequate”, are marked as hazards, because they are increasing the likelihood of Safety Occurrences (not necessarily only the investigated one – see rule 1 from Issuing Recommendations).

The follow-up action is to analyse these hazards and to decide upon the necessary safety improvements (eventually issue safety recommendations and their related remedial actions).

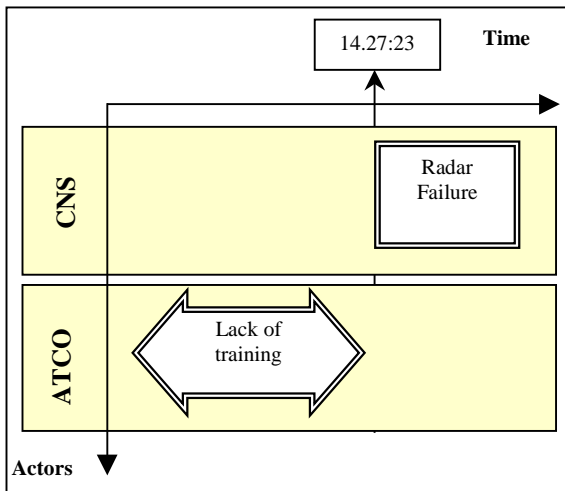


Figure 8

Chapter 5

Event Reconstruction – top-down process

Answering the question HOW?

5.1 *What is Event Reconstruction?*

To create the network of factors.

Event Reconstruction is the phase of the occurrence investigation process that should deliver all the rebuilt representation of the network of factors that have brought about the event.

5.2 *How SOFIA supports Event Reconstruction?*

SOFIA uses the various contributors and the Generic Sequence Model.

Event Reconstruction provides a depicted sequence of event/conditions linked with direct/indirect/reductive contributors' correlation. Types SOFIA contributors are exemplified from ① to ⑦ below:

① **Direct Contributor** – represented by straight arrow.

The test for a direct contributor, is the question “If event 1 is removed does it prevent event 2?” If yes – 1 is a direct contributor for 2.

Examples (Figure 9) are “Pilot erroneous read-back” and “ATCO lack of hear back”. If, either of them is removed the misinterpretation of ATS clearance could not have happened. Therefore, they are both direct contributors.

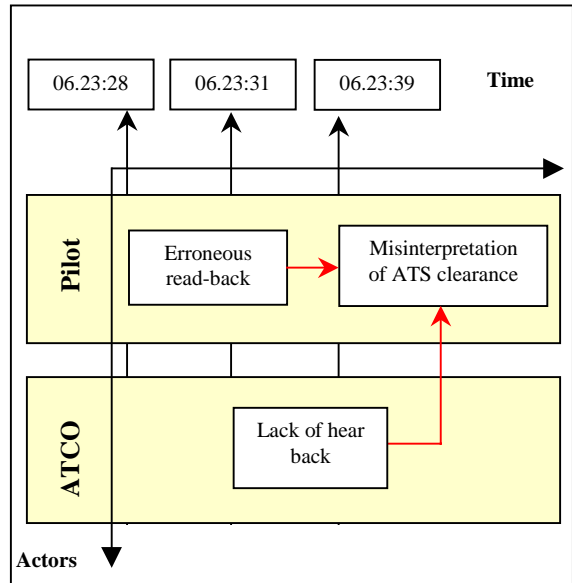


Figure 9

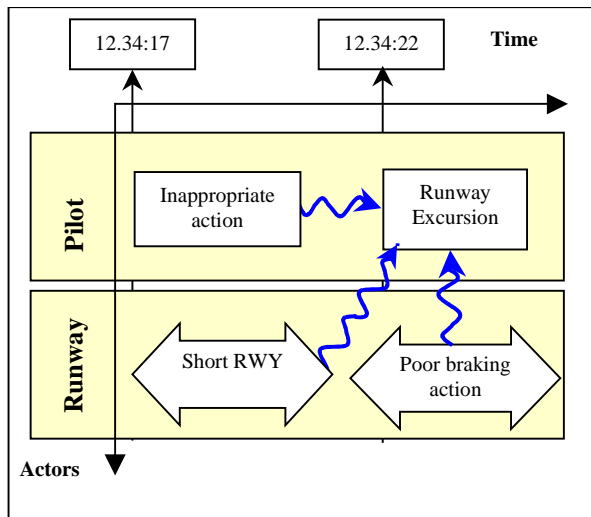


Figure 10

② **Indirect Contributors** – represented by a curved arrow. Without the first event/condition, it is considered that the second might still have happened. The first is only increasing the likelihood of the second. Example of 3 indirect contributors for one Runway Excursion is given in Figure 10. There the event “inappropriate crew action” and conditions “short runway” and “poor braking action” have increased the likelihood of the Runway Excursion. However, if some of them are removed, Runway Excursion might still have happened.

