Aircraft System Safety – A New Approach To Assessing In-Service Performance

Steven James Bond CEng MRAeS

A thesis presented for the degree of
Doctor of Philosophy in Air Transport Engineering

City University, School of Engineering and Mathematical Sciences

September 2006

Word Count: 78,618

CONTENTS

CHAPTER THREE – THE SAFETY ANALYSIS PROCESS AND HOW IT IS GOING WRONG

TABLES

ABSTRACT

Increasingly stringent equipment performance and reliability requirements are being specified to the aerospace industry by aircraft manufacturers, driven by the expectations of both certification authorities and operators. The reality is that aircraft system and equipment reliability in service can fail to meet the design expectations.

This thesis details the problem areas within the current analysis process, describing the procedures currently in use and showing what can go wrong. It goes on to propose action that can be taken to ensure safety levels are maintained and details a new approach that is unique to this thesis. The author has devised a new System Safety Compliance Model (SSCM) for ensuring that aircraft system safety standards can be better maintained. Evolved from his earlier highly successful database system at TRW Lucas Aerospace, SSCM will be:

- Demonstrably cost effective
- A step change in process capability, offering "something new"
- Instantly accessible at shop floor level to everyone in the business
- Easy to use and as automated as possible to minimise staff training requirement
- Capable of performing instant re-assessment of safety performance down to system level and including consideration of a variety of operating environments and conditions
- The industry standard repository of component reliability data
- "Centrally" owned by a world-wide recognised industry body

SSCM is the first system to operate in such a way, and will ensure that the original system safety analysis performed at the design stage, is continually assessed for accuracy throughout its in-service life. If the new methods detailed in this thesis are adopted and acted upon, there is a high probability of a reduction in the risk of aircraft systematic failure in service, leading to increased safety in aviation. The model can be equally applied to other areas of transportation such as railways.

ACKNOWLEDGEMENTS

I would like to thank my project supervisors Professors Roger Wootton and David Stupples, plus Professors Dinos Arcoumanis and Tassos Kokkalis and Doctor Ray Neve all of City University for their considerable help and advice throughout this project.

I must also acknowledge the support and advice received from the following:

Ray Cherry of R W Cherry and Associates, Ray Christie formerly with the Civil Aviation Authority, John C Dalton of the Boeing Company, Randy Johnson at Embry-Riddle Aeronautical University, Bryan Kesterson of the Boeing Company and Jari Nisula of Airbus.

Finally, mention must be made of all those other professionals within the aircraft industry, whose work has gone before mine and has provided much useful data and information throughout this thesis.

DECLARATION

The work presented herein was carried out solely by the author, under the supervision of Professors David Stupples and Roger Wootton, in the School of Engineering and Mathematical Sciences at City University, in fulfilment of the requirements for the degree of Doctor of Philosophy.

The ideas and results are original, except where otherwise acknowledged or referenced, and no part of this work has been submitted previously to any University, college or other institution.

Steven James Bond

PERMISSION TO COPY

Steven James Bond

Aircraft System Safety Analysis – A New Approach

Supervisors: Professors David W Stupples and L R Wootton

School of Engineering and Mathematical Sciences
City University
London

I, the undersigned, am willing that this thesis should be made available for consultation in City University library, for inter-library lending, for use in another library, or for photo copy in part or in full – at the discretion of the librarian – on the understanding that users are made aware of their obligations under copyright.

