A QUALITATIVE COMPARATIVE ANALYSIS OF SOAM AND STAMP IN ATM OCCURRENCE INVESTIGATION

Richard Arnold

LUND UNIVERSITY
SWEDEN

Date of submission: 2009-06-30

A QUALITATIVE COMPARATIVE ANALYSIS OF SOAM AND STAMP IN ATM OCCURRENCE INVESTIGATION

Richard Arnold

Under supervision of

Professor Sidney Dekker

ABSTRACT

Systemic Occurrence Analysis Methodology **(SOAM)** is promoted by Eurocontrol for the analysis of Air Traffic Management (ATM) occurrences. Systems Theoretic Accident Model and Process **(STAMP)** based on systems theory has been defined by professor Nancy Leveson (MIT) to explain systems accidents (accidents arising from the interactions among components rather than individual component failure). This research analyzes an ATM occurrence using SOAM and STAMP and compares their usefulness in identifying *systemic* countermeasures. The results show that SOAM is a useful heuristic and a powerful communication device but that it is weak with respect to emergent phenomena and non linear interactions. SOAM directs the investigator to consider the context in which the events occurred; barriers that failed and organizational factors; the "holes in the Swiss cheese", but not into the processes which created them, or how the whole system can migrate towards the boundaries of safe operations. STAMP directs the investigator more deeply into the mechanism of the interactions between system components, and how systems adapt over time. STAMP helps identify the controls and constraints necessary to prevent undesirable interactions between system components. STAMP also directs the investigation through a structured analysis of the upper levels of the system's control structure which helps to indentify high level systemic countermeasures. The global ATM system is undergoing a period of rapid technological and political change. In Europe the Single European Sky ATM Research (**SESAR**) and in the US the **NextGen** programs mean that the ATM is moving from centralized human controlled systems to semi automated distributed decision making. Continuous Descent Arrivals flown on datalinked 4D flight paths that are tailored to local constraints and timed for merging traffic require digital information sharing and Collaborative Decision Making on a grand scale, as well as Functional Airspace Blocks designed for optimal airspace efficiency and safety. Detailed new systemic models like STAMP are now necessary to prevent undesirable interactions between normally functioning system components and to understand changes over time in increasingly complex ATM systems.

TABLE OF CONTENTS

List of Figures

1. Introduction

Background

Dekker (2002) pointed out that during investigations; "cause is something we construct, not find." What people find out depends on where they look, and on how they weigh the value of particular pieces of information. Where they look and how they evaluate information depends on what they believe about how and why accidents happen. The acronym WYSIWYG (what you see is what you get) was coined in the field of computer science. Hollnagel (2007) noted that accident analysis seems to follow a similar principle: WLFIWYF (what you look for is what you find). Models are central to investigators understanding about how accidents occur. Different models lead to different conclusions about causes, and *countermeasures*: WYFIWYF (what you find is what you fix).

Hollnagel (2004) identified 3 basic classes of accident models, which inform accident analysis; the *sequence of events* model; the *epidemiological* model, and the *systemic* model. These models developed historically in the order above. Huang (2007) summarized the classes as described below:

1. *Sequential* accident models regard the accident process as a chain of events caused by operator or machine failures and the aim is to improve the reliability of weak components.

2. *Epidemiological* models regard the occurrence as a result of missing or weakened barriers, and the preventative aim is to install and strengthen barriers.

3. *Systemic* accident models regard the occurrence of accidents as a result of a system loosing control, and the focus is on helping the system to stay in control.

The definitions of these classes are not universally accepted, some researchers notably Reason (2008 p.93) take a different slant. Reason describes a system perspective as "any accident explanation that goes beyond the local events to find contributory factors in the workplace, the organization and the system as a whole." Reason (2008, p.95) makes his position clearer "Firstly I believe that all of the models described by Hollnagel meet the criteria for system perspectives. Second, they all have and have had their uses. Just as there are no agreed

definitions and taxonomies of error so there is no single right view of accidents. In our business, the "truth" is mostly unknowable and takes many forms. In any case, it is less important than practical utility". The second part of Reason's statement is relatively uncontroversial; each model produces a different perspective, and all of them may be useful depending on the purpose. However, several researchers notably Dekker (2006) and Hollnagel, Woods, and Leveson (eds. 2006) have a very different interpretation about what constitutes a *systemic* analysis. To avoid confusion about the term "systemic" I will use Hollnagel's (2004) classes of models.

SOAM

The primary accident model promoted by the Eurocontrol and ICAO technical publications for analyzing Air Traffic Management (ATM) occurrences[1] for the past 3 decades has been the Reason Model of organizational accidents (Eurocontrol 2005, ICAO 1993, 1998 and 2006). Eurocontrol introduced the Systemic Occurrence Analysis Methodology (SOAM) for Air Traffic Management (ATM) occurrence investigations in 2005. The Eurocontrol guidelines on the Systemic Occurrence Analysis Methodology (ESARR[2] Advisory material / guidance document EAM2/GUI 8, page 8) describe SOAM as follows:

"SOAM is a comprehensive process for analyzing data collected as part of a safety occurrence investigation, and for generating logical findings and recommendations. The methodology has been designed in accordance with Eurocontrol specifications, and to integrate with other phases of investigation, as outlined in the "Guidelines for Investigation of Safety Occurrences in ATM" (EATMP[3], 2003). SOAM is one of a number of accident methodologies based on the Reason Model of organizational accidents. Full implementation of the methodology is expected to improve the degree to which the key safety objectives of ESARR2 are met."

"The main focus of SOAM is on two key phases of the investigation process: Analysis of factors contributing to the occurrence, and the development of recommendations".

---

[1] An occurrence is defined as: „Accidents serious incidents and incidents as well as other defects or malfunctioning of an aircraft, its equipment and any element of the Air Navigation System, which is used, or intended to be used for the purpose or in connection with the operation of an aircraft, or with the provision of an air traffic management service or navigation aid to an aircraft."

[2] ESARR Eurocontrol Safety Regulatory Requirement

[3] EATMP European Air Traffic Management Program

SOAM Methodological Overview

The SOAM guidelines provide a description of the SOAM version of the Reason Model as shown below in figure 1. The following two paragraphs are a description of the Methodological Overview extracted from the guidelines (Eurocontrol 2005, page 22).

"SOAM is a process for conducting a systemic analysis of the data collected in a safety occurrence investigation, and for summarizing this information using a structured framework and standard terminology. As with some root-cause analysis investigation methods, SOAM draws on the theoretical concepts inherent in the Reason Model, but also provides a practical tool for analyzing and depicting the inter-relationships between all contributing factors in a safety occurrence.

Reason's original model has been adapted and refined within SOAM. The nomenclature has been altered in accordance with a "Just Culture" philosophy, reducing the implication of culpability and blame by both individuals and organizations. In SOAM, Unsafe Acts are referred to simply as *Human Involvement*, Psychological Precursors of Unsafe Acts as *Contextual Conditions*, and Fallible Decisions as *Organizational and System Factors*."

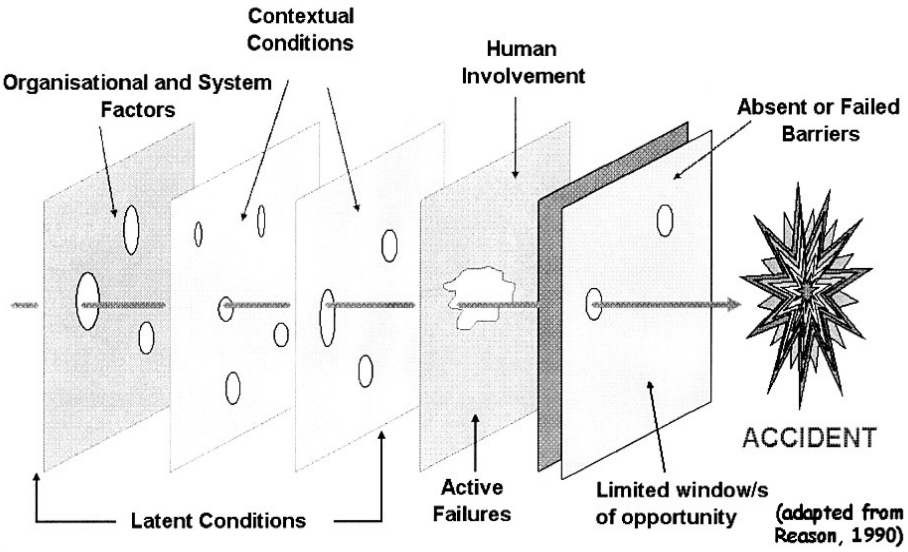


Fig 1 SOAM version of the Reason model (Eurocontrol, 2005)

The Reason model is commonly referred to as the "Swiss Cheese" model.

Increasing system complexity in ATM

From the end of Second World War until the turn of the century ATM changed relatively slowly. Even today the ATM system is essentially still a centrally controlled system in which human controllers separate and manage the flow of air traffic. Airspace is divided mostly along national boundaries and managed primarily by national Air Navigation Service Providers (ANSPs). This arrangement has reached its capacity and efficiency limit in many parts of Europe and across the developed world. European airspace is now in a period of rapid technological and political change. The Single European Sky (SES) initiative, Functional Airspace Blocks (FAB) and the Single European Sky ATM Research (SESAR) program are not driven primarily by a need to improve safety, but by the need to increase capacity and efficiency – safely. Hundreds of millions of Euros is being invested in these programs and a similar airspace modernization project is taking place in the United States SES equivalent NextGen.

The need to increase efficiency is no longer just a financial necessity; climate change and the need to reduce carbon dioxide and other environmental impacts are now also crucial. The Intergovernmental Panel on Climate Change (IPCC) 1999 report on Aviation and the Global Atmosphere stated that improvements in ATM and other operational procedures could reduce aviation fuel burn by 18%. The ATM influence over carbon dioxide emissions was estimated at 12%[4]. Substantial efficiency improvements are promised by technologies such as; automated arrival and departure sequencing tools to maximize the use of runways and airspace, Continuous Descent Arrivals (CDA), de-conflicted routings, automated gate (parking) allocation and integrated refueling and other ground services.

In 2007 the International Civil Aviation Organization (ICAO) urged all 190 member states to have Performance Based Navigation (PBN) implementation plans ready within two years. PBN essentially means a shift to more accurate and efficient aircraft trajectories by moving away from ground based navigation aids in favor of satellite guided area navigation procedures. Airbus and Boeing now build all their production aircraft with advanced Required Navigation Performance (RNP), which will be able to benefit from Continuous Descent Arrivals flown on datalinked 4D flight paths that are tailored to local constraints and timed for merging traffic. The pressure is now mounting for the national ANSPs to

[4] Source: Flight International, Environmental Special Report, 28 April 2009.

reorganize the way airspace is structured and upgrade the ATM system so that the aviation community can benefit from these technologies.

Over the last two decades satellite technology has revolutionized Communication Navigation and Surveillance (CNS). In the past aircraft relied on ground based navigational aids, the position of aircraft was relatively approximate and controllers took almost total responsibility for sequencing and separation. Today the position of aircraft is known very much more precisely, and pilots are increasingly aware not only of their own position but also the disposition of other traffic. Cockpit display of traffic information and automatic sequencing tools mean that the ATM system is gradually moving from *centralized human control* to *semi automatic distributed decision making*. Central in this transition is the change from *analogue* information such as hand written paper control strips and audio radio communications to *digital* electronic flight strips and data-links. Information about the position of aircraft and their control instructions (and a host of other digital information) will soon be fully exchangeable across a range of automated and semi automated digital technologies. In the near future the management of aircraft will rely on a Collaborative Decision Making (CDM) approach, in which ANSPs, airlines and airports all over the world will co-operate so that aircraft can fly optimal trajectories. This will require digital information sharing on a grand scale and optimal airspace design.

New technology changing the nature of failure

New technology, especially computer technology, has led to a dramatic increase in *interactive complexity*[5] and tight coupling[6] in many socio-technical systems. The replacement of mechanical and electro-mechanical devices with software has removed most of the physical constraints that limited complexity in engineered systems. In engineering and in complex socio technical systems a new vulnerability has *emerged* from the vast increase in the number of possible interactions between system components (Leveson 2002 & 2004, Cook 2004, Dekker 2005 & 2006, and Hollnagel 2008). U*nanticipated interactions between components* (physical or human), mean that the *system as a whole can now fail without the failure of any individual component*. "The *nature* of failure in complex socio-technical organizations is

[5] Interactive complexity does not mean only that the system has many parts, but also that they are connected in unexpected ways (Leveson 2002).

[6] In tightly coupled systems, intervention or substitution is difficult or impossible; disturbances propagate rapidly through the entire system leaving operators confused about the system's state (Perrow 1999).

changing… Safety and reliability is no longer the same thing (Leveson, 2002)". Nothing needs to be broken or missing for a complex system to fail; in fact all the components may be working exactly as designed or trained, but unexpected interactions and normal variability can still result in catastrophic failure.

Drift

At the same time as the complexity of socio-technical organizations has been increasing the last decade has also been one of globalization and the privatization of many public services, resulting in increasing competition. Faster cheaper better has become the mantra in many industries including ATM. Rasmussen's (1996) model of *drift* (fig.2) shows how *local adaptations* in response to these pressures drive a system towards the boundary of safe operations.

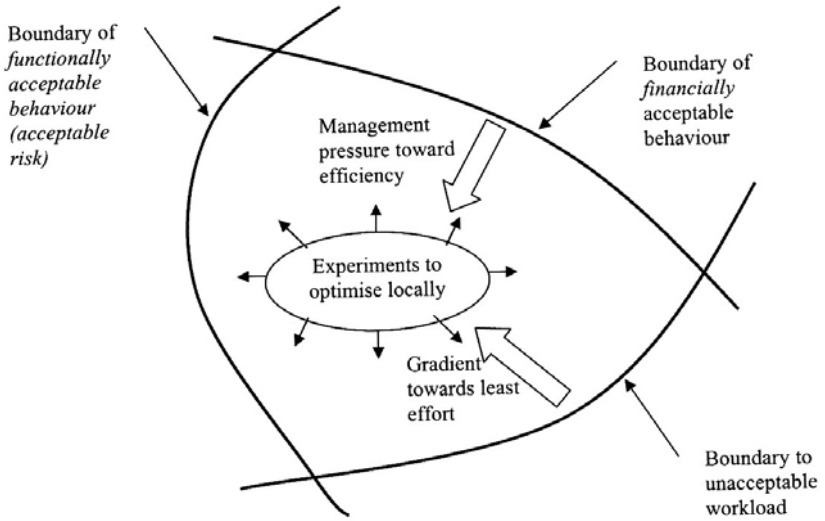


Fig. 2 Rasmussen's model of drift (Rasmussen, 1996)

Drift does not imply recklessness, negligent management, or lazy operators. Dekker (2006) described how "Deviations from standards become established as the new norm, and a lack of adverse consequences tends to re-affirm that the new norm is safe. *Incrementally over time and without realizing it*, people begin borrowing from safety" (my italics).

Rationale

By the 1990s the concept of barriers and defenses in depth; primarily using Reason's (1990) Swiss Cheese Model (SCM) of failure was well established in many socio-technical industries including ATM. However, a series of accidents around the turn of the century culminating in the Überlingen disaster in July 2002 did not fit the model particularly well, especially with respect to *drift*. In 2006 Eurocontrol published a Technical paper "Revisiting the Cheese Model" (Eurocontrol, 2006) to assess the strengths and weakness of the SCM. The analysis concludes with an acknowledgment of the contribution of the SCM, especially on its power as a communication device, but also noted that "*The SCM does not provide a detailed analytical accident model or a detailed theory of how the multitude of functions and entities in a complex socio-technical system interact and depend on each other*" and this "*may limit its use in analysis and as support for proactive measures"*. I have quoted the conclusions rather selectively, but the weaknesses identified suggest that methods of analysis which do address the detail *of how the multitude of functions and entities in a complex socio-technical system interact and depend on each other* may reveal some useful additional insights.

Dekker (2006, p. 82) acknowledged Hollnagel's classes and described how the "different models are good at explaining different things. But different models also have different problems and can be misleading in various ways. The sequence of events and epidemiological models imply a linear pathway. Epidemiological models do not account well for non linear interactions; they rely on "failures" up and down an organizational ladder".

Chain of events and epidemiological models of accidents may not provide adequate explanations for emergent phenomena. The reductionist approach; breaking systems into their components and examining their *reliability* does not account well for unanticipated non linear interactions. In short, *the system as a whole is more than the sum of its component parts*. Decades of Human Factors research have demonstrated that: "Accidents and incidents in complex systems are not caused by failures of individuals, but emerge from the conflux of multiple systems factors, each necessary and only joints sufficient. *The source of occurrences is in the system not in its component parts* (Eurocontrol, 2008 my italics)".

There seems to be something of a paradox in the Eurocontrol position. On the one hand it recognizes that "The source of occurrences is in the system and not in its component parts", but SOAM is based at least in part on the Reason Model of organizational accidents, which it

acknowledges "does not provide a detailed analytical accident model or a detailed theory of how the multitude of functions and entities in a complex socio-technical system interact and depend on each other" and this "may limit its use in analysis and as support for proactive measures". New technology is steadily increasing the complexity of ATM systems and this may mean that SOAM will soon need to be supplemented with additional analysis.

New Models

Around the turn of the century many leading human factors leading researchers (Woods and Cook (2002), Leveson (2004), Cook and O'Connor (2004), Hollnagel 2004 and Dekker (2006 b), Richard Cook (2004)) began calling for new models to better explain failures in increasingly complex systems. In essence they called for an end to the reductionist and dualist approaches (breaking systems down into their components, and systems *or* people (components). Rather than looking for barriers which failed or were absent, broken components or human error, instead they called for an explanation of emergent phenomena; *unanticipated interactions* between components and drift, in context and in complete systems - the systems perspective. Clearly, a model that accommodates these characteristics must be fundamentally different to the prevailing epidemiological model with its linear pathway, active failures and latent conditions. Two new systemic models (which meet Hollnagel's (2004) description of systemic) for analyzing complex socio-technical systems have been proposed; FRAM[7] and STAMP.

STAMP

Leveson (2008) quoted Einstein "without changing our patterns of thought, we will not be able to solve problems we created with our current patterns of thought". She made a compelling case that it is time for a paradigm shift in the way we analyze accidents and question their underlying assumptions. Leveson directly challenged all the fundamental assumptions of the epidemiological models:

1. The assumption that safety is increased by increasing reliability i.e. that "If components do not fail, then accidents will not occur".

[7] FRAM (Functional Resonance Accident Model) was proposed by Erik Hollnagel (2004). The model describes system *functions* rather than components or structures. Adverse events are accounted for in terms of *functional resonance* and *normal performance variability.* Resonance refers to interactions between functions.

2. The assumption that retrospective analysis of adverse events is required and perhaps the best way to improve safety.

3. The assumption that accidents are caused by chains of directly related failure events.

4. The assumption that accidents are caused by operator error.

5. The assumption that "rewarding "correct" behavior and punishing "incorrect" behavior will eliminate or reduce accidents significantly".

Leveson (2004) proposed STAMP a model based on basic *Systems Theory*. STAMP stands for Systems –Theoretic Accident Model and Processes. "Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interactions among components that result in a violation of system *constraints"* (Leveson 2007, my italics). In STAMP safety is viewed as a *control problem*. "The control processes that enforce the safety constraints must limit system behavior to the safe states implied by the safety constraints." "STAMP treats a system not as a static design, but as a *dynamic process* that is *continually adapting* to achieve its ends and to react to changes in itself and its environment". According to Leveson (2008), STAMP accounts for "social and organizational factors, such as; structural deficiencies in the organization, flaws in the safety culture, and inadequate management decision making and control. These are directly represented in the model and treated as a complex process rather than simply modeling their reflection in an event train". "Human error is treated as part of an ongoing process that is influenced by context, goals, motives and mental models."