③ **Reductive Contributors** – represented by curved arrow, marked with the symbol “↓”.

Without the first event/condition, it is considered that the second might still have happened. The first event/condition is only reducing the likelihood of the second.

Example of Reductive Contributor for a Human Error is given in Figure 11 – “Good training programme” actually reduced the probability of “Human Error”, but “Fatigue” in turn increased that likelihood and made it happen.

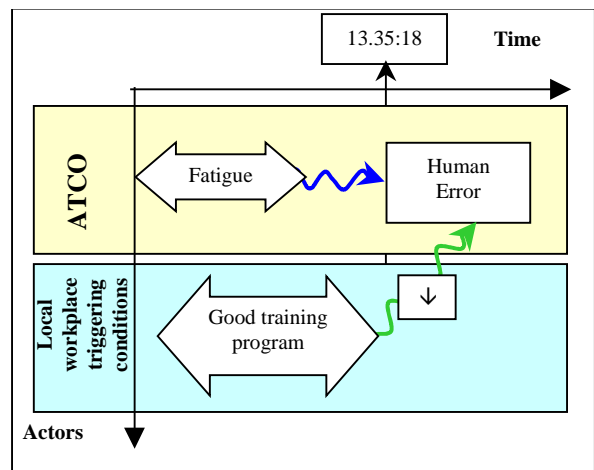


Figure 11

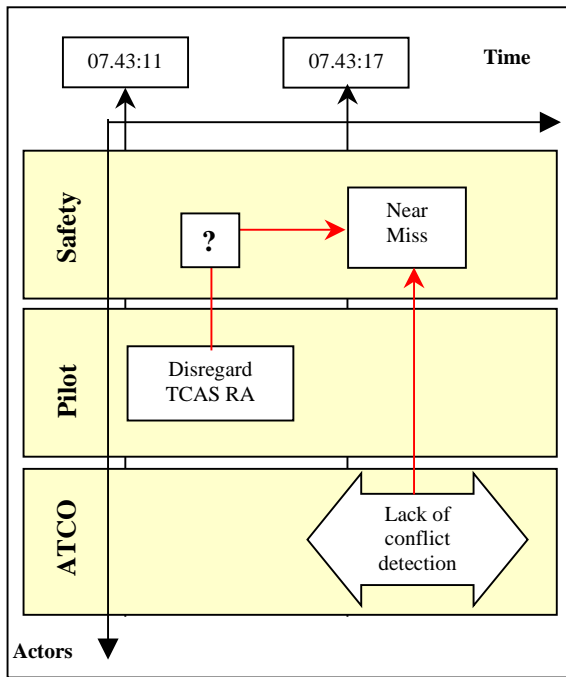


Figure 12

④ **Suspected Direct Contributors** – represented by a question mark on the direct contributor arrow.

Depicts the uncertainty, about if the event/condition happened and/or if it is a direct contributor to another event/condition.

An example is given in Figure 12. There the event “Near-miss” has one confirmed direct contributor “lack of ATCO conflict detection”. If this contributor is removed the event could not happen. “TCAS RA disregarded by the pilot” is an unconfirmed direct contributor because we are not sure if this actually happened and/or if this is direct contributor.

The correlation between the two elements is marked as suspected, but the “suspicion” requires putting more effort to remove the existing uncertainty.

⑤ **Alternative Direct Contributors** – represented by “OR” symbol on the contributor’s connecting point.

Figure 13 depicts how some possible alternative direct contributors (hypothesise) for the second event/condition are represented on the SOFIA work sheet.

The example represents two possible alternative direct contributors for the “Aircraft engine failure”. The first one is due to “maintenance error”, and the second alternative is due to “bird strike in flight”.

More effort in the investigation is needed to filter out only one alternative and to fix exact moments in time.