Steven James Bond

GLOSSARY

AAIB	Air Accident Investigation Branch
AC	Advisory Circular
a.c.	Alternating Current
ACJ	Advisory Circular Joint
AD	Airworthiness Directive
AFM	Aircraft Flight Manual
AOC	Air Operator Certificate
APU	Auxiliary Power Unit
ARP	Aerospace Recommended Practice
ASAP	Aviation Safety Action Programme
ATA	Air Transport Association
ATP	Advanced TurboProp
BAC	British Aircraft Corporation
BAE	British Aerospace
BITE	Built In Test Equipment
CAA	Civil Aviation Authority
CAP	Civil Air Publication
CASA	Civil Aviation Safety Authority
CAST	Commercial Aviation Safety Team
CCA	Common Cause Analysis
CDR	Critical Design Review
CIR	Customer Incorrect Repair
CSDB	Common Source DataBase
DER	Designated Engineering Representative
DETR	Department for the Environment Transport and the Regions
DGAC	Direction Générale de l'Aviation Civile
DMC	Direct Maintenance Cost
DOC	Direct Operating Cost
DRACAS	Defect Reporting Analysis and Corrective Action System
EASA	European Aviation Safety Agency
ECCAIRS	European Co-ordination Centre for Aviation Incident Reporting Systems
EICAS	Engine Indication and Crew Alerting System

EMI	Electro-Magnetic Interference
EPGS	Electrical Power Generating System
ETOPS	ExTended OPerationS
EU	European Union
EZAP	Enhanced Zonal Analysis Procedure
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FDM	Flight Data Monitoring
FHA	Functional Hazard Analysis
FMC	Flight Management Computer
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FOQA	Flight Operations Quality Assurance
FRACAS	Failure Reporting Analysis and Corrective Action System
FSF	Flight Safety Foundation
FTA	Fault Tree Analysis
GAIN	Global Aviation Information Network
HHA	Human Hazard Analysis
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICBM	InterContinental Ballistic Missile
IDG	Integrated Drive Generator
IFA	International Federation of Airworthiness
ILS	Integrated Logistic Support
IPC	Illustrated Parts Catalogue
IR	Implementing Rules
ISC	Industry Steering Committee
JAA	Joint Airworthiness Authority
JAR	Joint Airworthiness Regulation
JSAT	Joint Safety Analysis Teams
JSIT	Joint Safety Implementation Teams
JSSI	Joint Safety Strategy Initiative
LROPS	Long-Range OPerationS
LRU	Line Replaceable Unit
MEDA	Maintenance Error Decision Aid

MF	Manufacturing Fault
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MMEL	Master Minimum Equipment List
MMH	Mean Maintenance Man-hours
MOP	Measures Of Performance
MRB	Maintenance Review Board
MRO	Maintenance Repair Organisation
MSG	Maintenance Steering Group
MSI	Maintenance Significant Item
MTBF	Mean Time Between Failures
MTBUR	Mean Time Between Unscheduled Removals
MTTR	Mean Time To Repair
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NFF	No Fault Found
NPRD	Non-electronic Parts Reliability Data
NTSB	National Transportation Safety Board
OEM	Original Equipment Manufacturer
OIRAS	Operational Incident Reporting & Analysis Systems
PCDU	Power Conversion Distribution Unit
PSSA	Preliminary System Safety Assessment
RAeS	Royal Aeronautical Society
RCM	Reliability Centered Maintenance
RFI	Request For Information
RFP	Request For Proposal
RFQ	Request For Quotation
RTRT	Reliability Trend Review Team
RVSM	Reduced Vertical Separation Minima
SAE	Society of Automotive Engineers
SARP	Standards And Recommended Practices
SB	Service Bulletin
SMS	Safety Management System
SOP	Standard Operating Procedure
SSA	System Safety Analysis

SSCM	System Safety Compliance Model
SSI	Structurally Significant Item
SSPP	System Safety Programme Plan
STEADES	Safety Trend Evaluation, Analysis and Data Exchange System
TC	Type Certificate
TGL	Temporary Guidance Leaflet
TQM	Total Quality Management
TSO	Technical Service Order
UK	United Kingdom
Vdc	Volts Direct Current

CHAPTER ONE – INTRODUCTION

1.0 THE AIR TRANSPORT ACCIDENT RATE

The air transport industry remains the safest form of mass transportation. A comparison with other transport types [1], as reported by the International Civil Aviation Organisation (ICAO), shows that the fatality rate in the United Kingdom per one billion kilometres travelled in each case is approximately as follows: motorcycle 49, bicycle 34, car 6.7, train 0.7, airline 0.1.