Purpose of this research

The aim of this research is a qualitative comparative analysis of the (Eurocontrol) Systemic Occurrence Analysis Methodology (SOAM) and (Leveson's) Systems Theoretic Accident Model and Processes (STAMP), in Air Traffic Management Occurrence Investigation.

The research questions are:

1. **What are the *differences* between the results of analysis, of an ATM occurrence, using SOAM and STAMP?**

2. Does STAMP provide a *useful* perspective for analyzing ATM occurrences?

In Lund (Sweden) in March 2009 Nancy Leveson defended criticism of STAMP; quoting John Box “All models are wrong, but some of them are useful”.

The crucial point about a *systemic* analysis is that it should *help identify systemic countermeasures;* this is the definition of “useful” used in this research. Analysis which identifies individual or component failures is likely to treat only symptoms, it may prevent the *same* incident from occurring (for a while), but it is unlikely to reduce the number of incidents or contribute much to system safety overall in a complex socio-technical system.

2. Method

Single case study

The subject in this study is ATM occurrence investigation. ATM is a complex socio-technical system; intrinsically multifaceted and with blurred boundaries, which necessitates a detailed study. Single detailed case studies allow a deep understanding of a single case, but there are limitations on how generalized the key findings can be, or whether they are mostly limited to that single case. Increasing the number set by analyzing more occurrences would have consumed more resources than were available, but may be justified by the results of this study.

General Methodology

The general methodology used is Qualitative Comparative Analysis. The study is of a single ATM occurrence; N=1. Two variables are being compared SOAM and STAMP; the outcome of interest is their usefulness in identifying systemic countermeasures. The output from a SOAM analysis is a SOAM chart. The output from a STAMP analysis is a model of the hierarchical control structure, and sub models of the control and constraints at each level. Both techniques produce a framework for thinking about the occurrence intended to help "generate recommendations". Their usefulness in identifying systemic countermeasures is compared.

Case selection

In order to justify generalized conclusions in a single case study, case selection is crucial. Accordingly, a typical (garden variety) occurrence with a significant ATM contribution to a loss in separation was sought. The occurrence selected was identified by the Air Navigation Service Provider (ANSP) as an example of a typical ATM occurrence and was used as a case study for 60 investigators from many European countries at an international (closed) forum in Nov 2008. The people directly involved in the occurrence were available and willing to co-operate, the case was relatively fresh (7 months old) and detailed information including a full investigation report and a complete record of the voice and radar recordings was available.

De- identification

Safety in safety critical industries like ATM, always have a political dimension. Establishing a "Just Culture" in European ATM is still a work in progress. Accordingly, the ANSP

(rightly) protects its safety data from undue outside probing. The ANSP agreed to release the information from the original investigation and allow a limited re-investigation for this research under 2 conditions:

1. The data in the study had to be de-indentified.
2. The study shall not involve a comparison with the original investigation.

Accordingly, ´the data has been de-identified by substituting the aircraft call-signs with the aircraft types, and withholding the identities of the; ANSPs, ATM units, and operators involved. The airspace map on page x is fictional. The airway route names, navigation fixes and the general shape of the airspace have been altered, but the relationships between the players and relative positions of the routes and proportions of the relevant parts of the airspace are accurate. The airspace is in Western Europe. The Air Navigation Service Provider involved handles more than 3 million IFR flights a year and the occurrence happened in September 2008.

The de-indentified original investigation report is shown in the next chapter (Chapter 3). The recommendations have been deleted.

Limitations of conventional ATM investigations

Historically, ATC voice and radar display recordings are the starting point of most ATM reconstructions. ATC voice recordings are transcribed according to set of standard conventions. Conventional voice transcripts cover only one channel (often between only two of the many players) and do not illustrate how other system parameters were changing or how multiple activities overlap. The time base is often compressed and sections of time without speech taking place omitted. A time-line that shows periods of apparent inactivity (even inactivity may be poignant), but also shows periods of intense activity with sufficient discrimination is problematic. The transcript can be broken into episodes with a time base relevant to the data being examined, and highly detailed analysis of voice recordings "conversational analysis", which examines tone and sentence construction sometimes reveals useful information about crew co-operation (Nevile and Walker, 2005). However, this level of discrimination requires specialist skills that are only available under extraordinary

circumstances. Additionally, "elbow co-ordination"[8] between Radar Controllers and Planners and even between adjacent sector control consoles is currently unrecorded.

Deciding when a reconstruction should start and end has important implications. In practice ATM reconstructions usually begin 2 or 3 minutes before the loss of separation being investigated (to establish a simple traffic picture prior to the event), and ends when standard separation is re-established. Prior to and after the occurrence there is no separation loss and everything is therefore deemed to have been safe. The apparently simple decision about where to start and end the reconstruction biases the whole investigation towards the last moments of an occurrence; and towards a sequential interpretation of causation. *History and context,* safety culture, safety resilience, and emergent phenomena like drift are easily omitted…

A reconstruction needs to illustrate not only history and context but also overlapping communications, between multiple players over multiple channels and data about other parameters for example; distance between targets or to a sector boundary or fix, vertical separation, rates of climb, speeds, remaining fuel, deteriorating weather or visibility, conflict alerts, display information, traffic load, focus of attention, etc; "reconstruct the unfolding mindset "(Dekker 2006), but this kind of hard analytical work is time consuming and until recently has been absent from most AOI.

Re-analysis using only the information from existing sources limits the data set to that used in the original investigation. Additionally, original reports do not necessarily reveal the accident model/s that was/were used to gather or analyze the data. Direct comparison of different analytical perspectives without re-investigation is therefore problematic. The original investigation report is comprehensive and illustrates many parameters interacting over time, with particular attention to the voice and radar recordings and provided the Human Factors data necessary under the ICAO SHELL[9] structure. However, in order to provide enough information to be used for both SOAM and STAMP a limited re-investigation was necessary.

[8] Pointing, flagging strips and unrecorded spoken communications
[9] SHELL stands for: Software, Hardware, Environment, Liveware, Liveware (the ICAO Human Factors model)

Objectivity

Heisenberg's uncertainty principle can be explained by the statement that; "the measurement of position necessarily disturbs a particles momentum, and visa versa – i.e., that the uncertainty principle is a manifestation of the observer effect". A similar problem arises during comparative analysis. Direct comparison requires separate analysis of the same event using different techniques, but analysis of an event inevitably involves individual bias (even if only subconsciously) and may also affect the second analysis. Analysis of the same event by different individuals using different models will involve individual biases, so absolutely unbiased direct comparisons are impossible.

There is no view from nowhere and therefore no objective reality. Accordingly, so that a reader can consider the persuasiveness of the conclusions it is necessary to be clear about how the data being analyzed was collected and to leave a trace, so that the logic of the analysis can be followed - transparency.

How the data was collected

The model of analysis used in the original investigation was not disclosed. Re-investigation was necessary to collect information about history and context, and to provide an "independent" account of the occurrence which could be analyzed using SOAM and STAMP. An account of an occurrence can be provided by an investigation based on the principle of "Local Rationality". The Local Rationality Principle (summarized after Dekker 2006) is that:

"What people do, where they focus, and how they interpret cues, *makes sense from their point of view*, their knowledge and understanding; their time and resources, at the time…"

What people do is a function of what they know, their available resources and what their goals are. A crucial part of the Local Rationality principle is that people are not "unlimited cognitive machines"; their rationality is bounded. They cannot know or see everything at the same time. Accordingly, there is a big difference between observable data and available data, and even inert knowledge and active knowledge (current understanding). People in operational work do not have unlimited time or resources, they have; multiple inputs, multiple tasks, multiple goals, and limited time and resources – *bounded rationality*.

Local Rationality is a principle of investigation rather than a model of analysis. An investigation using local rationality makes it possible to produce a "Locally Rational Occurrence Scenario" (an account) that is not dependent on a particular accident model, which can then be analyzed using SOAM and STAMP. A locally rational account is not a view from nowhere, *but the view is disclosed and it is independent of SOAM or STAMP* (The Locally Rational Occurrence Scenario is shown in Chapter 5).

In order to provide a locally rational account (Locally Rational Occurrence Scenario) it was necessary to make an operational area survey and interview the people involved in the occurrence.

The first step in preparing the re-investigation was a careful study of the original report (shown in Chapter 3).

Operational area survey

A survey was made of the operational area in the Area Control Centre. The equipment and working arrangements at the console involved in the occurrence was explained and photographed. *Normal operations* were observed, discussed and described. A limited description of the operational area obtained during the operational survey is the subject of Chapter 4.

Interview structure

Interviews were conducted with; the Radar Controller, the Planner, and the Unit Safety Manager (in that order) involved in the occurrence. The interviews process proceeded as follows:

The account from the original investigation was divided into 4 episodes:

1. **History and context:** The working arrangements, airspace and procedures, configuration of equipment and people; descriptions of the tasks being performed, roles and responsibilities.

2. The situation leading up to the occurrence - **Pre Short Term Conflict Alert** (**STCA).**

3. The situation at and immediately after the occurrence - **Post STCA.**

4. **Counterfactuals**: What might have helped them get the right picture? What; could, should or would have helped?

5. **Miscellaneous**: The SHEL Checklist, Critical Incident Stress Management (CISM), Safety Culture, Hierarchy, Organizational factors, Team Resource Management (TRM), Safety nets, Future developments.

Before the interviews a series of questions were prepared to probe each episode accordingly.

Episodes 2 and 3 were analyzed according to Ulrich Neisser's perceptual cycle to identify moments of special interest:

1. **Shifts in behavior**; especially communications which show that people have realized that the situation has changed.
2. **Actions to influence the process:** Actions (or lack of actions) that indicate what people thought was going on.
3. **Changes in the process:** System information (including alarms) that point to the human behavior that is going on around them; behavior that precedes or follows it.

Questions to probe these moments were derived from Gary Klein's work on Natural Decision Making (Klein, 1998); adapted to "*enter the controller's tunnel / reconstruct the unfolding mindset* "according to Dekker (2006, see fig 3 below).

Fig 3 Tunnel figure

The interviews questions were scripted but there were supplementary questions for clarity and many answers were supported with hand drawings (these are not shown). Other areas of interest which were raised during the interviews were explored. The interviews were not tape recorded but hand written notes were taken and the drawings were retained. A summary of the questions and answers "record of interviews" were typed afterwards from these materials.

As an investment in common understanding, a draft of the "record of interview" was supplied to the each interviewee, and returned within two or three days; there were only minor alterations for accuracy or tone. Each "record of interview" in this study is the agreed (de-identified) summary of the interview. The records of interviews (summaries of the questions and answers) are shown in Annexes A, B and C.

Hard Facts

A replay of the occurrence with simultaneous Radio Telephony (RT) and the radar data displayed on a laptop computer was available. RT and radar data from *all* the aircraft in controllers' area of interest were studied (not just the two aircraft directly involved). Screen shots of the minutes leading up to the incident and the incident itself were also made available; the position and speed of all the traffic could be studied at critical moments. Some of the screen shots had to be deleted due to de-identification, but radar screen shots were the source of the numerical data (hard facts) in this report and were used in the "time line of significant events" Fig 5 (page 37).

The facts in the original report are entirely consistent with the information obtained in the re-investigation and are undisputed.

3. Original Investigation Report

Infringement of separation between

B738[10]

&

A319

Area Control Centre - Blue

29 Sep 2008, 15:38:30 UTC

[10] The aircraft call-signs have been substituted with the aircraft type identifier; B738 stands for Boeing 737 800 series and A319 an Airbus 319.

Structure:

1. **Occurrence**
2. **Investigation documents**
3. **Chronology of events**
4. **Meteorological conditions**
5. **Technical aspects**
6. **Staffing**
7. **Traffic volume**
8. **Radiotelephony procedures**
9. **Procedures**
10. **Causes and HERA analysis**
11. **Evaluation**
12. **Risk assessment**
13. **Measures to be taken**

1. Occurrence

On 29 September 2008 at 15:38:30 (all times in UTC), an infringement of separation occurred at ECHO between A319 and B738. The infringement of separation occurred in the Sector No.1Top. Sector No.1 was working in a 3 - sector configuration[11].

> **A319**, IFR from XXXX to YYYY was cruising at FL 390 on the route segment **MIKE - CHARLIE** and was on the control frequency of **Yellow sector.**
>
> **B738**, IFR from WWWW to ZZZZ was climbing from FL370 to FL390 on the route segment **WHISKY - ALPHA - BRAVO** and was on the control frequency of **Sector No. 1 Top.**

The traffic volume prior to the incident was medium with normal complexity. There were about 6 or 7 entries per 10 minutes. The controller had been working at this position for 15 minutes.

At 15:35:26, A319 was transferred from Sector No.2 directly to Yellow Sector. This procedure is quite common since the flights MIKE – CHARLIE are in the Sector No.1 Top airspace only for a short period of time and usually do not constitute relevant traffic.

At 15:36:54, shortly after identification, A319 requested a level change to FL390. One minute later, B738 was cleared for FL390 after further coordination. In doing so, the controller failed[12] to see the restricting traffic A319. The distance between the two aircraft was 7 NM. B738 was about 3 NM, A319 about 5 NM from the crossing point of their tracks. Twenty-five seconds after the clearance, the level change of B738 could be discerned. At this point in time, the aircraft passed the crossing point. B738 had A319 in sight. It is conceivable that B738 delayed climbing until their tracks diverged. The two aircraft passed each other at the crossing point at 15:38:25 at a distance of 0.9 NM and 900 ft.

Traffic information was not provided. The controller did not intervene since he was convinced that the aircraft had obtained TCAS RAs and that it would be counterproductive to issue a possibly contradictory air traffic control instruction. His judgement of the situation was based on the tracks already having diverged by 2 NM.

At 15:38:25, separation was infringed. At 15:38:50, lateral separation was re-established at 5.3 NM.

The next proximity was documented at 15:38:30, with a distance of 1.4 NM / 800 ft. The prescribed minimum distances are 5 NM and 1000 ft. Afterwards, the lateral distance increased and vertical distance decreased within the separation criteria to 600 ft.

---

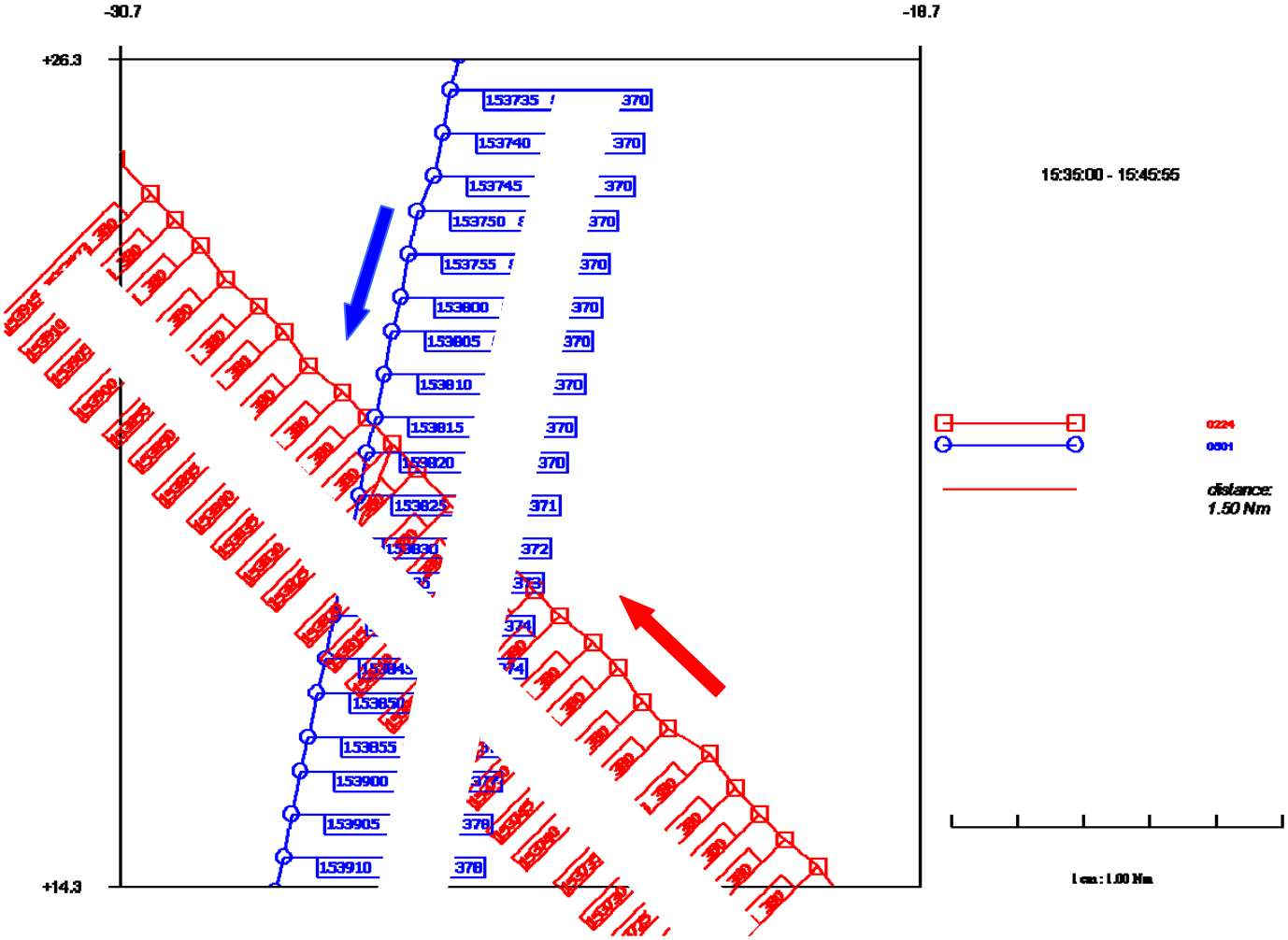
[11] Sector No.1 Top vertical limits FL355-600. There are two sectors beneath it with the same lateral boundaries but vertical limits: Sector No.1 High FL345-355 and Sector No.1 Low FL245-345.

[12] **"**Finding out what people could or should have done, does not explain *why* they did what they actually did".

"Counterfactuals are products of hindsight" Sidney Dekker (2002).

STCA emitted an alarm from 15:38:35 to 15:38:40 in Prediction Mode (blue), 10 seconds after the aircraft had passed the crossing point, since it was only then that the relevant parameters were met.
from 15:38:40 to 15:38:50 in Current Mode (red),
and from 15:38:50 to 15:38:55 in Prediction Mode (blue), each time with the quality "diverging".

According to the available data, no TCAS RAs were generated and thus were not reported.
When asked after the occurrence, B738 said that he had received TCAS information but it is not clear which kind of TCAS information. It was apparently the display of the traffic on the TCAS display.