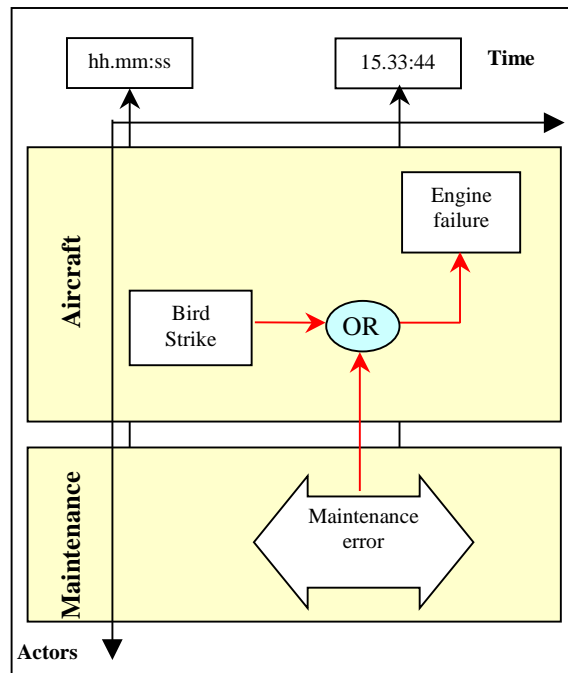


Figure 13

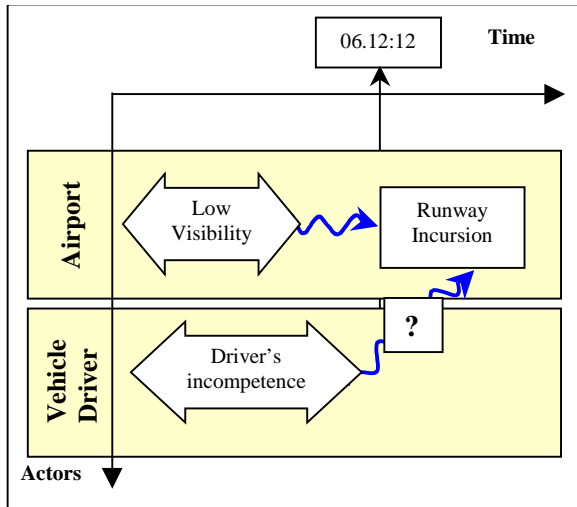


Figure 14

⑥ **Suspected Indirect Contributors** – represented by a question mark on the link between an indirect contributor to a subsequent event. Figure 14 depicts the uncertainty, of the event/condition having happened and/or if it is an indirect contributor to the second one represented on the SOFIA work sheet.

The example on Figure 14 means that for the condition “Airport vehicle driver’s incompetence”:

→ It is not sure if it exists and/or

→ If it exists – it is not clear whether it is direct or indirect contributor for the “Runway Incursion”.

⑦ **Suspected Reductive Contributors** – represented by curved arrow, marked with the symbol “↓?”.

Figure 15 depicts how the uncertainty of the event/condition happening and/or if it is a reductive contributor to the second event is represented on SOFIA work sheet.

The example in Figure 15 means that it is not sure if the event “See and avoid” exist for aircraft 1. We are sure the level bust of aircraft 2 directly contributed to the near miss. More effort is needed to identify aircraft 1 actions.

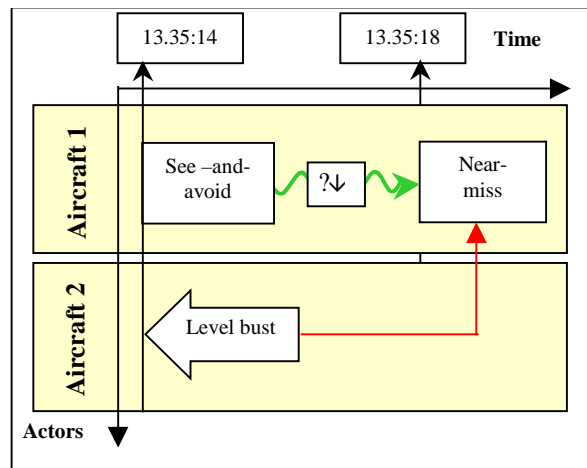


Figure 15

SOFIA provides a top-down process for Event Reconstruction. This starts from the final event and applies “why this happened” test for each event/condition.

This is achieved by application of the following “10 golden rules for event reconstruction”:

-
1. The only Goal is to Improve Safety and not to apportion blame or liability;
 2. Start from the final event and go step-by-step backwards, asking the question “why did this happen?”
 3. Try to identify as many contributors as possible to the event/condition using the contributor’s’ description from ① to ⑦ above. Do not proceed further until the all building block contributors are identified;
 4. Which are the contributors that if removed could have prevented the analyzed building block? Use Direct Contributor correlation for them;
 5. Which are the contributors that increased the likelihood of the analyzed building block, but whose removal does not prevent it? Use Indirect Contributor correlation for them;
 6. Which are the contributors that decreased the likelihood of the analyzed building block? Use Reductive Contributor correlation for them.
 7. Two Building Blocks linked with the Direct/Indirect contributor symbol have to be immediately (causally) next to each other. Is it possible for something to be between them? If yes - introduce it on the work sheet.
 8. Mark any uncertainty on the type of contributor and contributors’ existence with the question mark. Put more effort to remove these uncertainties.
 9. Check the temporal sequence of the building blocks by following the time line for each actor. This ensures the right sequence of events/conditions for the actor.
 10. Check the temporal relations of events/conditions for different actors by following the vertical marked moments in time. This ensures the right sequence of events/conditions for the different actors.
-

The SOFIA Work Sheet provides “Generic Sequence of Safety Occurrence” – Figure 16.