Thus the current high-level of safety within the commercial aviation industry can easily be demonstrated, and this is further born out by looking at the World hull loss and fatal aircraft accident rates reported by ICAO. Expressed as the rate per 1,000,000 scheduled departures, the hull loss rate was down to 1.0 in 2000, and declined further to 0.78 in 2004. The fatal accident rate per 100,000 flying hours has similarly declined as follows: 1975 0.17, 1985 0.13, 1995 0.08, 2002 0.07. However, in 2003 it increased again to 0.315.

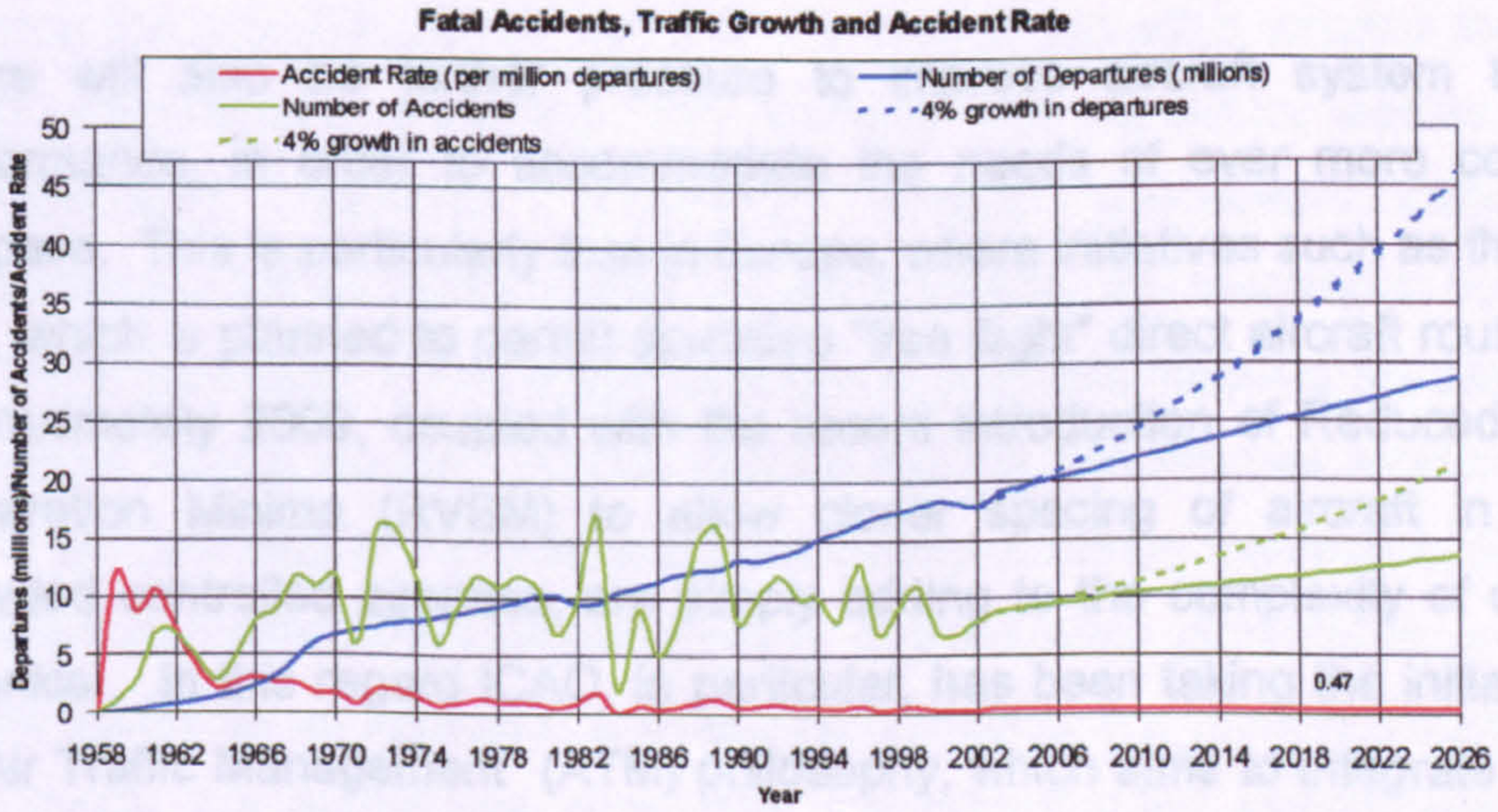


Figure 1 - Forecast Air Traffic & Accident Rate Growth ***(ICAO)***

Figure 1 illustrates not only this low accident rate, but also the effect that a widely forecast air transport traffic annual growth rate of 4% over the next few years (illustrated by the dotted lines) may have on the total number of major aircraft accidents each year. Some evidence suggests the real situation may not be this serious, but nonetheless, there remains the possibility that a doubling of air traffic movements will, as a result, double the number of accidents. Even though such events as the terrorist's attacks in the United States on 11 September 2001, the second Gulf War, etc., caused short-lived slowing of the industry's growth, from which it quickly recovered, this still means the industry could start to suffer a catastrophic accident involving a large (more than 7,500 kg empty weight) commercial airliner on average once a week. The picture is further complicated by forecast growth patterns in such parts of the World as China and South America, which are already seeing much higher rates of growth, in what statistics still show are riskier areas of airspace.