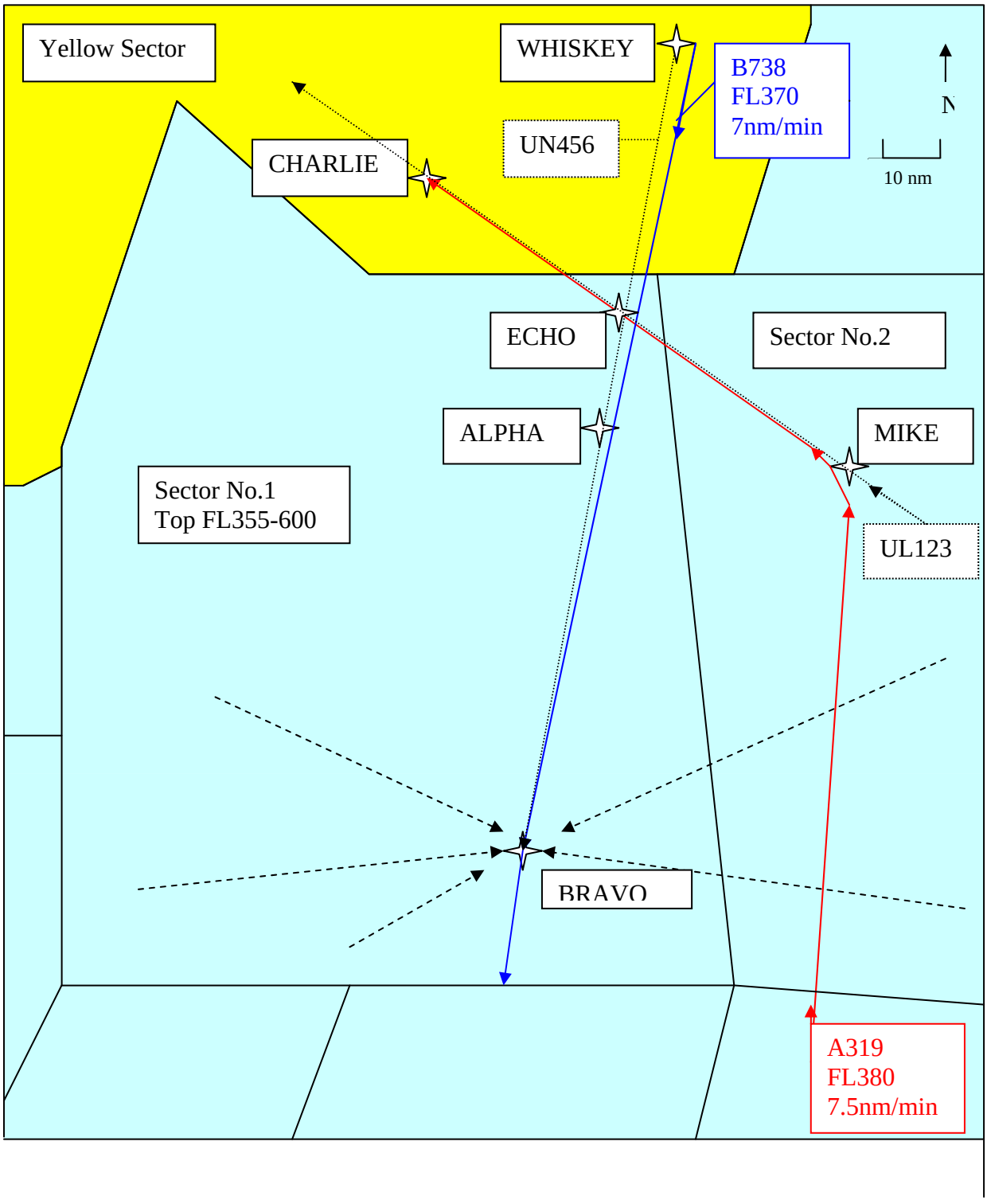


B738 is in Blue, A319 Red (Call-signs have been deleted)

After the infringement of separation, the air traffic controller was replaced by another controller. He declined the offer for CISM counselling.

Airspace Map

Flight paths of; B738 in Blue, A319 in Red.



2. Investigation documents

Position log
Break schedule
Controller / supervisor questionnaire
Flight progress strips
Transcript of radiotelephony communication
Evaluation of flight list interpreter
HERA analysis
LEGREC recording and plot
STCA analysis
Assessment sheet

3. Chronology of events

Time	Station	Text
15:34:20	B738	Radar good day B738 flight level 3.7.0.
15:34:26	Radar	B738 Radar hallo you´re identified.
15:36:54	B738	Radar B738 request.
15:36:56	Radar	Go ahead Sir.
15:36:57	B738	Any chance flight level 3.9.0. Sir?
15:37:00	Radar	Stand by short.
15:37:29	B738	And ah Radar B738 any report of turbulence ah flight level 3.9.0.?
15:37:34	Radar	No turbulence reported at that level on this freq.
15:37:37	B738	Thank you.
15:37:53	Radar	B738 climb flight level 3.9.0.
15:37:57	B738	Climbing flight level 3.9.0. B738.
15:38:25		**Separation is infringed for the first time, 0.9 NM 900 ft**
15:38:30		**1.4 NM 800 ft**
15:38:35		**First STCA alarm (blue), 2.3 NM 700 ft**
15:38:40		**First STCA alarm (red), 3.3 NM 600 ft**
15:38:45		**Last STCA alarm (red), 4.3 NM 600 ft**
15:38:50		**Horizontal separation has been re-established**
15:38:55		**Last STCA alarm (blue)**
15:41:52	Radar	B738 from Radar?
15:41:55	B738	Go ahead Sir B738.
15:41:56	Radar	Ah did you get an ah TCAS ah alarm during your climb?
15:42:00	B738	Yes Sir.
15:42:02	Radar	Roger.
15:42:06	B738	But we also had him visual.
15:42:08	Radar	Roger thank you.
15:45:44	Radar	B738 contact radar on x.x.x. decimal y.y.y. good bye.
15:45:50	B738	x.x.x.y.y.y. B738 bye bye.

4. Meteorological conditions

At the time of the incident, there were no significant meteorological conditions in the sector concerned. Another aircraft did request a different flight level due to turbulences, but at the levels of the two aircraft concerned no turbulences were documented.

5. Technical aspects

Technical problems or failures were not documented in direct connection with the incident.

6. Staffing

Radar controller Sector No.1 Top:

Third day of duty, late shift, 14:15 – 21:45, 83 minutes on duty, for 15 minutes at working position Sector No.1 Top, break: 15:45 – 16:15

Sector No.1 Unit endorsement since: May 2000

The controller had been fully briefed and was current.

7. Traffic volume

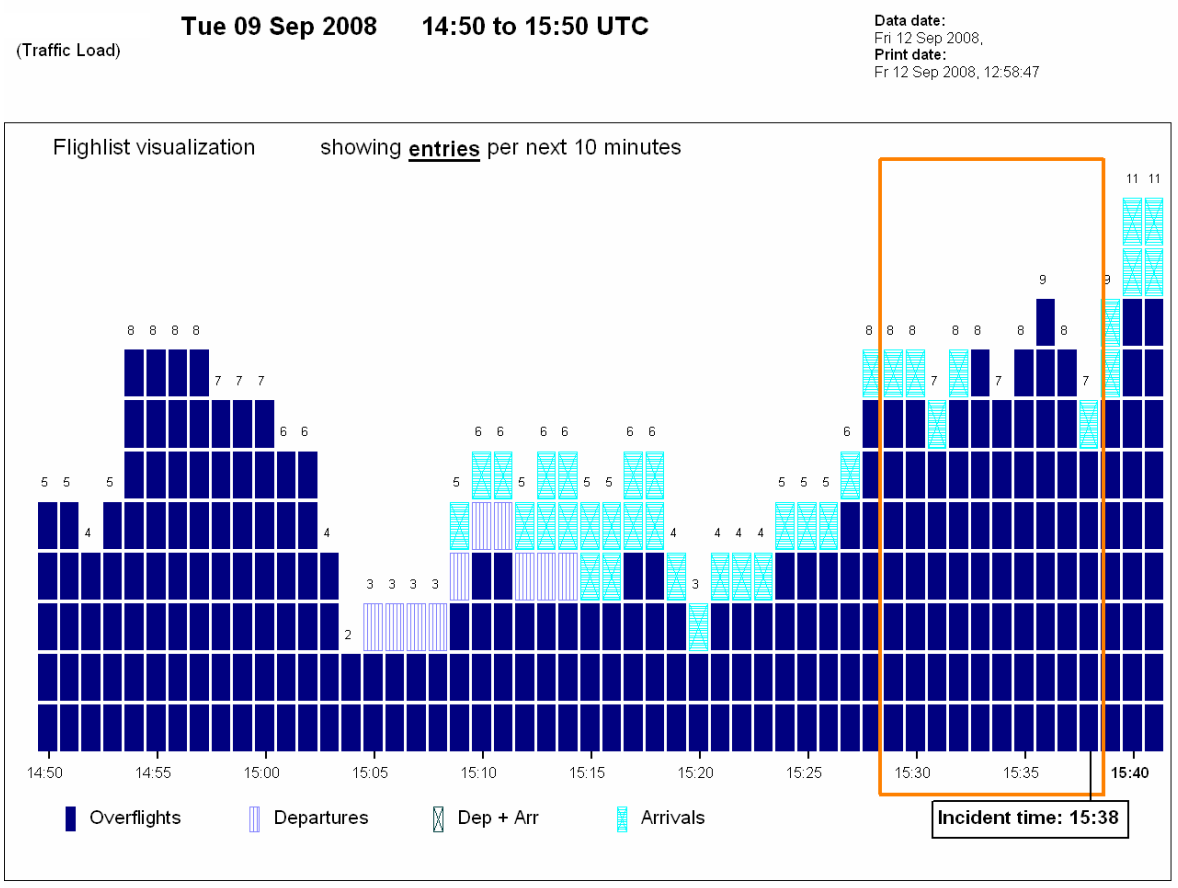
According to the controller, the traffic volume was medium with normal complexity prior to, directly before and during the incident.

The capacity default value for Sector No.1 Top is 49 aircraft per hour. From 14:50 to 15:50, 40 aircraft entered the sector, of which 11 were relevant to the controller during the 15-minute period from taking over the position to the incident. During this period of time, a medium traffic volume prevailed with an average of 6 entries per 10 minutes. Most of the flights were over-flights. This traffic mix is typical of the sector.

An increase in traffic volume was documented directly after the incident. The flight progress strips were probably already at hand at the working position thus heralding the imminent increase in traffic so that the controllers might have been occupied with analysis and planning activities.

Five aircraft were on the frequency at the time of the incident.

According to the available data, the controller's judgement of the situation was correct and logical.



8. Radiotelephony communications

Radiotelephony communications were carried out according to the rules and with a headset.

9. Procedures

No procedural errors were committed.

10. Causes and HERA Analysis

This infringement of separation was caused by the fact the controller failed to consider A319 as relevant traffic in connection with the climb of B738.

Error #1:
Error Description: The ATCO cleared B738 through the level of A319 without considering that traffic
Error Detail: Perception & Vigilance
Error Mechanism: No detection of visual information
Information processing: Monitoring failure
Contributing Factors: Traffic & airspace (other: one a/c not on own frequency) Weather (other: turbulences), Personal Factors (distracted by personal thoughts)

11. Evaluation

The controller had been working at the Sector No. 1 Top position for 15 minutes. Traffic was normal and moderate. Due to the traffic situation, it can be assumed that the controller quickly and comprehensively adapted to the situation in the sector.

The flight progress strips of a slight traffic peak to be expected 20 minutes later were already available at the working position at this time and the controllers were attending to analysis and planning activities for this peak. B738 had to be considered in relation to another aircraft, marked as crossing at FL370 over BRAVO.

The second aircraft involved in this infringement of separation, A319, had already been transferred from the Sector No. 2 to the Yellow Sector at 15:35, i.e. even before B738 requested FL390. This is not an official procedure but it has proved to be practical in the past and is common practice since the aircraft cover only about 15 NM in the upper corner of the Sector No.1 when flying on the route segment MIKE – CHARLIE of UL123. These flights do not normally constitute relevant traffic, unless they have to be considered for any climbs on UN456. But this happens only in exceptional cases.

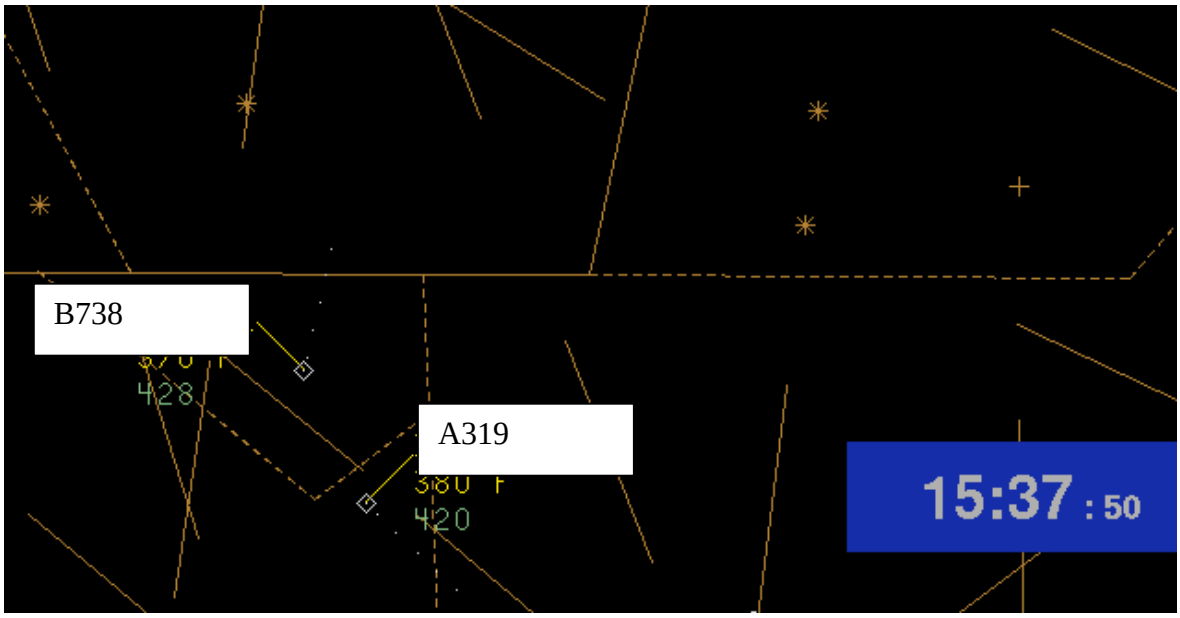
At 15:36:54, shortly after his identification, B738 requested a level change to FL390.

Since B738's request for FL 390 also solved the separation problem over BRAVO, the controller readily issued the clearance. This circumstance – in combination with A319 not being on the controller's frequency – formed the basis for this infringement of separation. In their statements, both controllers said that they might have been more "aware" of this flight and might have considered it as traffic in relation to B738 if they had actively identified it on their frequency.

Safety Management is of the same opinion. The case will therefore be presented in the Safety Panel with the request to publish a recommendation to this effect for air traffic controllers.

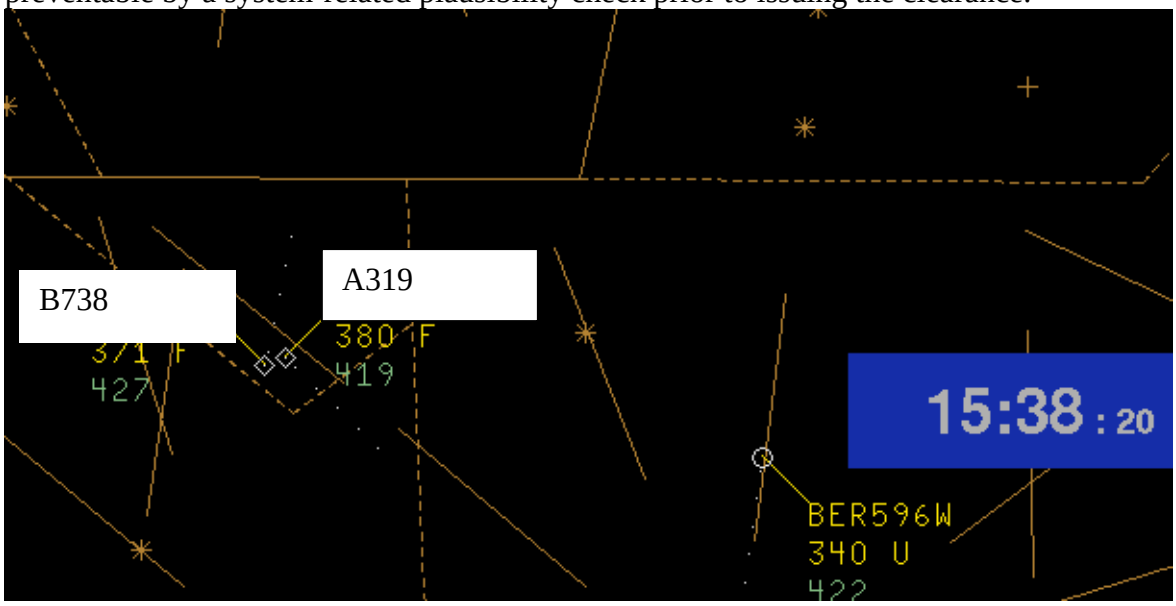
Another contributing factor was the controller's mental preoccupation with the quality of the teamwork prior to his break; in his opinion, the coordinator's planning had not been appropriate to the situation which put him as the radar controller unnecessarily under pressure. (HERA CC.: Personal Factors – distracted by personal thoughts)

At 15:37:53, B738 was cleared for FL390 after further coordination. In doing so, the controller failed to see the restricting traffic A319. The distance between the two aircraft was 7 NM. B738 was about 3 NM, A319 about 5 NM from the crossing point of their tracks.

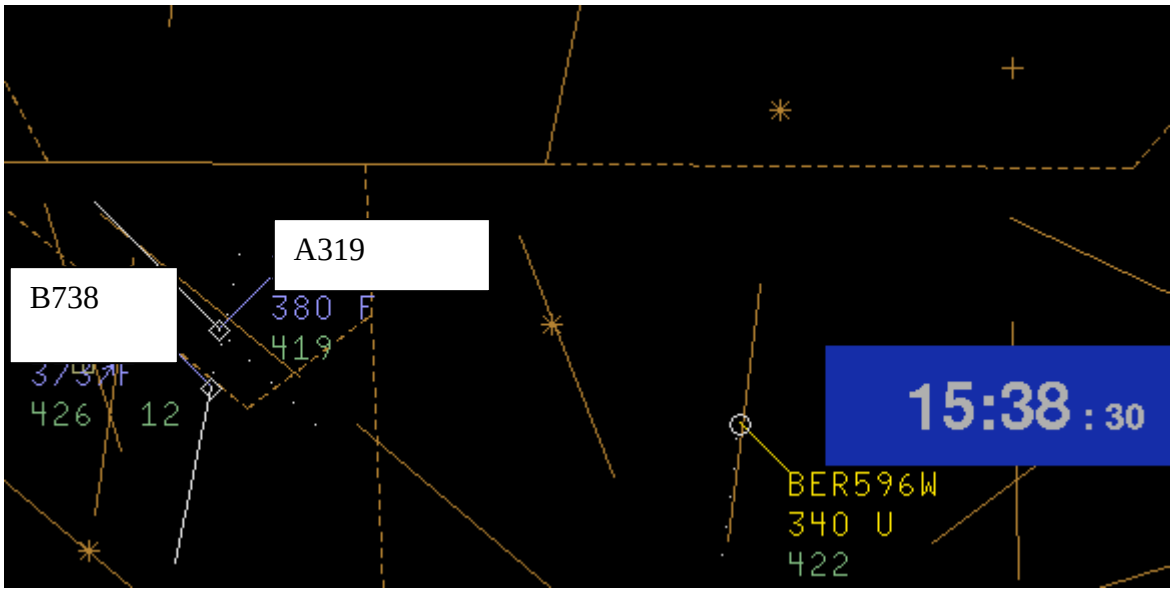


Twenty-five seconds after the clearance, the level change of B738 could be discerned, at this point in time, the aircraft passed the crossing point. B738 had A319 in sight. So it is conceivable that B738 delayed climbing until their tracks diverged. The two aircraft passed each other at the crossing point at 15:38:25 at a distance of 0.9 NM and 900 ft.

From the view of the investigator, this is a typical "blind-spot" case. Human errors of this kind where flights relating to a clearance are left completely out of account may only be preventable by a system-related plausibility check prior to issuing the clearance.