This is a tool to guide the analysis in the initial stage of Event Reconstruction. This Generic Sequence is composed of abstract events/conditions that are common for each and every safety occurrence. It is the investigator task to choose the particular option for a given occurrence of these generic events/conditions and then to continue the application of “10 golden rules for event reconstruction”.

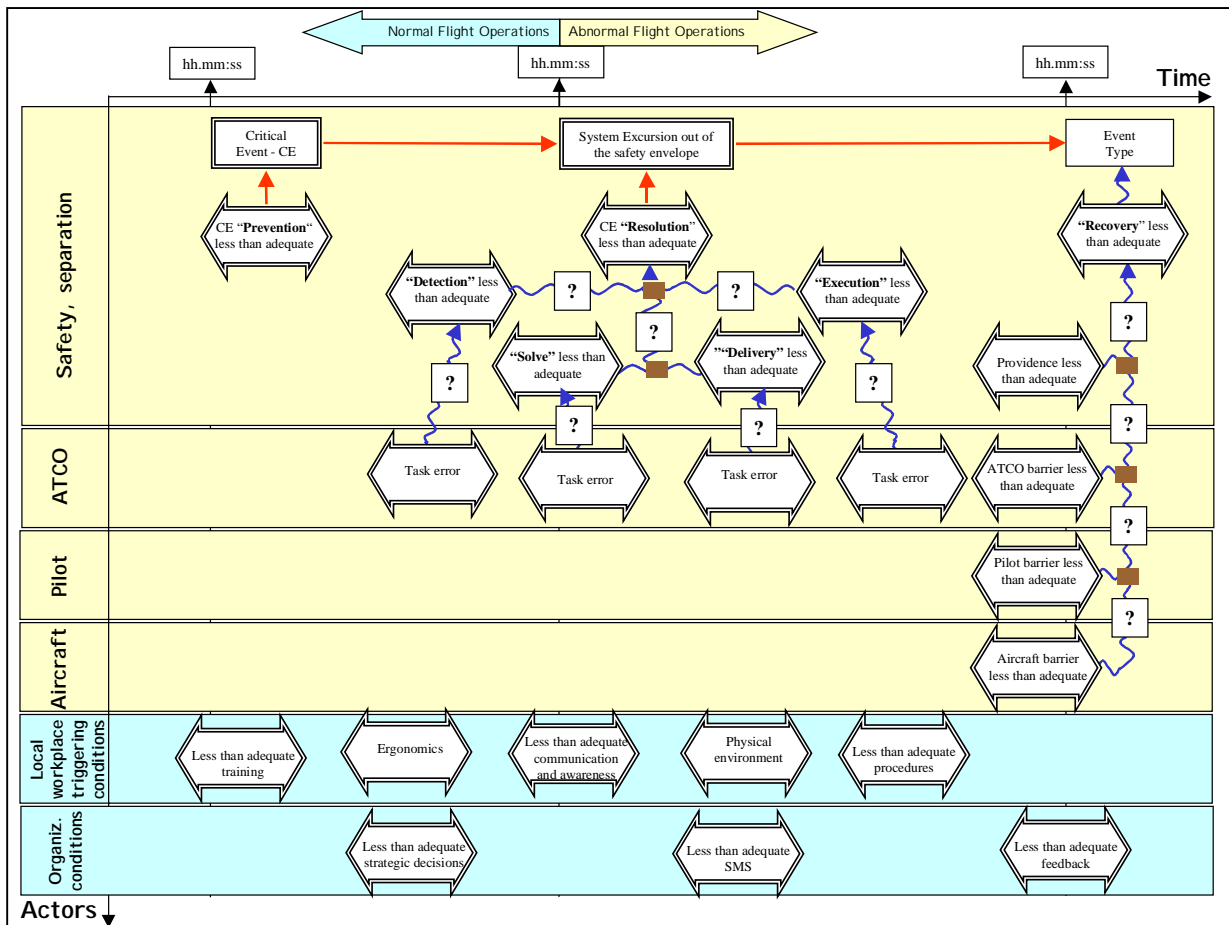


Figure 16

A key concept in the Generic Sequence is the term “System Excursion out of the safety envelope”.