This potential elevated accident rate will clearly not only be increasingly financially unsustainable by the industry, but is also likely to be unacceptable to the travelling public, placing considerable strain on an industry which is already struggling to survive as margins shrink to levels not previously seen. This downturn has resulted in all but one of the six major US carriers having periods in Chapter 11 bankruptcy protection over the last two years. A study by the NLR in the Netherlands [2], calculated that the average cost to the airline industry of a single passenger fatality in a commercial flight was $3.2 million.

There will also be further pressure to improve aircraft system technical performance, in order to accommodate the needs of ever more congested airspace. This is particularly true in Europe, where initiatives such as the Single Sky, which is planned to permit so-called "free flight" direct aircraft routing from approximately 2009, coupled with the recent introduction of Reduced Vertical Separation Minima (RVSM) to allow closer spacing of aircraft in already crowded controlled airspace, are simply adding to the complexity of on-board avionics. In this regard ICAO, in particular, has been taking the initiative with its Air Traffic Management (ATM) philosophy, which aims to integrate a global ATM system, with states and industry working together to design and implement an increased-capacity system with improved safety levels at its core.

While it is true that, in recent times, the years 2003 and 2004 both demonstrated some progress in further reducing the overall accident rate, there is no room for complacency, as was demonstrated by an upward trend in total numbers of fatal accidents and passengers killed in 2005. In that year there were 34 fatal accidents (28 in 2004), killing 1,050 people (466). Of these accidents, no fewer than 11 had technical or maintenance causal factors. Some accident categories, such as Controlled Flight In to Terrain (CFIT), with seven accidents in 2005, and those associated with the approach and landing phase of a flight, stubbornly refuse to go away or to demonstrate any significant and sustained improvement. Against this is an International Air Transport Association (IATA) target to reduce the accident rate to 0.65 per million departures by the year 2010.