At the time of the above screenshot, the controller was not yet aware of the situation.
It was STCA that signalled the situation to him. The STCA alert was triggered according to the parameters.
Traffic information was not provided. It would have made sense to give A319 traffic information but this aircraft was already on the Yellow Sector frequency. The controller did not intervene since he was convinced that the aircraft had obtained TCAS RAs and that it would be counterproductive to issue a possibly contradictory air traffic control instruction. His judgement of the situation was based on the tracks already having diverged by 2 NM.



In an analysis meeting, the controller logically explained his judgement of the situation. Any controller action would have served no useful the purpose. This is why this item received 0 point on the assessment sheet. (No intervention required)

No TCAS RAs were generated according to Mode S information. This is also in keeping with the TCAS logic. The tracks were diverging before the level change took place. This is why no RA was triggered. B738 apparently had the traffic on his TCAS display and also in sight. A319 did not become aware of the incident.

12. Classification

According to the criteria of the assessment sheet for infringements of separation caused by ATC, this incident is classified as

Significant

Reasons:

All relevant pieces of information were available but the problem was not recognised. The controller became aware of the problem through STCA. The problem was solved by chance. Remaining separation 50%+ vertical distance. Intervention was not required and would have served no useful purpose.

13. Measures to be taken and recommendations

Deleted

4. Operational area survey

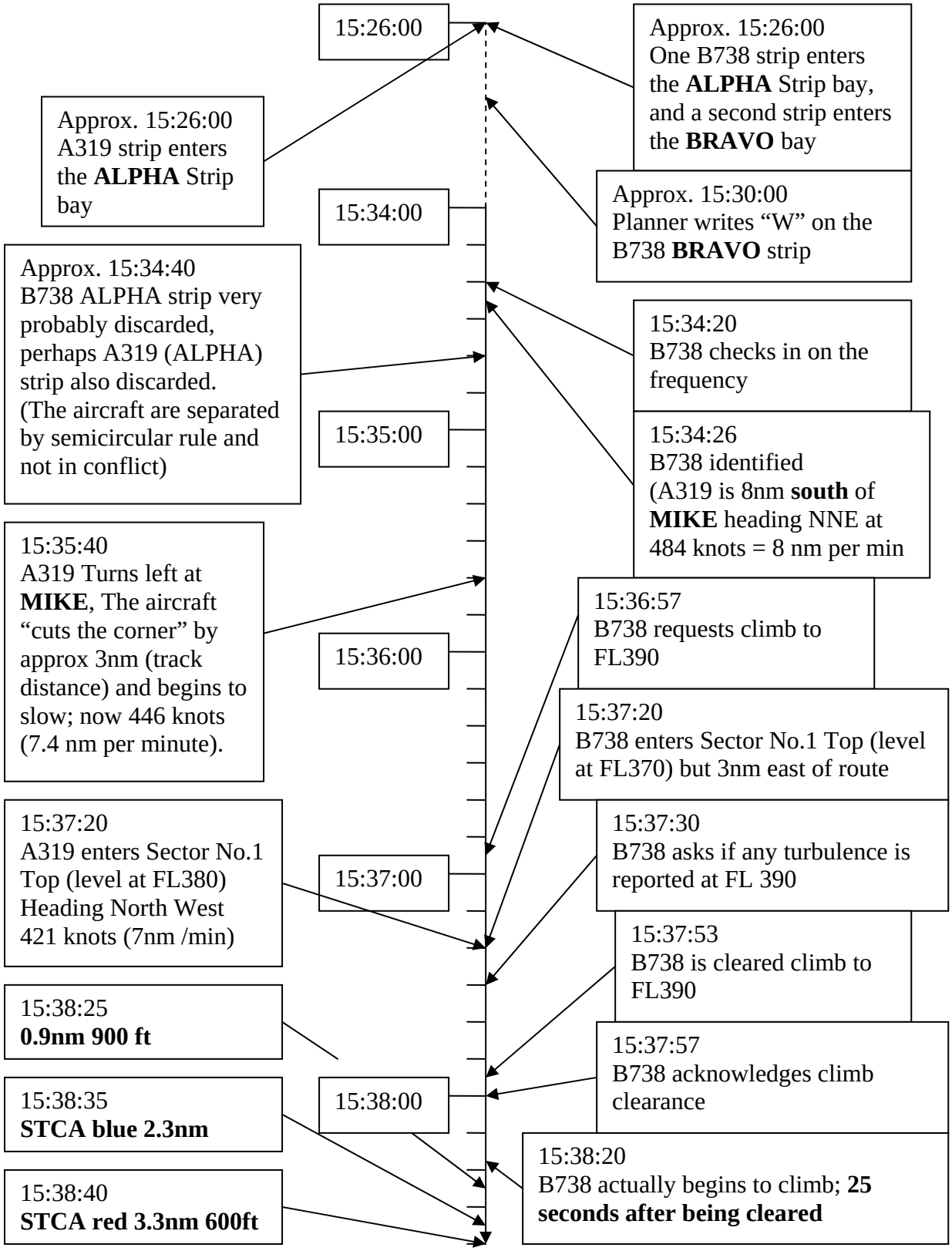
A plan of the Operations room showing the disposition of all the sectors, supervisor stations, Flight Data preparation areas, and controller working positions was provided (but has been deleted due to de-identification). Approximately 60 people work in the Operations room at any particular moment. The room is staffed 365 days a year, 24 hours a day.

The physical process of paper flight strip handling from preparation by the flight data personnel through the controller strip bays until discarded was traced and photographed. The flight strips are prepared by the flight data personnel and placed in a chute which guides them into the appropriate controller strip bay 10-15 minutes before the aircraft enter the sector's boundaries.

The radar display options were demonstrated and photographed; these are set to suit individual controller preferences. There are two height filter options. A height filter can be set to filter out all aircraft at selected Flight Level. In the Sector No. 1 Top; this is usually set to filter out all aircraft 5-10 thousand feet (5-10 flight levels) below the base of the sector's vertical boundary. A second filter; the Brightness Level Selection (BLS) can be selected so that all aircraft *within* a selected level span are displayed with yellow labels; aircraft below and above this second filter are displayed with grey labels. The overall effect is that aircraft inside the sector's vertical limits are easy to distinguish from those below it. ***However, aircraft above the sector's lower vertical limit that are outside the lateral boundaries are displayed exactly as those inside the sector.*** No conventional commercial aircraft fly *above* the sector's vertical limit (Flight level 600).

In the same building adjacent to Area Control Centre (ACC) active at the time of the occurrence, construction and testing of a completely new (ACC) is taking place. The new ACC is due to become operational approximately 10 months after the date of this report and will replace the existing centre. It is equipped with "glass" digital electronic flight strips, state of the art radar displays, and new communications and information display interfaces. This area was also inspected and photographed (the photographs have been deleted due to de-identification).

Fig 5 Timeline of significant events



5. Local Rationality Occurrence Scenario

The original investigation report provided a comprehensive account of the occurrence and the facts are undisputed. The re-investigation, concentrated on history and context and attempted to "unfold the developing mindset" of the two controllers using the principle of local rationality.

"The point of an investigation is not to find where people went wrong; it is to understand why their assessments and actions made sense at the time"
Sidney Dekker (2002, p.65)

Radar Controller "record of interview" (Page 69)

Q10. When did you first become aware of the problem?

My first indication that I had a problem was when the STCA went off – ***until that point A319 had not entered my consciousness.***

In a Locally Rational Occurrence Scenario this data is crucial. *The central challenge is to explain why the presence of A319 did not enter the Radar Controller's consciousness prior to the STCA.*

"When people loose situational awareness, what replaces it?"
Sidney Dekker (2006)

Two specially selected, rigorously trained, licensed and current, experienced, highly motivated, professional Air Traffic Controllers were working at the time of the occurrence. All the relevant equipment was functioning perfectly and they were diligently performing the tasks that they had been assigned. They were "normal people, doing normal work". No training was in progress, they were not fatigued and they were not overloaded.

"The reconstruction of mindset begins not with the mind; it begins with the circumstances in which the mind found itself."
Sidney Dekker (2006)

1. Standard company regulations require that aircraft be transferred to the sector frequency 3 minutes before they enter the sector's airspace. When aircraft check in on the sector frequency they *report their flight level* and are *identified* (their reported or expected position is correlated with the position displayed on the radar and the controller accepts responsibility for separation). A check mark (tick) is annotated on the flight strip to indicate that it is on the frequency, and the reported flight level is cross checked with the level on the strip and on the radar display. Identification is a significant cognitive task. Both controllers and the Safety Manager stated that taking the aircraft on to the control frequency and identifying the traffic "*actively engages the controller's attention*". This is not speculation. To anyone with domain experience it stands out like the Eifel Tower. This is exactly the process that B738 followed and it can be traced in the transcript on page 29 in the original report:

15:34:20	B738	Radar good day B738 flight level 3. 7. 0.
15:34:26	Radar	B738 Radar hallo you're identified

B738 unequivocally "entered the Radar Controllers consciousness".

2. UL 123 transits through Sector No.1 airspace for 15 nm. Commercial jet aircraft at the relevant altitudes cruise at approximately 7.5nm per minute, so are usually in the Sector No.1 airspace for only 2 minutes. Provided there is no change in altitude aircraft on UL123 are procedurally separated from traffic on UN456 by the semicircular rule. Accordingly, A319 was transferred directly from sector No. 2 to Yellow Sector. At the time of the occurrence this was not an official procedure, but it had been the accepted practice for at least 5 years. After the occurrence this practice was formalized, and became an official local instruction. Clearly, if it takes only 2 minutes to cross the airspace it is impossible for Sector No.1 to accept the aircraft on frequency and transfer them to the next sector (Yellow) 3 minutes before the sector boundary.

3. The flight strips are usually retained in the strip bays until the aircraft they represent have passed the position fix denoted by the bay. When aircraft have passed the final fix in the sector's airspace and 3 minutes before the boundary of the next sector, the aircraft is transferred to the frequency of the next sector and the strip is discarded. It is

now impossible to be sure where the ALPHA bay strips for either aircraft were at the time of the occurrence, but from the strip annotations and the re-investigation interviews it seems probable that both strips had already been discarded, there was no procedural conflict over ECHO, B738 would pass it only 30 seconds after entering the sector, and A319 was already on the Yellow Sector frequency.

4. The air routes UL123 and UN456 intersect at point ECHO. ECHO is 3nm from the northern edge of the Sector No. 1 airspace boundary and 10nm from the eastern boundary (the loss of separation occurred 4nm south east of ECHO). The sector lateral dimensions are approximately 60 x 90 nm. Relative to the size of the sector the ECHO intersection is extremely close to the edge of the sector boundary (3nm in sector of 5,400 square nautical miles

5. The ECHO fix does not have an individual strip bay; relatively few aircraft pass through it and the intersection is clustered under the ALPHA strip bay. Provided that there is no level change aircraft on UL123 and UN456 are separated by the semicircular rule. Those few flights that do pass through ECHO are therefore usually unproblematic. ECHO is at the periphery of the airspace and usually little of any consequence happens there.

6. In contrast, the majority of the sector's aircraft pass through point BRAVO. Six air routes intersect at this location; it is a high traffic density and high complexity intersection. Accordingly, BRAVO has a dedicated strip bay and no other fixes are clustered under it. Physically BRAVO and ALPHA are at opposite ends of the sector (and the radar display) about 70nm from each other, and normally they are also at opposite ends of the scale in terms how much controller attention they demand.

7. 15:34:20 B738 checked in on the frequency and was identified approximately 20nm north of the Sector No.1 boundary. At this moment *A319 was in Sector No. 2 airspace, 8nm south of MIKE heading NNE,* cruising at 484 knots, level at FL380. A319 was still heading *away from Sector No.1 airspace*; no obvious lateral conflict was discernable on the radar display. A319 was visible on the radar; displayed with a yellow label in accordance with the Brightness Level Selection (BLS). All aircraft within the vertical span of the BLS are displayed in this way; regardless of whether

they are in or out of the sector lateral boundaries. In the adjacent sectors the vast majority of aircraft with a yellow label had to be disregarded, especially those headed away from Sector No.1 and procedurally (as indicated on the strips) even after the turn at MIKE the aircraft were still vertically separated by the semicircular rule.

8. B738 tracked approximately 3nm east of his assigned route; this brought the aircraft 3nm closer to the Sector 1 boundary east abeam ECHO, narrowing the distance between aircraft and the airspace boundary by about 30%, compared to the distance had he tracked over ECHO. A319 clipped the corner at MIKE and the aircraft slowed down (slowing 50 knots between 15:33:00 and 15:33:20) when it changed direction; probably due to an increase in head-wind. It seems unlikely that either controller *ever* assessed the conflict on radar before the STCA, but the combination of; B738 being east of track, and A319 cutting the corner at MIKE and slowing down might have deceived their judgment even if they had.

9. The B738 ALPHA strip was most probably discarded from the ALPHA strip bay at or shortly after the aircraft was identified. It is probable that the A319 strip was simultaneously discarded. No level change was planned and the aircraft were therefore not in conflict. Controllers routinely "de-clutter" their working area at the earliest opportunity. At the time of the occurrence the Radar Controller recalled seeing only one strip; B738's BRAVO strip, in the *BRAVO* strip bay.

10. The B738 *BRAVO* strip had a warning "W" marked on it to indicate a separation problem with another aircraft over BRAVO. This warning would have been a powerful stimulus directing the attention of both controllers towards BRAVO on the radar display and the BRAVO strip bay.

11. Although the traffic load in the sector prior to and at the time of the occurrence was only medium; the planned (future) traffic over BRAVO was building up. Both controllers reported that solving the separation problems for aircraft approaching BRAVO was their main focus of attention. The increasing traffic can be seen on the traffic load graph on page 8 of the original report, and can be observed on the radar replay 8 minutes after the occurrence at 15:46:20, when B738 is overhead BRAVO.

12. 15:36:57 B738 requested climb to FL390, at this point the aircraft were now on converging headings, but it was another 23 seconds before A319 crossed the Sector No.1 airspace boundary. All aircraft which are above the sector's lowest vertical boundary are displayed identically, *whether they are inside or outside the lateral boundary makes no difference to the radar Brightness Level Selection.* Approximately 30-40 % of the traffic displayed on the radar is not in the sector's airspace and has to be disregarded by the Radar Controller; in either lower or adjacent airspace. Assessment of B738's climb request to FL390 indicated that it would solve the separation problem over BRAVO. However, the change in level over BRAVO needed to be coordinated with the next adjacent sector (further south).

13. 15:37:20 B738 asked if any turbulence was reported at FL390. At almost the same time A319 crossed the sector boundary for the first time. Turbulence cannot be seen on radar, so this would not be a reason for the Radar Controller to look at or around B738 on the radar. Both controllers reported that the focus of their attention was on BRAVO. The Planner was coordinating the B738 level change over BRAVO. Light turbulence is of no consequence for the Planner and would not therefore have drawn his attention towards ECHO.

14. 15:37:53 B738 was cleared to climb (recording of co-ordination with the next sector was unavailable, but co-ordination of the climb to FL390 is thought to have been completed at, or shortly before this moment). *A319 had not yet "entered the Radar Controller's consciousness" and the Planner was also "unaware of the immediate implications of the climb instruction".*

15. 15:37:57 The B738 pilot acknowledged the climb but had identified the A319 on his TCAS display and visually acquired the aircraft out of the cockpit window. *The pilot delayed his climb for 25 seconds.* At the point where the flight paths crossed the aircraft were 0.9nm apart laterally and 900ft vertically[13]. Rate of climb for a B738 is typically around 2000ft per minute. A pilot experiencing turbulence would not normally delay climbing to an alternative level where no turbulence had been reported.

[13]The minimum separation requirement was 5nm laterally or 1000ft vertically.

16. 15:38:40 The STCA Red alarm flashed and both controllers first became aware of the occurrence. The aircraft were already diverging laterally. The Radar Controller was concerned that any vertical controller intervention might contradict TCAS resolution advisory instructions and because the aircraft were already diverging laterally he did not intervene[14]. The Planner had no means of intervention. Both controllers were in mild shock, and were relieved from duty shortly afterwards. A319 was unaware that anything unusual had occurred.

[14] Confusion about which instruction to follow when contradictory instructions were received from the TCAS and a controller was a contributing factor in the Ueberlingen disaster in July 2002.

6. Systemic Occurrence Analysis Methodology (SOAM)

"Identifying an error is merely the beginning of the search for causes, not the end. The error, just as much as the disaster that may follow it, is something that requires an explanation. Only by understanding the context that provoked the error can we hope to limit its recurrence."
James Reason (1997, p.126)

A description of the SOAM is available in ESARR Advisory Material Guidance Document EAM2/GUI8. The notes below are a brief summary.

Every fact from the investigation is subjected to two tests:

Test 1: Does the fact represent a condition or event that contributed to the eventual occurrence and if so[15],

Test 2: Does the fact represent a *barrier, human involvement, a contextual condition, and or an organizational factor.*

Test two is applied using a process of classification until each fact is sorted into one or more of the SOAM categories.

Horizontal links represent the associations between a contributing factor at one level (e.g., a human action), and its antecedent conditions (e.g., the context in which the action took place). Facts at different levels should be linked if one is thought to have influenced the other.

The first stage in SOAM is to identify the protective barriers which have failed or been absent at the time of the occurrence.

[15] Items that fail the first test are not necessarily ignored but "should be detailed in a separate part of the report".

Check question for Barriers:

Does the item describe a work procedure, aspect of human awareness, physical obstacle, warning or control system, or protection measure designed to prevent an occurrence or lessen its consequences?

The next stage is to identify the human actions or non actions which immediately preceded the safety occurrence. Not why people acted as they did, but simply what were their actions or in-actions just prior to the event.

Check question for Human Involvement:

Does the item describe an action or non-action taking place immediately prior to and contributing to the occurrence?

Contextual conditions describe the circumstances that exist at the time of the occurrence. What were the conditions in place at the time of the safety occurrence that help explain why the person acted as they did?

Check question for Contextual Conditions:

Does the item describe an aspect of the workplace, local organizational climate, or a person's attitudes, personality; performance limitations; physiological or emotional state that helps explain their actions?

Organizational Factors describe circumstances which pre-existed the occurrence and produced or allowed the existence of contextual conditions, which in turn influenced the actions/or inactions of staff.