This is sometimes called Actual Conflict. A System Excursion is the status of the system at the border between Normal and Abnormal Flight, when the occurrence is an incident/accident.

When the occurrence is an ATM specific event the System Excursion is at the border of Normal and Abnormal Air Navigation System Operations.

In fact, a System Excursion is characterised by crossing the border of the safe operational envelope by one or more of the system safety parameters. The parameter could be relative distance between the aircraft, relative distance between the aircraft and the surface or obstacle, pitch, bank, speed, acceleration etc.

For each System Excursion there is:

One precursor Critical Event (CE) - without which the System Excursion could have been prevented. A Critical Event in ATM is also called a Potential Conflict. In fact, a Critical Event is characterised by a tendency (together with proximity) for one or more of the system safety parameters to move towards the border of the safe operational envelope. A Critical Event is not always entirely preventable. Sometimes it is part of the normal operations. Example of this is “Closing tendency between two aircraft in the air”. No matter how good our system is it is not possible to remove all the potential conflicting points. The challenge is to reduce their numbers to as low as is achievable;

One final event – Incident/Accident/ATM specific. A final event is described in HEIDI as Event Type.

Table 1 provides a possible mapping scenario between these events.

One important issue is that these categories are neither a binding or complete list.

Ideally both the Critical Event and System Excursion should be defined considering the controllability of the situation for the given type of accident. On one hand a Critical Event should be the moment in time after which is clear that a control action will be required (irrespective of the actor – pilot, ATCO, system etc.). On the other hand a System Excursion is the moment in time after which marginally small changes in some of the controls or circumstances could lead to disproportionate change in the safety margin. This is in fact a situation “at the edge”, with small controllability.

Table 1

CRITICAL EVENT	SYSTEM EXCURSION OUT OF THE SAFETY ENVELOPE	EVENT TYPE	
		Incident	Accident
Closing tendency between two aircraft in the air - two aircraft on conflict paths.	Separation minimum infringement between two aircraft.	Near miss.	Mid air collision.
Closing tendency between airborne aircraft and object on the surface.	Minimum safe height/altitude infringement.	Near air-ground collision.	Air-ground collision.
Closing tendency between airborne aircraft and terrain surface.	Minimum safe height/altitude infringement.	Near collision with the ground.	Collision with the ground.
Closing tendency between aircraft and static obstacle on the movement area.	Separation minimum infringement aircraft and static obstacle on movement area. Inadequate separation.	Near ground-ground collision.	Ground-ground collision.
Closing tendency between aircraft and another aircraft, mobile object or vehicle on movement area.	Separation minimum infringement between aircraft and another aircraft, mobile object or vehicle on movement area. Inadequate separation.	Near ground-ground collision.	Ground-ground collision.
An unintended entry of aircraft, vehicle or person on a RWY or RWY strip.	An unauthorized simultaneous RWY usage (take-off).	Near ground-ground collision. Near air-ground collision.	Ground-ground collision. Air-ground collision.
An unintended entry of aircraft, vehicle or person on a RWY or RWY strip.	RWY occupied and landing aircraft bellow DH/MDH.	Near ground-ground collision. Near air-ground collision.	Ground-ground collision. Air-ground collision.
Closing tendency between aircraft and Runway edge/end.	Runway Excursion.	Near ground-ground collision.	Ground-ground collision.
Closing tendency between airborne aircraft and airborne object.	Separation minimum infringement between airborne aircraft and airborne object. Inadequate separation.	Near air-air collision.	Air-air collision
Closing tendency between aircraft and segregated airspace.	Separation minimum infringement between aircraft and segregated area. Inadequate separation.	Near air-air collision.	Air-air collision.
Closing tendency between aircraft and area with adverse meteorological conditions.	Separation minimum infringement between aircraft and area with adverse meteorological phenomena. Inadequate separation.	Variants*	Variants*
Landing and take-off cleared at contaminated runway.	Landing and take-off commencing at contaminated runway.	Near ground-ground collision.	Ground-ground collision.
Closing tendency for the aircraft safety parameters towards their critical values – “safety envelope” borders.	Excursion for the aircraft safety parameters out of their critical values – “safety envelope” borders. Loss of control.	Variants*	Variants*
Failure or human error or external event.	Loss of critical ATM system function.	ATM specific occurrence.	

Variants* - more than one variant for the event type is possible for that Critical Event/System Excursion

Generic Contributor for a Critical Event is “**Critical Event Prevention less than adequate**”. If CE is “Closing tendency between aircraft and static obstacle on the movement area” then one example of less than adequate prevention is existence of this object on the movement area.

Once a Critical Event, System Excursion and Final Event are chosen the Generic Sequence Analysis continues with their generic contributors.