1.1 HUMAN FACTORS *VERSUS* ENGINEERING FAILURES

Another frequently quoted statistic states that of the total number of accidents (and indeed of non-catastrophic incidents), something approaching three-quarters are either due to, or have a contributory causal factor of, human error. For example, in a June 2002 Statistical Summary [3], Boeing examined a sample of 210 hull loss accidents from 1992 to 2001, and identified the flight crew as the primary cause in 66% of these. Regardless of whether the "human factor" as it is now universally known, originates on the flight deck, in the hangar, on the ramp or in the air traffic control tower, this extraordinarily high rate has become the major focus for air safety improvement effort around the globe. Many organisations, including both advisory and regulatory bodies, aircraft manufacturers, systems suppliers, aircraft operators, maintenance organisations and air traffic control service providers, are involved in substantial and on-going efforts to find ways of understanding and reducing the percentage of human factors events. These include the US Commercial Aviation Safety Team (CAST) and in Europe, the Joint Safety Strategy Initiative (JSSI), both accident reduction target driven groups, concentrating primarily on such high profile accidents as approach and landing accidents and runway incursions. In this thesis, the author will show that the statistics for aircraft system and

component failure issues are such that continued effort is also needed in these areas.

Industry bodies including the Flight Safety Foundation agree, however, that compared with all other forms of transportation, airline flying is both relatively and acceptably safe. Furthermore, most agencies, such as the Flight Safety Foundation in its annual review of airline accidents [4] also agree that the primary causes of fatal accidents are generally in the ratio of 80% due to human factors and 20% due to "system" failures. Interestingly, the JSSI team looking at key safety areas on which to focus, has prioritized the top four as CFIT, approach and landing, loss of control, and design, showing that at least in some quarters, concern is starting to be expressed on technical issues.

1.2 WHAT IS BEING DONE TO IMPROVE IT?

Today there are many good reasons to focus on reducing the accident rate still further. As has already been said, given the predicted growth in air travel over the next decade, unless something significant is done, there may be something like one major aircraft accident every week within the next decade. This is obviously an unacceptable situation both for the industry at large and the travelling public, as well as affecting those who are already reluctant to fly. Furthermore, with the coming of even larger aircraft such as the Airbus A380 and Boeing 747-8, the aviation insurance industry is rightly concerned at the potential for very large compensation payments, way beyond anything that has been seen to date, in the event that one of these types suffers a major accident.

Pressures on the airline industry such as environmental concerns about atmospheric pollution, and ever-increasing fuel prices, coupled with the impact of low-cost carriers, has lead to erosion of profit margins to very low levels. Thus it can be seen that any significant addition to the operators' overall cost burden through the knock-on effects of increasing accident numbers, may have a very serious effect on the survivability of at least some carriers.

1.3 WHY THE INDUSTRY SHOULD BE WORRIED ABOUT SYSTEM FAILURES

Figure 2 – Total Fatal Accidents And Design / Maintenance Primary Causes

Figure 2 looks at the total fatal accident numbers from 1999 to 2005 and considers those with design or technical failures and also maintenance errors, as a primary cause. From this it can be seen that these causes are increasing as a percentage of the total accidents.

Many organisations are actively concentrating their efforts on those 75-80% of accidents for which the major causal factor was considered to be "human error". Another driver for this focus is coming from the industry regulators, including the Federal Aviation Administration (FAA), which has stated that:

"Since most aircraft accidents are caused by something other than equipment failures, increasing the reliability of the installed systems to try to improve safety will have little positive effect on reducing aircraft accidents when compared with reducing accidents due to pilot error"

Is this true, or is the issue of aircraft system safety in danger of being overlooked as the focus remains on human factors? Has the industry perhaps become lulled into a false sense of security by a perception that the system

safety analytical process must be working efficiently, since there has not been a significant number of accidents directly attributable to system failures? The emphasis on human factors events must be taken into account in the system safety arena too, as is evidenced by the increasing incidence of maintenance errors, which may in turn be driven, on occasion, by poor design. The issue with design is that efforts to make systems increasingly reliable obviously costs money and with systems generally performing very well now, the point of diminishing return on design cost and effort can be reached. This is the basis of the principle of As Low As Reasonably Practical (ALARP), whereby the balance of cost against performance improvement is measured, and which takes into account such mitigating issues as human skill and competence in the face of unusual situations. Despite this, there are still additional steps that can be taken to improve the situation throughout the product life cycle from start of design to final withdrawal from service, and to do so in a cost effective manner, as this thesis will show.