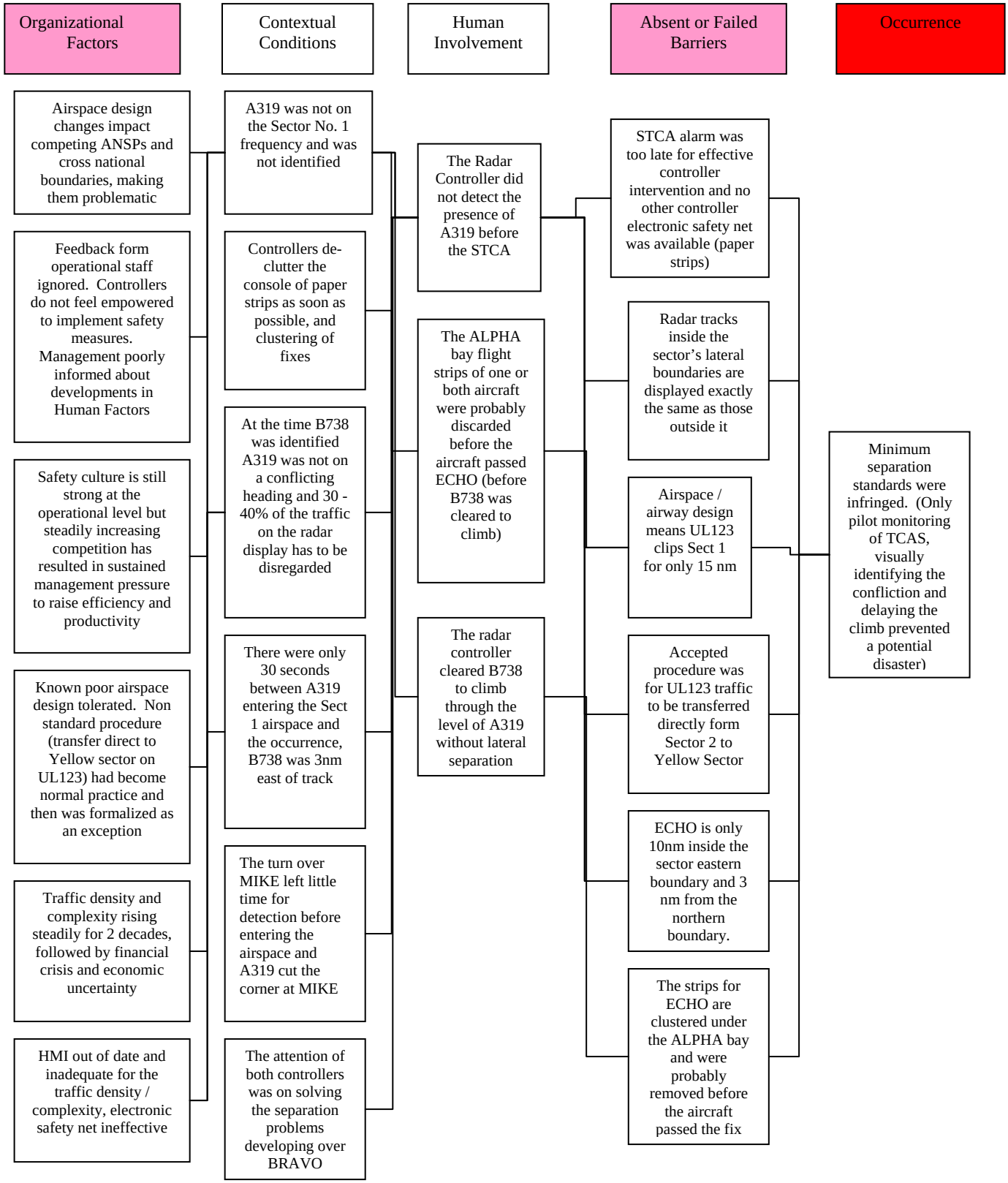
Check question for Organizational Factors:

Does the item describe an aspect of an organization's culture, systems[16], and processes or decision-making that existed before the occurrence and which resulted in the contextual conditions or allowed those conditions to continue?

[16] Includes hardware, administration, communication and socio-technical systems

The data from the original report and the Locally Rational Occurrence Scenario was used to perform a SOAM analysis and the resulting SOAM chart is shown in fig 6 below.

Fig 6 SOAM Chart



When formulating recommendations the SOAM guidelines direct the investigator to target the *barriers that failed or were absent* and the *organizational factors* (shown under the headings in pink). "Errors are part of the condition and cannot be eliminated. As such, attempts to achieve this through additional training, harsher sanctions or more direct supervision will meet with limited success. To paraphrase Reason, errors are like mosquitoes – it is impossible to drain them all. It is far better to "drain the swamps" in which they breed. In the context of corrective safety actions, this means addressing the contextual conditions that precipitate error (Eurocontrol, 2005)".

"Contextual conditions are mostly the products of organizational factors (the exception being environmental factors such as weather, terrain and other natural phenomena) (Eurocontrol, 2005)."

"The SOAM process requires that each failed barrier should be addressed by at least one recommendation for corrective action. Each identified organizational factor should also be addressed by at least one recommendation, unless this factor has already been covered by a recommendation addressing barriers (Eurocontrol, 2005)".

7. System-Theoretic Accident Modeling and Processes (STAMP)

The following four paragraphs are a summary of STAMP extracted from the Safety-Driven Model-Based System Engineering Methodology Part 1: Methodology Description (Leveson, 2007, page 9), *adapted to this occurrence investigation*.

STAMP is an accident causality model in which accidents are conceived as resulting not from component failures, but from inadequate control or inadequate enforcement of safety-related constraints on the design, development, and operation of the system. Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interactions among components that result in a violation of system safety constraints.

In STAMP, safety is viewed as a control problem; accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled or controlled. The processes that enforce the safety constraints must limit system behavior to the safe states implied by the safety constraints. Figure x shows the Blue ANSP ATM control structure to enforce safety constraints. Each hierarchical level of the control structure represents a control process and control loop with actions and feedback. Two control structures are shown in figure 8 (page 53) – system development and system operations – both of which have different responsibilities with respect to enforcing system safe behavior.

STAMP treats a system not as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behavior to ensure safe operations, but it must continue to operate safely as changes and adaptations occur over time.

Furthermore, any controller – human or automated – must contain a model of the system being controlled. The process model (the plant, in control theory terminology) at one extreme may contain only one or two variables (such as that required for a thermostat), while at the extreme may require a complex model with a large number of state variables and

transitions (such as required for an ATM[17] system). Whether the model is embedded in the control logic of an automated controller or in the mental model of a human controller, it must contain the same information: the current sate (the current values of the system variables), the ways the system can change state (the system dynamics), and the desired relationship among the system variables (the control laws). This model is used to determine what control actions are needed, and is updated through various forms of feedback. When the model does not match the controlled process, accidents can result.[18]

STAMP terminology

Systems Theory relies on two pairs of ideas: (1) *emergence and hierarchy* and (2) *communication and control.*

Emergent properties are the result of unanticipated interactions between system components. Component may be performing exactly as designed, or individuals may be making entirely rational decisions at their level of the hierarchy, but in complex systems unanticipated interactions result in unexpected outcomes, some of which may be undesirable.

The emergent properties from a set of components at one level of hierarchy are controlled by *constraints* upon the degree of freedom of those components.

Safety constraints specify the relationships among system variables or components that constitute the non hazardous or safe system states.

Control is the imposition of constraints. The control processes that enforce the constraints must limit system behavior to the safe changes and adaptations implied by the constraints.

In closed systems unchanged components settle into a state of equilibrium. In open systems there are inputs and outputs, which result in changes in the environment and disturb the equilibrium.

---

[17] Leveson used „spacecraft", I have substituted the acronym ATM.

[18] This mental process model of the physical system being controlled has striking similarities with Neisser's perceptual cycle. When there is a mismatch between current understanding (mental process model) of the system state and the actual system state, then accidents can result.

A state of equilibrium in open systems can be achieved by communication. Communication is a two way process involving control and feedback. Feedback is information about the system variables and components – the system state.

Open systems are continually adapting to changes in the environment. To remain safe a system design must enforce the safety constraints as changes and adaptations occur over time.

Why systems fail – according to STAMP

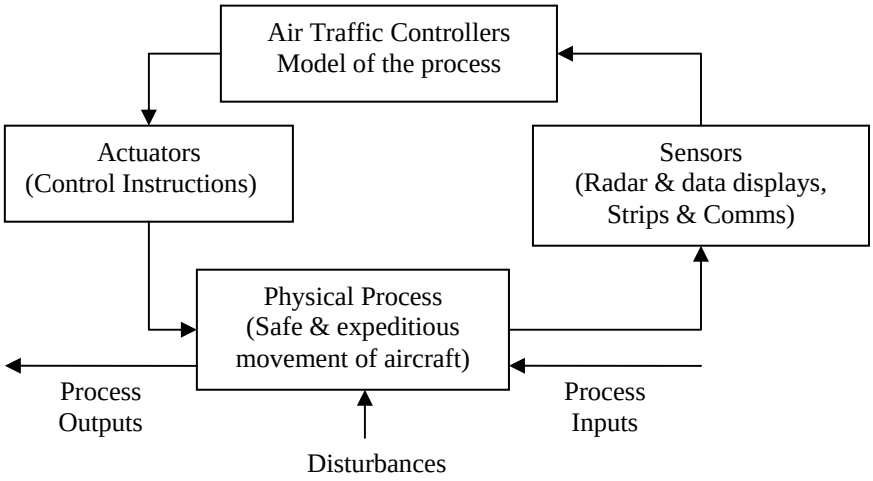
In systemic models accidents are viewed not as the result of *events or individual errors* but as *a loss of control.*

Accidents can result from interactions among system components that violate the system safety constraints; i.e. a lack of appropriate constraints on system behavior; leading to a loss of control.

Accidents can result from a lack of communication about changes in the environment or the system state; lack of communication leads to a loss of control.

A loss of control can occur when the difference between the mental model of the process and the physical process becomes too great.

Fig 7 Operator level model of the system



8. STAMP Analysis B738 and A319 Occurrence

The data from the original report and the Locally Rational Occurrence Scenario was used to perform a STAMP analysis and the resulting Hierarchical control structure chart and sub models are shown in figures 8, 9 and 10 below.

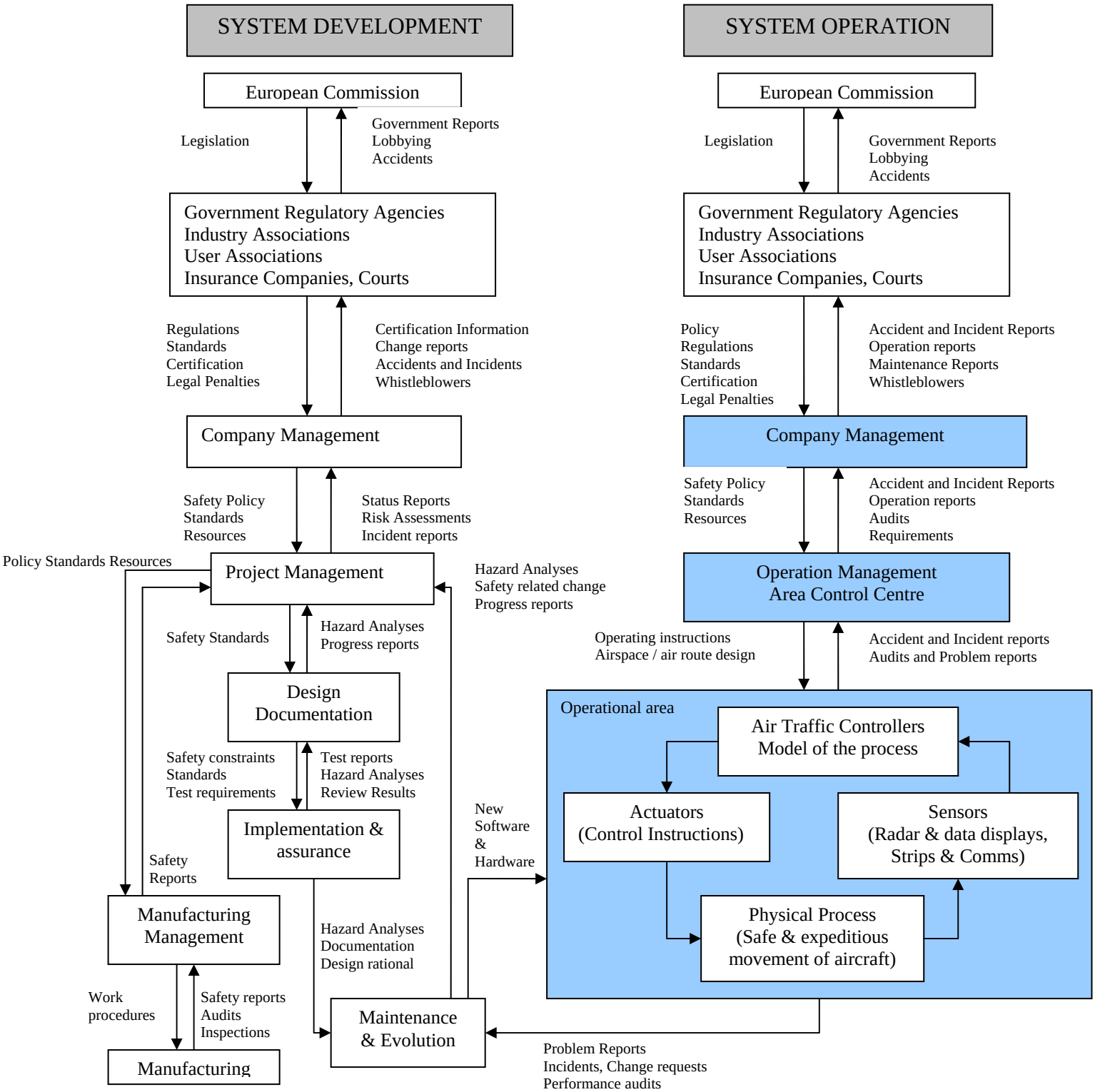
Hierarchy of the safety control structure

The first stage of a STAMP analysis is to draw out the hierarchical safety structure. The safety structure in figure 8 is from Leveson's generic structure adapted to the ATM system in this occurrence. The structure is a simplification: The Operation Management in the Area Control Centre (and every other level) has its own sub hierarchy (see fig. 13, page 88) and links with other levels of hierarchy including; Eurocontrol, International Civil Aviation Organization (ICAO), and the European Aviation Safety Agency (EASA) have been omitted. Additionally, in this occurrence 3 sectors are directly involved, Sector 1 and 2 come under the same Operational management, but Sector Yellow is under a separate ANSP in another nation state. Only the structure of the Sector No. 1 ANSP is shown.

A further complication is the ongoing harmonization program aimed at creating a "Single European Sky" (SES). The European Union is an evolving institution with many states competing for power and influence. There are currently 27 nation states in the European Union (and almost as many languages). Altogether this means that the safety control structure in Europe is currently evolving rapidly and is politically extremely complex. Nevertheless, every model is a simplification of reality; a simplified structure can still be used as a framework for thought. The STAMP analysis in this report is restricted mainly to the Operational ANSP part of the overall structure – shown in blue in fig 8.

The generic System Development structure is included because of its importance in the development and introduction of new technologies.

Fig 8 ATM System Control Structure Down arrows are controls, up arrows are feedback, horizontal arrows are inputs



Sub-models of the controls and constraints

The system hazard relevant to this occurrence is: The loss of standard separation between aircraft in the designated airspace.

The related system safety constraint is: The ATM system including; airspace design, surveillance systems, data displays, regulations, procedures and air traffic controllers must provide control instructions that will ensure minimum separation standards exist between aircraft in the designated airspace.

The hierarchical levels shown in blue in the safety control structure in figure 8 are analyzed to examine the:

Safety constraints
Context in which decisions were made
Inadequate control actions
Process model flaws

Fig 9 STAMP Operational Management and Controllers

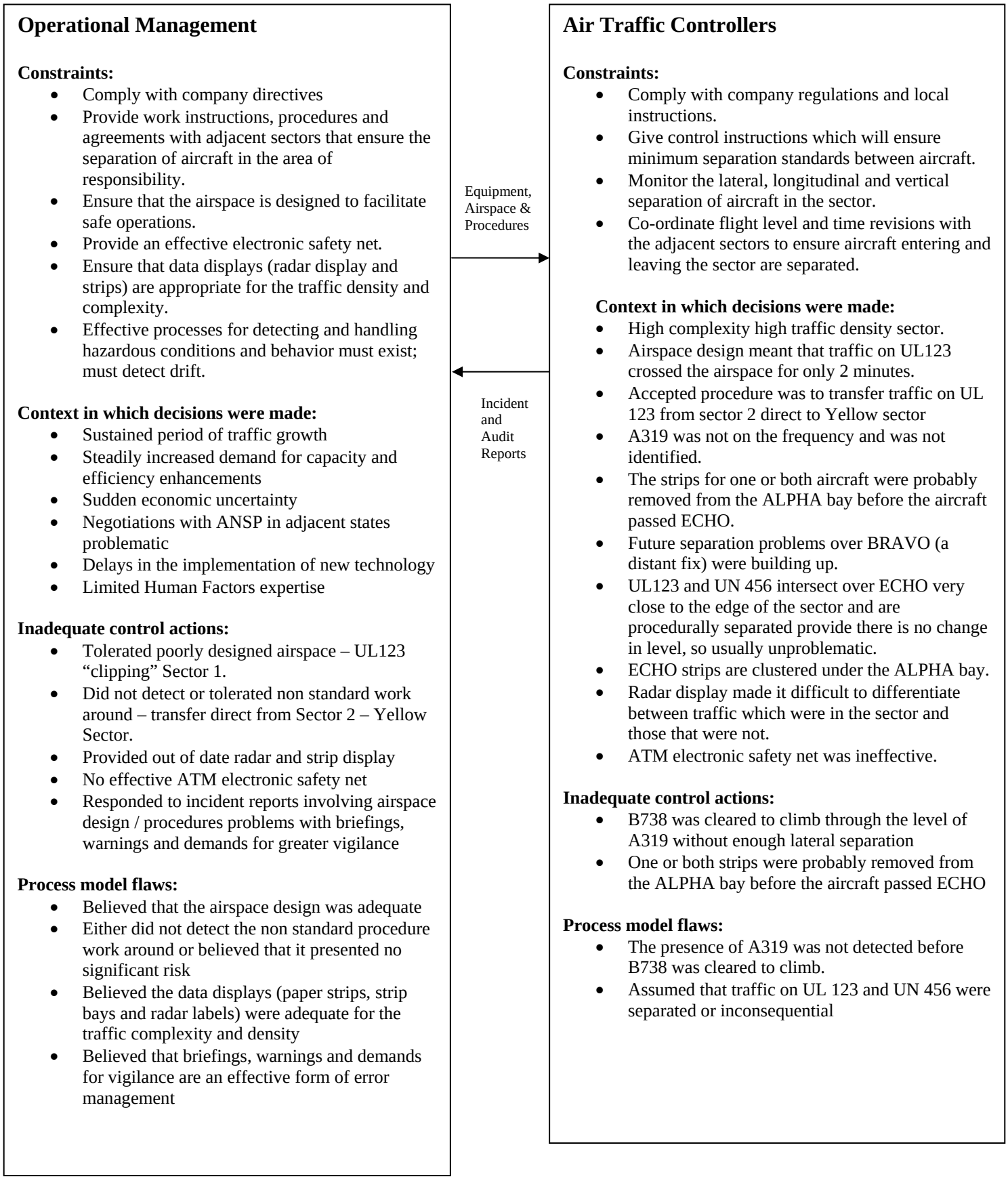


Fig 10 STAMP Company Management

Constraints:

- Comply with International Recommended Standards and Requirements
- Comply with European Commission directives
- Comply with Government policies and the law
- Provide an effective Safety Management System – safety oversight; detect and manage drift
- Negotiate airspace, and revenue arrangements with: Government, adjacent ANSP and states, and the airlines
- Develop and deploy technical systems appropriate for the traffic complexity and density
- Provide regulations and separation standards which will ensure the safe movement of aircraft
- Provide training in Human Factors

Context in which decisions were made:

- Steadily increasing air traffic; increasing complexity and intensity.
- Finite airspace and northern European weather
- Sudden economic uncertainty 9/11/2001 and Sep 2008 financial crisis
- Sustained airline and government pressure to reduce costs and increase productivity
- Essential Service – must provide services even where economically unsustainable
- Sustained airline pressure to minimize airline delays
- Unionized labor force and strong labor laws
- High fixed costs
- Skilled workforce with long training lag and a global shortage of controllers
- High training costs
- Increasing competition from other service providers with lower base costs and alternative airline routes
- Evolving European airspace – Single European Sky
- Rapidly evolving technology - Single European Sky ATM Research – rapidly increasing technological complexity
- Escalating cost of new technology
- New technology changes the work and has an unknown efficiency and safety benefits – opens new pathways to failure, brings new uncertainties
- Complex socio- technical system and a high risk industry
- Lack of current ATM operational experience in senior management positions
- Limited Human Factors expertise

Inadequate control actions:

Un-intentionally communicated that:

- Airspace redesign safety improvements must not reduce operating income
- Airspace redesign safety improvements must not reduce strategic competitive advantages
- Operating procedure or route modifications to improve safety must not reduce airspace capacity
- Negotiating airspace safety enhancements across national borders should be avoided, and:
- Provide outdated technical equipment – radar display, paper strips and electronic safety net inappropriate for traffic density & complexity
- Inadequate investment in Human Factors training
- Inadequate resources allocated to the detection and management of emergent phenomena - especially drift.
- Rejected systemic safety recommendations which might increase costs or reduce income
- Accepted over reliance on briefings, warnings and vigilance to sustain safety
- Operational feedback channel did not functioning effectively. Either not flowing, not understood, or ignored.
- Did not address the increasing complexity of the system and update the safety model accordingly.