Generic Contributor for a System Excursion is “**Critical Event Resolution less than adequate**”. If CE is “Closing tendency between two aircraft in the air - two aircraft on conflict paths.” then the ATCO has to **identify** the conflict, to **develop** some plan to solve it, to **deliver** the instruction to the crew and crew has to **execute** it. Any deficiency in this sequence could contribute to the “Critical Event Resolution less than adequate”. One possible deficiency for each of these contributors is **ATCO Task Error**.

Task Error is not a psychological explanation of the error (which is delivered by using a different tool - HERA), but simply how the error was observed.

If CE is “Closing tendency between two aircraft in the air - two aircraft on conflict paths” then less than adequate recovery may take place due to any of:

Generic Contributor for Final Event is “Critical Event Recovery less than adequate”.

- **ATCO barrier less than adequate** – lack of awareness and/or ineffective intervention;
- **Pilot barrier less than adequate** – lack of awareness and/or ineffective action;
- **Aircraft barrier less than adequate** – ineffective aircraft systems and barriers (TCAS, aircraft maneuverability, etc.) ;
- **Providence less than adequate** – lack of chance, bad encounter geometry etc.

Table 2

Task Error	Detect	Solve	Deliver	Execute
Separation error	●	●		
Controller-Pilot Communication error	●		●	●
Radar Monitoring Error	●	●		●
Aircraft Observation/Recognition Error (TWR)	●	●	●	
Co-ordination Error	●	●		
Flight Progress Strip Usage Error	●	●		
Control Room Communication Error	●	●	●	
Aircraft Transfer Error	●	●		
Operational Materials Checking Error	●	●		
HMI Input & Functions Use Error	●	●	●	●
Training, Supervision or Examining Error	●	●	●	●

Reconstruction should try to finish the single branch of contributors at the organisational level. This is the level where real systemic, rather than individual safety improvements can be recommended.

To understand the real systemic factors, the reconstructed chains of contributors should try (if possible) to go down to the organisational conditions.

A useful guideline for this is that the lower level is playing the control role for the upper one – Figure 17. For example Local factors are controlling the behaviour of the Actors, Organisational factors are controlling Local factors and sometimes directly controlling Actors. A feedback loop should exist to inform the lower level about the state of the upper one and about the efficiency of the controls.

Any deficiency in the control and feedback loops should be considered as a contributor and should be depicted on the SOFIA work sheet.

Controllability as discussed in Chapter 1 was depicted in Figure 17 using the metaphor of the “rolling ball”. The more difficult it is to stop the ball rolling (less controllability) the more severe the safety occurrence.

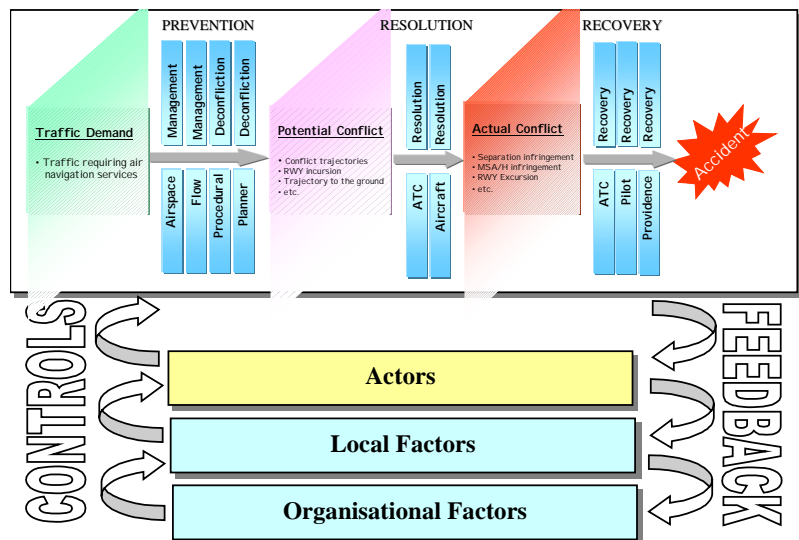
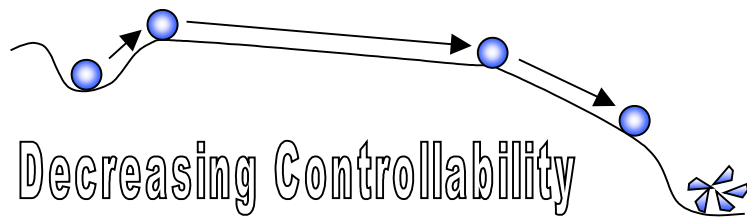


Figure 17

Such a checklist can be derived from the work of the professor Nancy Leveson.

1. *Inadequate Enforcement of Constraints (Control Actions):*

1.1 Unidentified hazards;

1.2 Inappropriate, ineffective or missing control actions for identified hazards:

1.2.1 Design of control algorithm (process) does not enforce constraints:

- Flaws in creation process;
- Process changes without appropriate change in control algorithm (asynchronous evolution);
- Incorrect modification or adaptation.

1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup):

- Flaws in creation process;
- Flaws in updating process (asynchronous evolution);
- Time lags and measurement inaccuracies not accounted for;

1.2.3 Inadequate co-ordination among controllers and decision makers;

2. *Inadequate Execution of Control Action:*

2.1 Communication flaw;

2.2 Inadequate actuator operation;

2.3 Time lag;

3. *Inadequate or missing feedback:*

3.1 Not provided in system design

3.2 Communication flow

3.3 Time lag

3.4 Inadequate sensor operation (incorrect or no information provided)

A generic checklist helps to determine if the control and feedback loops are contributors.

Event Reconstruction phase is defined in scope and depth by the following stopping rules:

-
1. Stop reconstruction at the building block, which describes the event/condition which is outside the control of the relevant organisation – for example “aircraft maintenance”;
 2. Stop the reconstruction at the building block for which a single remedial action could be allocated to a single responsible entity/person;
-

Chapter 6

Event Analysis

Answering the question WHY?

6.1 What is Event Analysis?

To assess the risk associated with the identified factors.

Event Analysis is the phase of the occurrence investigation process that should deliver the list of identified and analysed adverse factors.

6.2 How SOFIA supports Event Analysis?

Event Analysis is used to understand the safety occurrence causality. This is achieved by application of the following “5 golden rules for event analysis”:

1. Which are the events/conditions that increased the likelihood of the **Final Event**, or could increase the likelihood of another (different from the investigated one) safety occurrence? Use Hazard Symbol (double line bordered building block) to mark them on SOFIA work sheet;
 2. Identify if there are chains of direct contributors;
 3. Some of the blocks from the chain of direct contributors are hazards, but not all of them;
 4. Some hazards are outside the chain of direct contributors. Some hazards are not even linked to the final event at all;
 5. Blocks from a chain with at least one indirect contributor increase the likelihood of this safety occurrence.
-

6.3 Human Error Analysis

During the Event Reconstruction phase the Investigator identifies task errors – Table 2. These errors are the visible part of the human behaviour. To get into the invisible, cognitive part the Investigator can use the Human Error in ATM (HERA) technique, developed by EUROCONTROL Human Factors and Manpower Unit.

Then the Task Error building block will be composed of four layers:

SOFIA provides a link to the Human Error in ATM (HERA) technique.

- **Task Error** – What task failed?
 - **Error Detail (ED)** – What cognitive process was implicated in the error? HERA uses four Error Details domains – Perception and vigilance, Memory, Planning and decision making and Response execution;
 - **Error Mechanism (EM)** – What cognitive function failed, and in what way did it fail?
 - **Information Processing (IPs)** – How did the error occur in terms of psychological mechanisms?
-

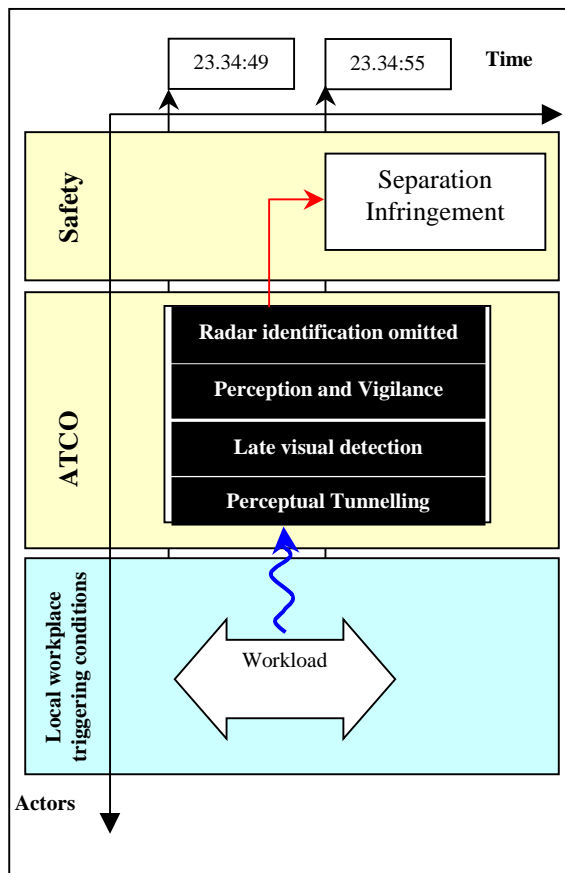


Figure 18

How SOFIA is depicting the HERA - related symbols?