Process model flaws:

- Assumed the airspace design and procedures were safe or that the channels for modifying them were functioning
- Assumption that poorly designed airspace or systems can be safely operated *sustainably* by operator vigilance or reliability enhancements
- Thought that the radar display and paper strip system was appropriate for the traffic complexity and density
- A lack of understanding about how unanticipated interactions in complex systems can result in failure without any individual or component failure. Thought that safety and reliability is the same thing.

13. Comparison of the Results

The author does not claim “the view from nowhere”; every analysis is subject to bias. A reader may weigh the value of particular facts differently to those shown in either the SOAM or STAMP analysis. The report attempts to be transparent about the sources of information and reasoning behind the selections made and the fact that other interpretations using the same data can produce different detailed results is self evident. Nevertheless, there are distinct general differences in the output from the 2 methods of analysis.

The output from SOAM analysis is a SOAM chart. This can be viewed on a single piece of paper and the information in each box can be linked directly to the “facts” from the local rationality occurrence scenario, the records of interviews, or data from the original investigation.

The SOAM methodology directs the investigator to target recommendations to items under *Organizational factors* and *Barriers that failed or were absent*, but the chart does not direct the investigator to analyze these headings in any more detail than the categories of the boxes and the links between them. The investigator is directed to look up and down the levels in the organizational chain, but not directed *into* the *processes* within them. SOAM provides limited insight into the detailed behavior of components in the system as a whole; how the holes are *created;* how the system *migrates* towards the boundaries of safe operations; or why the holes line up. Emergent phenomena and the mechanisms of non linear interactions between components are not directly addressed.

The output from the STAMP analysis is three pages of text and diagrams, and only 3 levels from the System Operation part System Control Structure were analyzed. STAMP directs the investigator more deeply and specifically within structured sub headings into the relationships between components at each level. In the language of SOAM; how holes in the Swiss cheese are *created – emergence and drift*. STAMP directs the investigator to examine the processes in the system as a whole; in the language of SOAM *“why the holes line up”* **–** a lack of control and constraints.

The B738/ A319 occurrence is a good example of a system migrating towards the boundary of safe operations (drift) and unanticipated interactions between normally functioning components. The mechanism of drift can be traced through the STAMP analysis. The equipment was functioning perfectly, the controllers followed the established procedures, and there was nothing unusual in the way that they performed their work. Nothing needs to be broken for a complex system to fail.

Drift does not imply recklessness, negligent management, or lazy operators. Simply, that; "Deviations from standards become established as the new norm, and a lack of adverse consequences tends to re-affirm that the new norm is safe. Incrementally over time and without realizing it, people begin borrowing from safety" (Dekker, 2006).

The controllers on duty at the time of the occurrence were running a risk, not deliberately taking one. The continuously increasing need to improve efficiency along with rising traffic density and complexity produced *locally rational system adaptations* ***at all levels***. Local adaptation of procedures, politically pragmatic airspace design, outdated information displays, realistic use of equipment and an ineffective electronic safety net, allowed the system as a whole to migrate to a point where a tiny system disturbance (the unusual disposition of the traffic on a particular day), meant that the controllers model of the system did not match the physical process. Two normal controllers doing normal work were led to the edge of a disaster.

The practice of transferring aircraft on UL123 direct from Sector 2 to the yellow sector is arguably the most significant local adaptation. The process by which it gradually became the accepted procedure and how it was eventually formalized can be traced. The original report (p.33) states that:

> "The second aircraft involved in this infringement of separation, A319, had already been transferred from the Sector No. 2 to the Yellow Sector at 15:35, i.e. even before B738 requested FL390. This is not an official procedure but it has proved to be practical in the past and is common practice since the aircraft cover only about 15 NM in the upper corner of the Sector No.1 when flying on the route segment MIKE – CHARLIE of UL123. These flights do not normally constitute relevant traffic, unless they have to be considered for any climbs on UN456. But this happens only in exceptional cases."

The Safety Manager's Record of Interview (page 84) demonstrates how this practice became established as the norm over a period of at least 5 years.

What was the time frame / history over which development of the; "accepted practice" to transfer UL123 traffic direct to Yellow Sector?

I cannot be exact about when the practice first developed; the structure of the airspace and air routes changes over time. The complexity and the intensity of traffic increased significantly over the years, but it has been the accepted procedure for at least 5 years."

This is a perfectly rational adaptation as illustrated by Question 4 (page 84).
Could clearer company guidance / procedures or design have helped them make better goal trade –offs?

Requiring aircraft on UL123 to check in on the frequency would add to the frequency load, they would only be on frequency for around 2 minutes while they "clip" the airspace and under normal circumstances they never conflict with other traffic. Redesigning the airspace or route structure to avoid the "airspace clipping" might improve the situation, but might also create new problems elsewhere. Airspace redesign would require co-operation / compromise with another (competing) Air Navigation Service Provider. It is possible and has been done in the past, but it would be a complex task and has to be balanced against the probability of this event re-occurring and the effectiveness of alternative countermeasures.

A lack of adverse consequences tends to re-affirm that the system is safe. (Planner interview, p. 78)

Did the situation fit a standard scenario?

No. About once a month one or other aircraft has not reached the assigned level, but this fact is either coordinated from the other sector or noticed on the radar. In this case, prior to the climb instruction, both aircraft were in level flight.

Has this situation occurred before or since?

No, not in 10 years as Planner or Radar controller

Although problems persisted in the sector immediately below, where level changes are more common. (Planner p, 79)

Has this situation or something similar happened to others?

Not with aircraft in level flight, but aircraft not reaching the assigned level by the airspace boundary is a problem; this should be coordinated but this does not always happen.

Safety Manager (p.81)

Has this situation occurred before or since?

Not in this high level sector, but in the sector below it when climbing aircraft have not reached the assigned level as expected, there have been 4 similar events that had the potential for a loss of separation between Oct – Nov 2008. In each case the aircraft was coordinated entering the sector in level flight, but was actually still climbing.[19] *These cases were all resolved by controller intervention before there was a loss of separation.*

After the occurrence what had been "accepted practice" was formalized as a local instruction. The decision to formalize the procedure was not in accordance with the advice given by the Safety Manager but it was not taken by amoral or negligent management. It was taken in consultation with the Safety Panel and once again it is perfectly rational at that level.

As Safety Manager I make recommendations to the Chief of Section, and the Area Control Centre Safety Section at the company HQ. The Chief of Section refers the recommendations to the Permanent Board of that rating group (comprises 6 controllers) and the Safety Panel (12 controllers, made up of 4 controllers from each of the 3 EBG (airspace blocks) in this Area Control Centre). The Safety Panel and the Permanent Board then report back to the Chief of Section. The Chief of Section considers their advice, but ultimately the Chief of Section has to decide whether or not to implement a particular recommendation. In a complex case like this; with a recommendation from the Safety Manager conflicting with advice from the Permanent Board and the Safety Panel, balancing the feasibility, risks and benefits, and coming to a decision is an extremely challenging task.[20]

---

[19] *Aircraft climb performance varies according to; the aircraft type, upper winds, air temperature, humidity and aircraft loadings (fuel, passengers and cargo). If an aircraft is co-ordinated to enter airspace in level flight but cannot reach the level before the airspace boundary, then a revision should be co-ordinated.*

[20] *A drawing of this Hierarchy was made as per fig 13 (page 88)*

The Chief of Section's decision was to formalize what had become the accepted practice; i.e. UL123 traffic shall be transferred direct to Yellow Section.

Airspace and air route design is not driven just by safety and expedition. The context of airspace design includes many other variables; national boundaries, competition between ANSPs, revenue arrangements, legal responsibilities, and alternative air routes.

The SOAM analysis could be used to support a recommendation that the Sector No 1 airspace should be re-designed to avoid UL123 clipping it. The STAMP analysis would support this recommendation but STAMP could be used to identify systemic countermeasures much higher up the hierarchical control structure, for example; STAMP directs the investigation to consider measures aimed at the European Commission level that would facilitate the early introduction of Functional Airspace Blocks; this would involve resolving issues such as cross border legal liabilities, competition and revenue sharing, which would facilitate the re-designed of airspace with the emphasis on safety and efficiency across the whole European continent; instead of just the corner of one sector in one ANSP.

The higher up the control structure the more *systemic* the countermeasures identified by the analysis are likely to be. However, there is a catch. The higher up the Control Structure the investigator probes, inevitably the further away from the proximal events of the particular occurrence being investigated one is led; the more links there are in the chain of evidence the more tenuous the argument becomes. Hard evidence is essential to build a compelling case for high end recommendations, but the higher up the control structure one probes the more difficult it becomes to gain access to politically sensitive information. It is possible to speculate that had the STAMP analysis continued up to the European Commission level, a link might be drawn between the failure of the European Union to ratify a particular treaty and how this may have undermined the European Commission's authority to bring governments to the negotiating table and make the compromises necessary to resolve cross border and ANSP revenue arrangements and introduce Functional Airspace Blocks. This may or may not be "true", but speculation of this kind is difficult to argue convincingly without hard evidence to support it. In a climate of intense competition and economic uncertainty,

investigations which may lead to countermeasures that could affect strategic interests or threaten short term economic stability or competitive advantage are likely to be unwelcome by those negatively affected, and resisted accordingly.

Access to high level information might be justified by clusters of incidents; where low level countermeasures have proved ineffective, or after an accident involving loss of life. If B738 and A319 had collided the repercussions from the loss of around 350 lives might open the way for the higher links in the control structure to be investigated, but the higher levels of the control structure are, for all practical purposes, "off limits" during single incident investigations. Even some of the items in the Company Management sub analysis in this study are clearly speculative.

Both techniques direct an investigator to probe deeper than just the immediate proximal events, direct "causes" or individual blame. Despite the completely different theoretical origins of the techniques; SOAM from cognitive psychology and STAMP from systems theory and computer engineering, there are some parallel concepts. The concepts of a barrier and a constraint have some similarities, and holes that line up could be viewed as unanticipated interactions. The SOAM chart and the STAMP sub models especially at the Air Traffic Controller level have some similarities accordingly. The SOAM analysis identified the failure of the ATM electronic safety net (STCA), the radar display, or the strips to prevent the occurrence – barriers that failed. It is difficult for an electronic safety net to provide early enough warning in circumstances where the aircraft are in close proximity laterally and the confliction is produced vertically. However, STAMP directs the analysis more deeply into how the components interact and the concept of control and constraints, which suggest new countermeasures even at the lower levels.

In the adjacent new ACC electronic flight strips and state of the art radar displays are being assembled. Designing new safety constraints into this system is now technically possible. For example:

- If an aircraft enters a sector but is not represented by an electronic flight strip (in a relevant bay), then the controller could be alerted.
- If an aircraft has not been logged on the electronic flight strip as identified and on the frequency but the aircraft has or is about to enter the sector, then the controller could be alerted.

- If an aircraft enters the airspace at a flight level different to the coordinated level indicated on the flight strip, then the controller could be alerted.
- It should not be possible to discard electronic strips before the aircraft they represent has passed the relevant fix.
- Aircraft that are inside a sector's vertical *and lateral* boundaries could be displayed differently to aircraft that are outside the sector.

However, new airspace, electronic flight strips, new displays with interlocking alerts and especially new forms of automation will add complexity, change the work, and produce new pathways to failure. There will, of course, also be new expectations about efficiency and capacity…

The importance of communication and control in the "System Development" half of the STAMP system control structure (page 53) as the new system *develops and adapts over time* is clear.

The model of the process that air traffic controllers presently use is relatively unaffected by automation. The controller level system diagram below (fig 11) is a reasonable representation of the current situation.

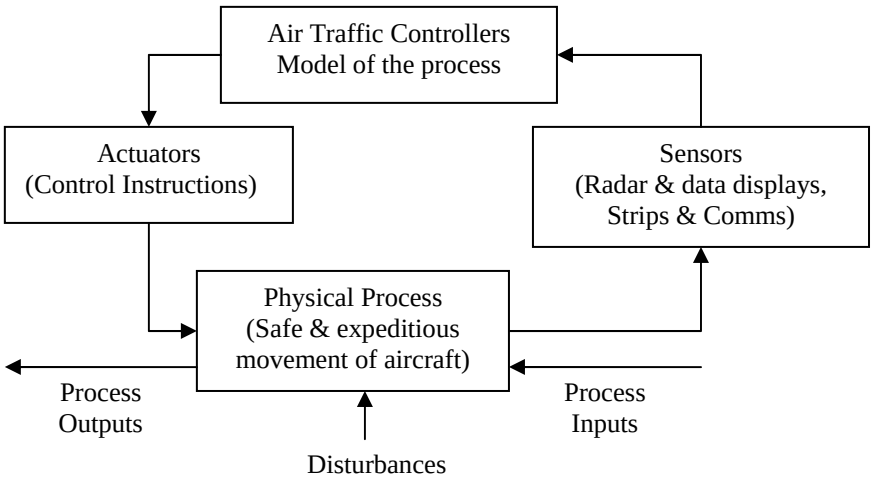


Fig 11 controller level system diagram

The new technology necessary for the aviation industry to benefit from "Continuous Descent Arrivals flown on datalinked 4D flight paths that are tailored to local constraints and timed for merging traffic" (as described in the introduction), will mean a steady increase in

Collaborative Decision Making, automation and semi automation both in the air and on the ground. The controller level system diagram above will change into something more like the representation (in fig 12) below.

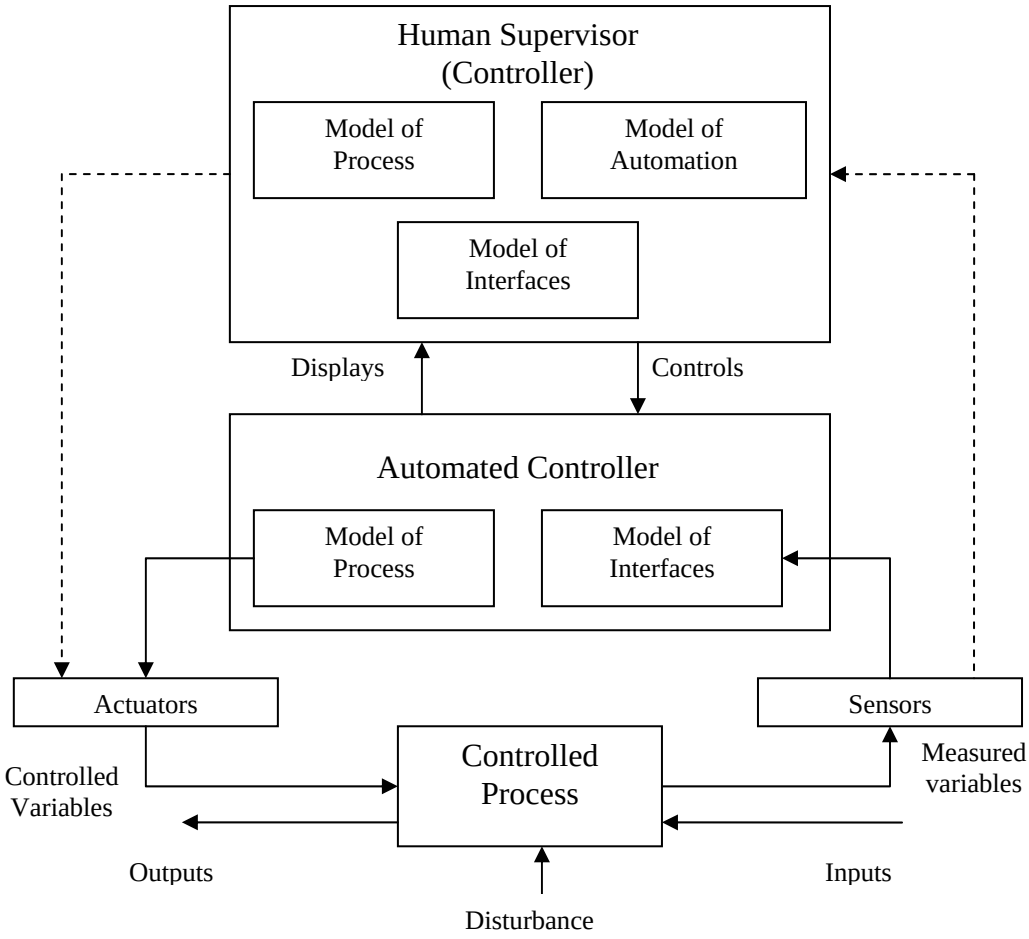


Fig 12 Standard three level control loop incorporating automation (after Leveson, 2007)

Detailed systemic models will be necessary to understand the process in which the components in this more complex system as a whole interact and adapt over time. Control and constraints will be needed to prevent interactions with negative outcomes from occurring.

14. Conclusions

The B738 /A319 occurrence was not the result of component failure, but resulted from a gradual migration of the whole system to the point where a minor disturbance almost triggered a disaster.

The Locally Rationality principle is a vital part of an investigation because it helps the investigator avoid hindsight. By definition it rejects the notion of an event or an error as the end point of the investigation. Local Rationality compels the investigator to search for a rational explanation of events, actions or inactions, and by doing so lifts the blanket covering the underlying context and processes.

SOAM is a useful heuristic and a powerful communication device. SOAM might be summarized as “quick and dirty”, it is easily applied from the evidence that is accessible in regular ATM incident investigations, it helps identify flaws in the system at all levels, and it draws the investigation away from the proximal events. SOAM is a useful first step for addressing the context in which the events occurred. However, SOAM is weak with respect to emergent phenomena. SOAM is a snapshot of the final system state; the holes are visible, but the process by which they are created is not addressed.

The complexity of ATM systems is growing and the rate of increase is accelerating. Unanticipated interactions between normally functioning components is becoming increasingly important with this rise in complexity. At the same time competition and scarcity of resources drive the whole system towards the boundary of safe operations. The migration is incremental and the steps are rational at every level at which they are taken.

Complex systems are not static, the components interact and affect each other and the whole system is changing and adapting over time. STAMP looks more deeply into the interactions and interdependencies between components and tracks the process of change over time.

STAMP leads an investigator through a structured analysis of the higher levels of a systems control structure, which helps an investigator to identify high end systemic countermeasures. However, high end recommendations are more difficult and often more expensive to

implement than low level recommendations. Compelling evidence is necessary to obtain the political traction to implement high end recommendations. *Single* ATM *incidents* do not normally generate enough political will to probe into the higher levels of a system's control structure, which is necessary to make a credible STAMP analysis, but when low level countermeasures have proved ineffective, where clusters of incidents indicate deeper systemic problems, or after accidents, then a STAMP analysis would provide a powerful additional perspective.

A glimpse into the future importance of control and constraints in an ATM system of increasing complexity is neatly illustrated in the STAMP analysis of the B738/A319 incident. Systemic models like STAMP will be necessary to understand and control the interactions between system components in increasingly *automated* complex systems.