HERA symbols are used in addition of the symbols from Figure 3 for more detailed analysis of the Human Error.

The symbols remained the same, but the inverse colour coding is applied – white text on the black building block background.

The example in Figure 18 shows the Task error “Radar identification omitted “ with the underlying cognitive levels:

- Error Detail domain - Perception and Vigilance
- Error Mechanism – Late visual detection
- Information Processing – Perceptual Tunnelling

Workload is an indirectly contributing Contextual Condition to the Error.

Once the four Error levels are determined, the analysis continues with the Error Context.

Error context describes all the surroundings of the Error – when did the event occur, who was involved, where did it occur, how did it occur and what information or topic did the error involve.

To describe the context of the error normal SOFIA symbols are used – Events/Conditions/Contributors types.

Chapter 7

Issuing Recommendations

Answering the question: WHAT TO BE DONE?

7.1 *What is the process of Issuing Recommendations?*

To decide on risk mitigation.

Issuing Recommendations is the phase of the occurrence investigation process that should deliver the list of the proposed recommendations.

7.2 ***How SOFIA supports Issuing the Recommendations?***

This is achieved by application of the following “4 golden rules for Issuing Recommendations”:

-
1. For each identified hazard use a safety assessment process to derive safety recommendation;
 2. Sometimes hazard-derived safety recommendations have nothing to do with this particular safety occurrence;
 3. Removing any of the building blocks from the chain of direct contributors prevents this particular safety occurrence. Is it feasible? Could this create another risk?
 4. Removing any of the building blocks from other chains could have decreased the likelihood of this particular safety occurrence. Is this decreasing enough? Is this feasible? Could this create another risk?
-

Annex A – All the golden rules at ones

FACTUAL INFORMATION GATHERING

1. Enter all identified information into the Sofia work sheet, using the appropriate building blocks;
2. Assign for them relevant moment in time;
3. Add links between building blocks and appropriate HEIDI elements
4. Check if all the relevant events and conditions are considered by answering to the question "what have been different in the system, compared with the normal operations?" Assess these deviations for their safety significance.

EVENT RECONSTRUCTION

1. The only Goal is to Improve Safety and not to apportion blame or liability;
2. Start from the final event and go step-by-step backwards, asking the question "why this happened?"
3. Try to identify as much contributors as possible to the event/condition using the contributor's' description. Do not proceed further until the all building blocks contributors are identified;
4. Which are the contributors that if removed could have prevented the analyzed building block? Use for them Direct Contributor correlation;
5. Which are the contributors that increased the likelihood of the analyzed building block, but which removal does not prevent it? Use for them Indirect Contributor correlation;
6. Which are the contributors that decreased the likelihood of the analyzed building block? Use for them Reductive Contributor correlation.
7. Two Building Blocks linked with the Direct/Indirect contributor symbol have to be immediately (causally) next to each other. Is it possible for something to be between them? If yes - introduce it on the work sheet.
8. Mark with the question mark any uncertainty on the type of contributor and contributors' existence. Put more effort to remove these uncertainties.
9. Check the temporal sequence of the building blocks by following the time line for each actor. This ensures the right sequence of events/conditions for the actor.
10. Check the temporal relations of events/conditions for different actors by following the vertical marked moments in time. This ensures the right sequence of events/conditions for the different actors.

EVENT ANALYSIS

1. Which are the events/conditions that increased the likelihood of the **Final Event**, or could increase the likelihood of another (different from the investigated one) safety occurrence? Use Hazard Symbol (double line bordered building block) to mark them on SOFIA work sheet;
2. Identify if there are some chains of direct contributors;
3. Some of the blocks from the chain of direct contributors are hazards, but not all of them;
4. Some hazards are outside the chain of direct contributors. Some hazards are even not linked at all to the final event;
5. Blocks from the chain with at least one indirect contributor are increasing the likelihood of this safety occurrence.

ISSUING RECOMMENDATIONS

1. For each identified hazard use safety assessment process to derive safety recommendation;
2. Sometimes hazard-derived safety recommendation has nothing to do with this particular safety occurrence;
3. Removing any of the building blocks from the chain of direct contributors prevents this particular safety occurrence. Is it feasible? Could this create another risk?
4. Removing any of the building blocks from another chains could have decreased the likelihood of this particular safety occurrence. Is this decreasing enough? Is this feasible? Could this create another risk?