Safety and reliability is not the same thing. Traditional safety analysis tends to concentrate on component reliability (physical or human) and direct causal relationships. However, the growing complexity of ATM systems being developed under the Single European Sky and NextGen programs mean that safety analysis needs to consider not just reliability but also how all the components in the system as a whole interact with each other and change over time. Systemic models like STAMP are needed *now* to identify the *controls and constraints* that are necessary to prevent interactions with undesirable outcomes in increasingly complex ATM systems.

Annex: A

Radar Controller Record of Interview

Friday April 17 2009 10:00 hrs for 2hrs & 15 minutes

Description of the Working Arrangements:

Positions of the Radar Controller / Planner - Supervisor and others see *Fig deleted*

Radar setup: scale *set at 212nm, h*eight filters: *aircraft below FL335 were filtered out*; STCA *working;* RVSM *yes.*

Airspace boundaries / co-ordination partners – ATS route structure – crossing points *See fig z, Vertical limits were FL355-660, lowest useable level FL360*

Strip bays and strips generally, and then specifically for the routes used by B738 and A319 (*see fig a).*

A319 "standard" handling procedure / route / co-ordination – and strip handling

Standard company regulations (ATM Manual) require that aircraft should be transferred to the sector control frequency 3 minutes prior to entering the sector boundary. Nevertheless, "because aircraft on MIKE –CHARLIE section of UL123 only travel for approximately 15nm (for 2 minutes) through the Sector No. 1 it was accepted practice to transfer them direct to the Yellow Sector". Traffic on UL123 (such as A319) is in the west-bound semicircle at even flight levels; traffic on UN456 (such as B738) is in an east-bound semicircle at odd flight levels. Therefore, provided there is no level change, these flights do not conflict.[21]

Part 1 - Before the STCA

1. What Information sources were you relying on?

   The Radar, the Radio, the Flight Strips and the Planner

2. What were you seeing?

   The Radar and the Strips

---

[21] *After this occurrence the "accepted practice" outlined above was formalized.* The operational order for transfer of communication for Sector No. 2 on UL 123 was amended to reads as follows: "For traffic along UL123 communication shall be transferred to Yellow Sector". In all ATM documentation, as directed by ICAO regulations, the word "shall" means mandatory.

Safety briefings were conducted concerning the A319 / B738 separation breakdown.

3. Where was your attention focused?

The BRAVO area was about to get busy and was the main focus of my attention

4. What were your goals?

Traffic separation over BRAVO and service to B738 to avoid turbulence

5. Were there goal trade offs – time or other resource pressure?

No – I saw no trade- offs, it appeared to be a win / win situation.

6. Where was the Planner's focus of attention?

BRAVO

7. What were the Planners goals?

Separation over BRAVO and co-ordination – the Planner would ***not*** *be concerned about reports of light turbulence, it only becomes significant to the planner if turbulence becomes moderate or worse.*

8. What were your expectations about the Planner's role?

We had (and still have) an excellent working relationship. I trusted him completely and have no doubts about his competence. He fulfilled my expectations of a Planner.

9. Where was the A319 strip – what does the absence of hand written strip markings indicate?

The A319 and B738 strips would automatically have come into the ALPHA bay; a second B738 strip would simultaneously come into the BRAVO bay. There is no bay for the point at which the two routes intersect at ECHO – it would be impractical to have a strip bay and strips for the point at which every route intersects – this would result in an unmanageable number of bays and strips. Because ECHO and ALPHA are fairly close they are clustered under ALPHA. There are no hand written marking on the A319 strip because it did not come on the frequency, and there was no deviation from its planned times or levels.

*What I realize now is that the **ALPHA** strip for B738 was not retained / copied as part of the original investigation evidence. There was no procedural conflict between the planned levels of the A319 and B738 – if there had been, then there would have been a "W" indicating "warning" written in the end box of **both ALPHA** strips. There was no procedural conflict and therefore no "W" on the A319 ALPHA strip that we do have. There is a "W" on the B738 **BRAVO** strip; this indicates a conflict with another aircraft over BRAVOI – not ALPHA and this conflict was solved by climbing B738 to FL390.*

*Controllers generally reduce the amount of information they have to process as a matter of strategy; so if there is no perceived conflict information is often disregarded / discarded at the earliest opportunity. There was no conflict over ALPHA at the planning stage, and the A319 was not coming on frequency. It is now impossible to be certain about where the ALPHA strips were when the conflict actually occurred, but the fact that the B738 strip was not impounded suggests that it had been discarded and even the A319 strip may have been out of the ALPHA strip bay. **When the request for climb was made by B738 I recall only one strip – in the BRAVO bay**, the clearance to climb was intended to solve the BRAVO conflict and avoid the turbulence.*

10. When did you first become aware of the problem?

*My first indication that I had a problem was when the STCA went off – **until that point A319 had not entered my consciousness.***

Part 2 - Post STCA

11. How would you describe the situation at that point?

The STCA alarm attracted my immediate attention; the labels of both aircraft flashed in red and the lateral separation distance was indicated (there is no audible STCA alarm).

12. After the STCA how did you judge that you could influence events?

When the STCA went off the aircraft were already diverging (separation was increasing), I was concerned about passing a vertical control instruction which might contradict a TCAS RA, so I did not intervene. There is a common misperception that the radar display shows an absolutely accurate representation of where the aircraft are at a particular moment. This can give the impression that if the minimum separation requirement is 5nm

laterally and 1000 feet vertically and the radar display indicates 4nm and 800, that there is still a margin of safety of 4nm and 800ft. This is misleading because the radar display shows a ***calculated most probable position*** *based on complicated algorithms and there is a radar update rate. The altitude readout is based on mode Charlie information which is dependant on instrument accuracy. Aircraft altitude is calculated on air pressure; not some absolute vertical distance, and the aircraft themselves occupy vertical space. Furthermore, wake turbulence is still a factor at high altitude – you don't have to hit them to hurt them. Wakes from a close encounter can seriously damage aircraft in flight even at high altitude. There is sound reasoning behind the apparently wide prescribed separation standards. Commercial jet aircraft at these altitudes (around 37,000 feet) typically cruise at around 450 knots or 7.5nm per minute (ground speed), so on reciprocal headings they close at a rate of 15nm a minute.*[22]

13. Did the situation fit a standard scenario?

No, separation at the point that these routes intersect is normally assured by the semicircular rule. The intersection is usually of minimal interest, it's a comparatively quiet part of the sector route structure.

14. Has this situation occurred before or since?

Three colleagues who work the same sector have told me informally (anecdotal / unreported) about similar events they have experienced that had the potential for a loss of separation at the same intersection.[23]

Part 3 - Counterfactuals

1. How long do you estimate A319 was "*observable*" on radar before the STCA went off?

A319 followed UN789 for about 20 minutes before turning left at MIKE. During this period it would have been visible on my radar, but this route section was in the adjacent

[22] 1 nautical mile = 1852 meters, 15nm/minute = 1668 km/hr

[23] *An occurrence under almost identical circumstances occurred in another BLUE control centre approximately 3 months later, and was formally investigated.*

sectors and not conflicting with any of my traffic – I don't recall seeing it. After it turned left at MIKE there was about 4 minutes before the STCA.

2. How many aircraft tracks cross your radar but are not in your airspace?

The Height filter was set to screen out flights below FL335; my lowest useable FL was FL360. Flight levels 340 and 350 are not in my sector but are two of the most used flight levels (they are fuel efficient for cruising jet aircraft and usually above the weather). I estimate that between 30-40% of the targets displayed on my radar are not in my airspace. These targets are displayed identically to targets in my airspace; the only difference is the Mode Charlie height readout. I can't screen them out because I need to consider them during co-ordination with the sector underneath mine, especially when I need to resolve a conflict vertically into their airspace, and I need to see traffic climbing or descending in or out of my sector.[24]

3. What would have helped you get the right picture?

If A319 had checked in on my frequency (before entering the airspace), then I would have been alerted to its presence.

4. Would any specific training, experience, knowledge or co-operation have helped?

No.

5. If a key feature had been different, what would you want it to be?

Having A319 on the frequency… Nevertheless, an aircraft that checks in and off the frequency for just a couple of minutes and doesn't usually need any control, adds to frequency congestion and co-ordination in a sector, that is already traffic intensive and complex.

6. Could clearer company guidance / procedures or design have helped you make better goal trade –offs?

I did not feel under excessive production pressure. The ATS route structure or airspace boundary design could be modified to avoid UL123 clipping the airspace, but changing the route structure might create new problems elsewhere. Modifying routes or airspace

[24] Tracks below the BLS have grey labels, Tracks in the BLS span are yellow.

boundaries that overlap another Air Navigation Service Provider (ANSP) are especially problematic. Changes affecting national interests and company revenues involve complex and sensitive negotiation.[25]

Part 4 - Miscellaneous

Human Error in ATM (HERA)

1. The "personal thoughts" you mentioned in the HERA interview – can you clarify? Were there problems with the same Planner? In the previous session?

The personal thoughts related to the previous control session (before the break). During this session I had been working in a <u>different sector with a different Planner</u>. There had been a lack of co-operation. I was irritated and had been mulling it over during the break. When the loss of separation happened I was engaged with solving the problems over BRAVO but the irritation during the previous session had been at the back of my mind. The thoughts were personal but work related. Personal thoughts unrelated to work are more easily left at the work-place door.

Critical Incident Stress Management (CISM)

2. What is you opinion of CISM?

There was a general discussion about our personal experience of post incident stress and the value of CISM. We both agreed that CISM is valuable.

3. Why did you refuse CISM?

There was no CISM peer diffuser with experience on my sector available – I was not comfortable that a diffuser from another sector would understand the situation. I did receive a diffusing benefit from the Safety Manager who investigated the occurrence. Working through the voice recording and his interviews helped me talk through and out what had happened. I did not suffer any flashbacks, night-sweats, depression or stress related feelings of anxiety after the incident.

Part 4

Unit Safety Culture - discuss:

Context – Safety / production efficiency balance

---

[25] The critical adjacent airspace is operated by a competing ANSP and from inside another nation state.

I did not feel under excessive production pressure.

Goal trade offs. ETTO

Efficiency Thoroughness Trade Offs are an operational reality

A "SHELL" checklist was used to check that all these item were covered in the interview or in the original report

Software – procedures / symbology

Hardware – machines – HMI - radar display – strip bays, RT congestion /clarity

Environment: noise, temp, training, distractions

Liveware (Human interactions) with Pilots and Planner - is the TRM functioning appropriately?

Liveware / Liveware – organization - context

Organizational - context

Roster cycle, adequate breaks?

Fatigue was not a factor

Training pressure?

Training was not in progress and was not a factor

Currency

Current in the position and licensed controller for 8 years

Change Management / pace of change

Not excessive and not a factor

Hierarchical – Feedback - Safety Management

A sketch of the section Safety management hierarchy was drawn

Safety culture

Safety culture at the operational level remains strong

Motivation / satisfaction

Highly motivated, ambitious and enjoy the profession

Valued, Supported, Empowered?

Input / opinions of Controllers are not always appropriately valued within the organization. I do not feel empowered to effect change.

Fatigue / Burnout

No, not fatigued and enjoying life.

Future

Electronic strips – safety nets – constraints

A discussion about the replacement electronic Human Machine Interface (HMI) soon to be implemented. Current understanding of the new system HMI is that an electronic flight strip pertaining to an aircraft in a sector cannot be discarded before the aircraft leaves the sector.

System for detecting airspace penetrations

A discussion about the benefits and drawbacks of safety nets

Equipment manufacturer feedback and design constraints

A discussion about the operational input to the development of the new HMI

Annex: B

Planner Record of Interview

Thursday April 30 2009 14:00hrs for 2hrs

Description of Working Arrangements:

Positions of the Radar Controller / Planner - Supervisor and others see *Fig x*

Radar setup: scale *set at about 212nm,* ***h*eight filters:** *I no longer recall the exact setting* **STCA** *working***, RVSM** *yes.*

Airspace boundaries / co-ordination partners – ATS route structure – crossing points *See fig y, Vertical limits were FL355-660, lowest useable level FL360*

Strip bays and strips generally, and then specifically for the routes used by B738 and A319 *See fig z*

Describe UL123 "standard" handling procedure / co-ordination – and strip handling.

The description was identical to the Radar Controller's account.

Standard company regulations require that aircraft should be transferred to the sector control frequency 3 minutes prior to entering the sector boundary. Nevertheless**,** because aircraft on MIKE –CHARLIE section of UL123 only travel for approximately 15nm (for 2 minutes) through the Sector No.1, accepted practice was to transfer them direct to Yellow Section. Traffic on UL123 (such asA319) is in the west-bound semicircle at **even** flight levels; traffic on UN456 (such as B738) is in an east-bound semicircle at **odd** flight levels. Therefore**, provided there is no level change**, these flights do not conflict.

Before the STCA

1. What Information sources were you relying on?

The flight strips, Radar, Radar Controller, and telephone co-ordination partners; 8 co-ordination partners – 7 adjacent sectors laterally and one below the airspace.

2. What were you seeing?

I was looking primarily at the strips, about 80% of the time I am looking at the strips and engaged in co-ordination with the adjacent sectors. About 10% of my time I look at the

radar and about 10% is free for general awareness of what is happening in the room around us.

3. Where was your attention focused?

The main focus of my attention was the BRAVO bay strips.

4. What were your goals?

Identifying any procedural conflictions, basically any traffic that will be; over the same fix, at the same level, within 10 minutes of each other, [26] *and co-coordinating revisions (changes of time estimate or flight levels) with the adjacent sectors.*

5. Were there goal trade offs – time or other resource pressure?

No, I was not under any pressure, traffic was picking up over BRAVO but it was not too complex and everything seemed under control.

6. Where was the Radar Controller's focus of attention?

I can't really say for sure, but I think we were both focused on BRAVO.

7. What were the Radar Controller's goals?

His goals are separation of the aircraft, and an expeditious flow of traffic.

8. What were your expectations about the Radar Controller's role?

We work as a team, but we have different roles. I'm concerned primarily with the strips and coordinating information with the other sectors. I monitor the radar and radio whenever I can, but it is not my role to check his every word or action. Of course we check understanding and communicate constantly by talking, pointing, with strip markings and strip movements, but we do not supervise each other. Our tasks are partly separate, but also continuous, simultaneous, and connected.

[26] Conflictions identified during the planning phase can be solved by co-ordinating a level change, speed control, route adjustment, or identifying the problem with a "W" (for warning) on the strip as a reminder that it must be monitored and solved later (laterally with a vector or vertically) by the Radar Controller.

9. When did the A319 and B738 strips first appear in the ALPHA bay?

The strips usually appear in the ALPHA about 15 minutes before their estimate for ECHO around 10-12 minutes before the airspace boundary. It can vary a little depending on the Flight Data's workload, but I don't think they were especially early or late.

10. How long did these 2 strips stay in the ALPHA bay?

It's not possible to be precise, but normally the B738 strip would stay in the bay at least until he checked in on the frequency, which should be at least 3 minutes prior to the airspace boundary. The A319 strip should stay in the bay until the aircraft has vacated the airspace. However, if there is no apparent confliction, and there wasn't, then they might both have been discarded before the aircraft actually pass each other.

11. Who removes the strips? Planner or Radar controller or both?

Usually the Radar Controller removes the strips, but if the aircraft have definitely past each other, then the Planner might remove them too. I'm not certain when they were removed or who moved them – they were procedurally separated, and seemed of little interest.

12. Where was the A319 ALPHA strip when the STCA occurred

I don't know, but I think that both strips had already been discarded.

13. What does the absence of strip markings on the A319 strip indicate?

The call-sign should have been crossed out to indicate that he was not coming on the frequency – but they never are. No warning W – because there was no planning confliction.

14. How long was the A319 in the ALPHA bay before the STCA?

I don't know whether the strip was still in the bay when the STCA went off or not, but the strip would normally have spent at least 10- 15 minutes in the bay.

15. Where was the B738 **ALPHA** strip when the STCA occurred?

I'm not sure, but the fact that the strip was not retained suggests it wasn't in the bay.

16. Why was B738 ALPHA strip not included in the records of the investigation?

I don't know, but presumably it wasn't considered significant.

17. Were there any notations on the B738 ALPHA strip?

Maybe a check mark to indicate that he checked in on the frequency, but there would not have been any warnings ("W") because there was no procedural conflict.

18. How would you describe the general traffic situation in the minutes just before the STCA?

No traffic overload, if anything we were under-loaded.

19. Was there any elbow co-ordination between Planner and Radar Controller about B738 and A319, which is not apparent from the strips or transcript?

No.

20. Were the separation implications of the B738 climb instruction apparent to you before the STCA?

No.

Post STCA

21. How would you describe the situation at that point?

I heard the Radar Controller's sharp intake of breath and saw the STCA flashing red. We were both shocked.

22. After the STCA how did you judge that you could influence events?

Planner intervention was impossible; it was already out of my sphere of influence.

23. Did the situation fit a standard scenario?

No. About once a month one or other aircraft has not reached the assigned level, but this fact is either coordinated from the other sector or noticed on the radar. In this case, prior to the climb instruction, both aircraft were in level flight.

24. Has this situation occurred before or since?

No, not in 10 years as Planner or Radar controller

25. Has this situation or something similar happened to others?

Not with aircraft in level flight, but aircraft not reaching the assigned level by the airspace boundary is a problem; this should be coordinated but this does not always happen.

Counterfactuals

1. How long do you estimate A319 was "*observable*" on radar before the STCA went off?

15- 20 minutes.

2. What would have helped you get the right picture?

If A319 had checked in on the frequency, then he would have been actively identified and the strip would have stayed in the bay until he was transferred.

3. Would any specific training, experience, knowledge or co-operation have helped?

Not really.

4. If a key feature had been different, what would you want it to be?

A319 on the frequency

5. Could clearer company guidance / procedures or design have helped you make better goal trade –offs?

A change in the route structure or airspace to eliminate aircraft clipping the sector would solve the problem. However, it is hard to see how this could be achieved. It is not a problem of politics; it's a problem of complexity. Changing the airspace would change the problem, maybe move it, but not necessarily solve it - (longish pause) unless a drop in capacity is tolerable, which of course becomes a more political question.

CISM

6. Did you consult a CISM diffuser?

No. I did talk it over with colleagues who understand the sector in the pub.

7. Did you suffer from any post incident stress?

No. I get more stress from having a new baby at home.

Unit Safety Culture

8. How would you describe the balance between safety / production efficiency in this sector?

Safety culture at the operational level is strong.

SHELL checklist

Software – procedures / symbology

As discussed.

Hardware – machines – HMI - radar display – strip bays, RT congestion /clarity

No additional factors – more colours would be a distraction.

Environment: noise, temp, training, distractions

Not a factor.

Liveware (Human interactions) with Pilots and Planner - was the TRM functioning appropriately?

Good working relationship.

Liveware / Liveware – organization – context

No additional factors were raised.

Organizational - context

Roster cycle, adequate breaks? - *Fatigue was not a factor.*

Training pressure, currency? -*Training was not in progress and current for 10 years.*

Change management / pace of change? – *Not a factor.*

Unit Hierarchical Structure – Safety Management – feedback? – *Functioning.*

Motivation / satisfaction? *Motivated and enjoying the profession*

Valued, Supported, Empowered? - *Management comments about controllers being a cost burden rather than being at the coal face of production are unhelpful.*
Fatigue / Burnout? – *Fatigue was not a factor*.

Safety Hierarchy – The perceived structure was sketched.

Annex: C

Unit Safety Manager Record of Interview

Thursday April 30 2009

History and context

The interview started with a tour of the Area Control Centre. A plan of the Operations room showing the disposition of all the sectors, supervisor stations, flight data preparation areas, and controller working positions was provided as per fig x. Approximately 60 people work in the Operations room at any particular moment. The room is staffed 365 days a year, 24 hours a day.

The equipment and working arrangements at the console involved in the occurrence was explained and photographed.

The physical process of flight strip handling from preparation by the flight data personnel through the controller strip bays until discarded was traced and photographed. The flight strips are prepared by the flight data personnel and placed in a chute which guides them into the appropriate controller strip bay 10-15 minutes before the aircraft enter the sector's boundaries.

The radar display options were demonstrated and photographed; these are set to suit individual controller preferences. There are two height filter options. A height filter can be set to filter out all aircraft at selected Flight Level. In the Sector No. 1 Top; this is usually set to filter out all aircraft 5-10 thousand feet (5-10 flight levels) below the base of the sector's vertical boundary. A second filter; the Brightness Level Selection (BLS) can be selected so that all aircraft *within* a selected level span are displayed with yellow labels; aircraft below and above this second filter are displayed with grey labels. The overall effect is that aircraft inside the sector's vertical limits are easy to distinguish from those below it. ***However, aircraft above the sector's lower vertical limit that are outside the lateral boundaries are displayed exactly as those inside the sector.*** No commercial aircraft fly *above* the sector's vertical limit (Flight level 600).

After the tour of the operational area the interview continued in an office. First we watched a replay of the incident with simultaneous Radio Telephony (RT) and the radar data displayed on a laptop computer. RT and radar data from **all** the aircraft in controllers sector was available (not just the two aircraft directly involved). Screen shots of the minutes leading up to the incident and the incident were also made available. A voice full transcript of the incident Radio Telephony is available. The investigation report from the original investigation was on the desk. The interview then continued with only the Safety manger and the researcher present.

The Occurrence

1. Did the situation fit a standard scenario?

   No, aircraft entering this high level airspace are usually in level flight (not climbing or descending) and are separated by the semicircular rule.

2. Has this situation occurred before or since?

   Not in this high level sector, but in the sector below it when climbing aircraft have not reached the assigned level as expected, there have been 4 similar events that had the potential for a loss of separation between Oct – Nov 2008. In each case the aircraft was coordinated entering the sector in level flight, but was actually still climbing.[27] *These cases were all resolved by controller intervention before there was a loss of separation.*

3. Has this situation or something similar happened to others (at another centre)?

   I do not analyze the safety data from other the other centers. Observations of this kind can only be made by Area Control Center Safety Section at our corporate headquarters, which receive the reports from all the control centers.

Counterfactuals

1. What would have helped them get the right picture?

[27] *Aircraft climb performance varies according to; the aircraft type, upper winds, air temperature, humidity and aircraft loadings (fuel, passengers and cargo). If an aircraft is co-ordinated to enter airspace in level flight but cannot reach the level before the airspace boundary, then a revision should be co-ordinated.*

If the A319 had checked in on the Radar Controller's frequency, then it would have actively engaged his attention. Passive monitoring was ineffective under the particular circumstances that occurred.

2. Would any specific training, experience, knowledge or co-operation have helped?

No.

3. If a key feature had been different, what would you want it to be?

A319 on the frequency and actively identified.

4. Could clearer company guidance / procedures or design have helped them make better goal trade –offs?

Requiring aircraft on UL123 to check in on the frequency would add to the frequency load, they would only be on frequency for around 2 minutes while they "clip" the airspace and under normal circumstances they never conflict with other traffic. Redesigning the airspace or route structure to avoid the "airspace clipping" might improve the situation, but might also create new problems elsewhere. Airspace redesign would require co-operation / compromise with another (competing) Air Navigation Service Provider. It is possible and has been done in the past, but it would be a complex task and has to be balanced against the probability of this event re-occurring and the effectiveness of alternative countermeasures.

5. What was the time frame / history over which development of the; "accepted practice" to transfer UL123 traffic direct to Yellow Sector"?

I cannot be exact about when the practice first developed; the structure of the airspace and air routes changes over time. The complexity and the intensity of traffic increased significantly over the years, but it has been the accepted procedure for at least 5 years.

Post Investigation

6. What recommendations were implemented?

Safety briefings were conducted, which described the incident and the separation problems with respect to vertical movements over ECHO. A Briefing Note was included in the standard controller briefing information system. This mandatory Safety Briefing had to be read and acknowledged by every controller holding a license in that rating

group. A warning notice from the Permanent Board has also been fixed to the sector console. The recommendation that traffic on UL123 traffic should be transferred to the sector frequency was rejected. The "accepted practice" of transferring UL123 traffic direct to Yellow Section was formalized.

7. Have the measures that were implemented been effective?

In the Top (high level sector) yes, so far there has not been a re-occurrence, but in the sector below where vertical movements are more common problems continue as we have already discussed.

As Safety Manager I make recommendations to the Chief of Section, and the Area Control Centre Safety Section at the company HQ. The Chief of Section refers the recommendations to the Permanent Board of that rating group (comprises 6 controllers) and the Safety Panel (12 controllers, made up of 4 controllers from each of the 3 EBG (airspace blocks) in this Area Control Centre). The Safety Panel and the Permanent Board then report back to the Chief of Section. The Chief of Section considers their advice, but ultimately the Chief of Section has to decide whether or not to implement a particular recommendation. In a complex case like this; with a recommendation from the Safety Manager conflicting with advice from the Permanent Board and the Safety Panel, balancing the feasibility, risks and benefits, and coming to a decision is an extremely challenging task.[28]

The Chief of Section's decision was to formalize what had become the accepted practice; i.e. UL123 traffic shall be transferred direct to Yellow Section.[29]

---

[28] *A drawing of this Hierarchy was made as per fig X*

[29] *The operational order for transfer of communication for Sector No. 2 on UL 123 was amended to reads as follows:*

"For traffic along UL123 communication shall be transferred to Yellow Sector".

In all ATM documentation, as directed by ICAO regulations, the word "shall" means mandatory.

The Chief of Section instructs the Operations Support Manager, who is responsible for implementing local regulations and negotiating any necessary agreements with adjacent sectors or from another Area Control Centre within our organization. If negotiation with another Air Navigation Service Provider (usually in another nation state) is necessary, then this would have to be conducted by the Operations Support Manager via the corporate HQ.

8. What happened to the B738 ALPHA strip? Were the other strips (all aircraft) BRAVO and other fixes retained?

No, not all the strips were retained. As a matter of standard procedure the Supervisor forwarded the relevant strips. Perhaps the B738 ALPHA strip could have been included in the original investigation notes, but I did not consider it pertinent. In all probability it has nothing written on it, and in any case it would not indicate <u>when</u> the strip was discarded.

Safety Culture

9. What is your assessment of the of production pressure; Safety / Production balance – goal trade offs. Efficiency Thoroughness Trade Offs?

Prior to Sep 2008 (global financial crisis) traffic levels had been growing steadily for several years. There was a corresponding slow rise in tension between controllers at the operational level and supervisors. From 2005 traffic increased 15 % in peak months, average about 8% and there was a substantial increase in the number of incidents. Because of early countermeasures like the Safety Action Plan; beefed up staffing in the Safety Management and managerial decisions driven by the Safety Management a turn-around could be achieved by Mid 2007. In 2008 the Key Performance Indicators (KPI) were back at normal levels. Since Sep 2008 there has been a significant drop in traffic. This has resulted in a noticeable decline in operations / supervision tension. Safety key performance indicators are now all in the green. Efficiency indicators are also all in the green, and the safety department's investigation case load has declined significantly.

It is not clear whether we had reached some sort of saturation level above which there is a steep increase in tension, or whether it is the rate of change in traffic density which is the critical factor. I suspect that controllers get gradually used to higher traffic densities. If there is a sudden decrease in traffic, then there is an easier workload and over time

people adjust to the easier conditions. If the traffic density returns to the higher level over a short period of time this could be a difficult transition. Rapid increases in traffic, even to levels that are known to be sustainable are likely to be challenging. Incremental change is easier to manage.[30]

10. How effective do you think that safety briefings which stress the need for vigilance are likely to be over the long term?

I always aim to implement systemic solutions rather than rely on warnings. The effectiveness of "active monitoring" is likely to decrease over time.

11. Are operational details understood at the management level; is there adequate operational expertise at the business level?

Yes, most of the key managers and the Chief of Section have controlling experience. Recent (current) operational experience is naturally more diluted as people move up the management chain to the business level, but we do have a functioning safety feedback channel. Investigations and other areas of safety concern are communicated openly and frankly. The freezing of the sector capacity limits is a good example of a functioning safety feedback channel with senior management.

12. Is there a Team Resource Management (TRM) problem between the functions of Planner and Radar Controller?

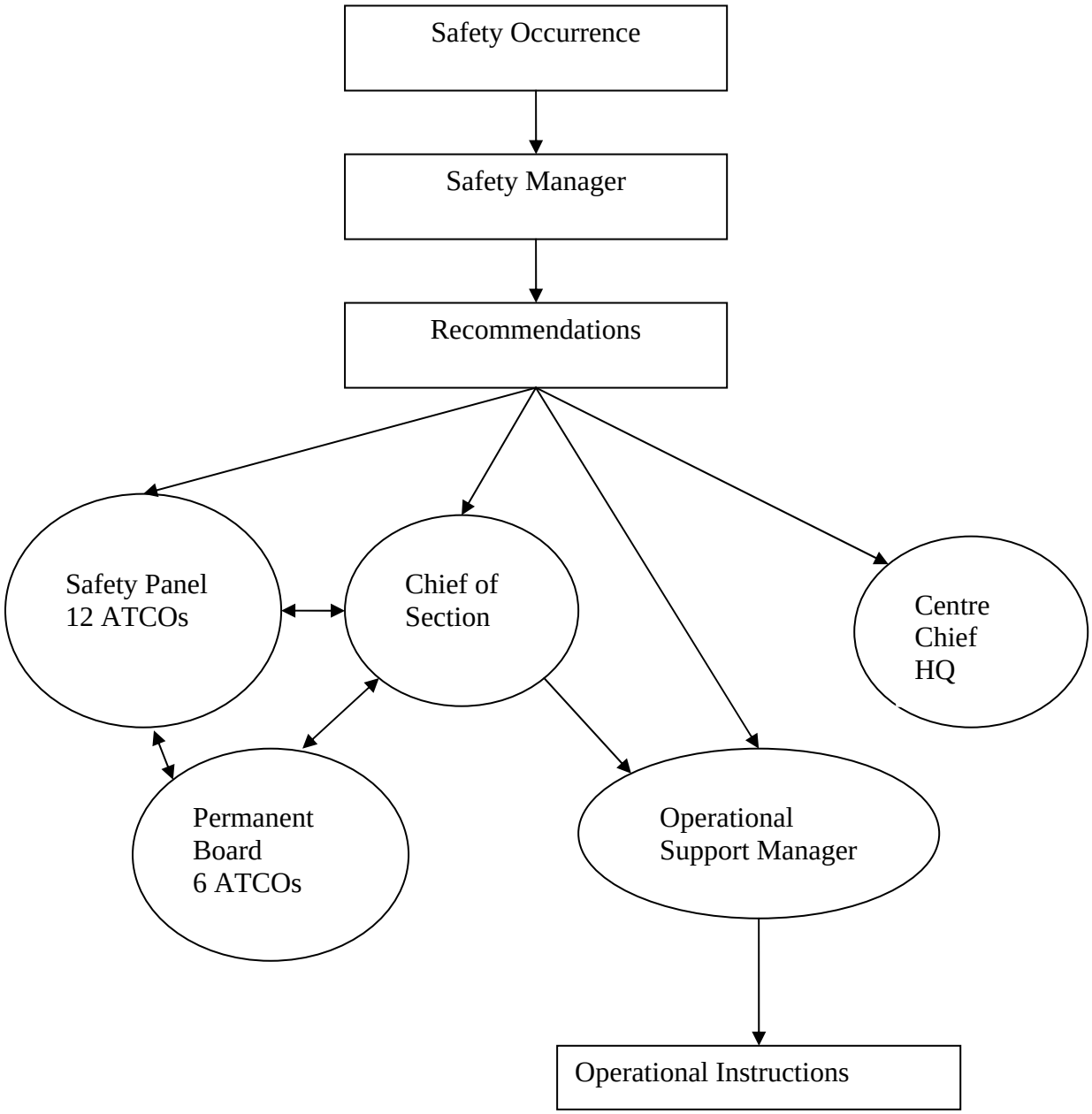
No, there are occasional clashes of personality, and some people are more able than others, but I see no evidence of a systemic TRM problem between these functions.

13. We had a short discussion about interactive complexity as described by Leveson (2002); "Normalization of deviance" (Vaughan 1996), and Jens Rasmussen's (1996) model of drift. We briefly discussed the SOAM and STAMP methodologies.

14. I asked if there were any missing items that he wanted to discuss. Nothing was raised.

[30] When there are fewer aircraft movements, the ANSP revenues fall, but the fixed costs remain high. Fewer aircraft allows a more flexible use of airspace, and the resulting track shortening further reduces the ANSP income.

Fig 13 Unit level safety management hierarchy



REFERENCES

Columbia Accident Investigation Board, (2003), Report, Vol.1, NASA, Government printing Office Washington D.C.

Cook R. (2004) *Thinking about accidents and systems*. University of Chicago Press

Dekker, S. (2001) *Reconstructing human contribution to accidents: The new view on error and performance* Tech report 2001-1 Lund University School of Aviation

Dekker S. (2002) *The Field Guide to Human Error Investigations* Aldershot UK. Ashgate

Dekker, S. (2005). *Why We Need New Accident Models* Lund University School of Aviation Technical Report 2005 -02

Dekker, S. (2005) *Ten Questions about Human Error*. Lawrence Erlbaum Associates

Dekker, S. (2006) *The Filed Guide to Understanding Human Error*. Ashgate

Dekker, S. (2006) *Past the Edge of Chaos.* Technical Report 2006-03. University of Lund.

Dekker (2008) Leading Opinion: Dekker on Resilience. YouTube (short film).

Dismukes K. Berman B. Loukopoulos L. (2007) The Limits of Expertise. UK Aldershot Ashgate

Eurocontrol (2000) ESARR2 Reporting and Assessment of Safety Occurrences in ATM

Eurocontrol (2000) ESARR 3 Use of Safety Management Systems by ATM Service Providers

Eurocontrol (2002) SOFIA Reference Manual

Eurocontrol (2003) Guidelines for Investigation of safety Occurrences in ATM

Eurocontrol (2003) The Human Error in ATM Technique HRS/HSP-002-REP-03

Eurocontrol (2003) Validation of the Human Error in ATM Technique HRS/HSP-002-REP-04

Eurocontrol (2005) Guidelines on the Systemic Occurrence Analysis Methodology (SOAM)) EAM2/GUI 8 ESARR Advisory Material / Guidance Document

Eurocontrol (2006) Revisiting The Swiss Cheese Model of Accidents. Eurocontrol Experimental Centre 13/06

Eurocontrol (2007) Pasquini A. *The fallacy of severity Classification in Risk Assessment Methods. Eurocontrol* Safety Seminar Roma Italy Oct 2007

Eurocontrol (2008) SAF-AOI ATM Occurrence Investigation IANS ATM Unit

Eurocontrol (2008) Just Culture Guidance Material for Interfacing with the Judicial System Ref. No. 08/02/06-07

Flight International (2009) World Airline Fatal Accidents and Fatalities 99-08 Flight International 20 -26 Jan 2009.

ICAO (1993) Human Factors Digest No.7 Investigating of Human Factors in Accidents and Incidents Circular 240-AN/144

ICAO (1998) Human Factors Training Manual Doc 9683 – AN /950

ICAO (2001) Aircraft Accident and Incident Investigation 9th Edition

Hollnagel E. (2004) *Barriers and Accident Prevention.* Aldershot. UK: Ashgate

Hollnagel E., Woods D. D., and Leveson N. (Eds.) (2006) *Resilience Engineering Concepts and Precepts. Ashgate.* Aldershot

Hollnagel E. (2007) *Human Factors: From Liability to Asset*. Retrieved Jan 2008 from Hollnagel's Website. pdf.

Hollnagel E. (2008) *The Changing Nature of Risks.* HFESA Journal, Ergonomics Australia Vol. 22, No. 1, March – June 08

Hollnagel E. Pruchnicki S. Woltjer R. & Etcher S (2009) *Analysis of Comair flight 5191 with the Functional Resonance Accident Model*.

Huang Y. (2007) *Having a New Pair of Glasses, Applying Systemic Accident Models on Road Safety. Linköping University Studies in Science and Technology, Dissertation No. 1051. ISBN 91-85543-64-5*

Klein G. (1999) *Sources of Power*, MIT Press Massachusetts USA

Laporte, T. R. and Consolini, P.M. (1991): *Working in practice but not in theory*: Theoretical challenges of "High-Reliability Organizations". Journal of Public Administration Research and Theory, 1, 19-47.

Leveson, N. (2002) *A New Approach to System Safety Engineering*. Cambridge, MA. MIT

Leveson N. (2004*) A New Accident Model for Engineering Safer Systems*. Safety Science, Vol. 42, Apr. 2004, pp. 237-270

Leveson N. (2008) *Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems.* Retrieved Jan 2008 from Leveson's Website: pdf.

Lowe C. (2008) A *Human Factors Perspective on Safety Management Systems*. Bristol UK Retrieved Jan 2009 from Lowe website pdf.

Marais, K. Dulac, N. and Leveson, N. (2004*) Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems*, MIT

Nelson P. S. (2008) A *STAMP Analysis of the LEX Comair 5191 Accident.* M.Sc. Thesis University of Lund

Nevile, M. and Walker, M.B. (2005) *A Context for Error* ATSB Aviation Research Report B2005/0108

Nouvel D. and Hollnagel E. (2004*) Introduction of the Concept of Functional Resonance* in the Analysis 33rd ESReDA Seminar: Future challenges of accident investigation

Perrow, C. (1984) *Normal Accidents Living with High-Risk Technologies*, Princeton University Press

Perrow, C. (1999) *Normal Accidents Living with High-Risk Technologies*, Princeton University Press

Rasmussen, J. (1994) *Risk management, adaptation, and design for safety.* Future Risks and Risk Management. Kluwer Academic Publishers

Rasmussen, J. Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad.

Reason J. (1990) *Human error*, Cambridge, UK: University Press

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

Reason J. (2008) *The Human Contribution*. Farnham, UK: Ashgate

Rochlin, G. Todd, R. La Porte and Roberts, K. (1987) *The self Designing High- Reliability Organization: Aircraft Carrier Flight Operations at Sea*, Naval War College Review

Rochlin, G. (1999) *Safe operation as a social construct*, Ergonomics Vol 42, No.11, p.1549-1560

Rochlin, G. Todd, R. La Porte and Roberts, K. (1987) *The self Designing High- Reliability Organization: Aircraft Carrier Flight Operations at Sea*, Naval War College Review

Snook S. (2000) *Friendly Fire* Princeton University Press, Princeton and Oxford

Strauch B. (2002) *Investigating Human Error: Incidents, Accidents and Complex Systems*, UK Aldershot Ashgate

Sagan, S. (1993) The *limits to safety. Organizations, accidents and nuclear weapons*, Princeton University Press

SINTEF Report (2004) *Organizational Accidents and Resilient Organizations Five Perspectives*, SINTEF Industrial Management Safety and Reliability

Vaughan, D. (1996) *The Challenger Launch Decision*. University of Chicago Press

Weick K. (1987) Organizational Culture as a source of high reliability. California Management review, 29, (2) 112-127

Weick, K. E. and Sutcliffe, K.M. (2001): *Managing the unexpected*. San Francisco: Jossey-Bass.

Woods, D.D and Cook R.I. (2002) Nine Steps to Move Forward From Error. *Cognition, Technology and Work, 4, 137-144.*

Woods, D. D. (2003) Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making. Committee on Commerce Science and Transport.


SIGILLVM · VNIVERSITATIS · GOTHORVM · CAROLINÆ
AD VTRVMQVE
1666