"A systematic event is one that can be due to faults in the specification, design, construction, operation or maintenance of the system or its components undesired state of a system, that is not associated with physical degradation of a component, that results from a given set of conditions being satisfied." [5]

A recent study [6] into causal factors in aircraft accidents between 1985 and 2004 showed that out of 728 accidents with the potential to have been prevented by the elimination of one causal factor, design was identified as the factor in 47 cases (6.45%). Had those design-related accidents been prevented it was postulated that no fewer than 3,303 lives would have been saved.

The main objective of the thesis is to demonstrate that there is a need to change the way in which industry currently goes about monitoring system safety performance in service, and propose an approach for monitoring and communication back to the points of origin within the design and manufacturing sector. This in turn should lead to a significant change in not only the methodology used for system safety assessment, but also its efficacy.

Attempts have been made in recent years to look at commonality of processes, but so far they tend just to highlight the different approaches adopted by various sectors of the industry, without offering solutions. Furthermore, there seems to have been no attempt to co-ordinate these initiatives and pull them together into an overall "game plan" for future systems analyses. A key issue is that while there are many systems in place to capture in-service event data at operator level, and allow the sharing of that data with both other airlines and the aircraft manufacturers (in itself often affected by data sensitivity issues), there is no similar system for getting relevant and vital failure and event data back to the system suppliers – the people well placed to understand what is going on - and thus initiate any safety enhancements which may be required as a result.

1.4 THESIS OBJECTIVES

Failure to understand the part on-going safety analysis has to play in establishing the optimum levels of aircraft safety, can lead to over-engineered/over-complex systems, ineffective built-in test capability, unexpected operational effects in service and safety margins being eroded. At best this might lead to expensive and time-consuming equipment re-design or modification, or perhaps equipment life constraints with an inevitable loss of confidence and rising cost.

When in-service event data is collected, the effects of varying operational and environmental scenarios are not always considered, communicated to those who need to know about them, or even understood at all. Thus the concept of in-house reliability databases based on empirical data remains in its infancy. A failure to notice problems, to listen to the equipment maintainers, to seek feedback from all the operators or to learn the lessons of history is still far too prevalent.

The industry needs to recognise this lack of effective feedback. Aircraft manufacturers, equipment manufacturers and their suppliers, operators and repair organisations should be encouraged through regulation to share experiences with each other in the interests of safety, and many attempt to do so already, with some limited success.

The objective of this thesis is therefore to develop a new methodology for establishing such a feedback loop, which will ensure that the required data is captured, analysed and acted on in a timely and robust manner.

1.5 HYPOTHESIS

The main constraint on maximising the effective use of vital in-service data is the lack of an effective, easy-to-use and universally adapted data collection, analysis and feedback method, which carries information back from an event on an aircraft to parts reliability and human factors events databases and a linked automated system safety analysis.

The principle theme of this thesis is that a reliable, robust, and rapid feedback mechanism from an aircraft incident arising from a systems failure to a manufacturer will reduce failures that cause systems incidents and hence improve aircraft safety and airline business performance.

The thesis is a complimentary activity to the research work completed in 2005 by fellow City University PhD student Mark Pierotti [7], who has recommended a range of revised aircraft maintenance schedule design procedures.

1.6 RESEARCH METHOD

The thesis looks at a considerable number of aircraft accidents and major incidents, analysing them for evidence of technical defects that are not always immediately apparent in investigation report summaries. Furthermore, it contends that a number may have been either completely prevented, or at least reduced in their impact, had the SSCM model at the core of this thesis, been available.

It is also contended that there are substantial potential financial benefits to the industry in terms of:

- Safety enhancement through a better understanding of system performance, failure modes and overall reliability

- Cost savings through a reduction in undesired events
- Cost savings through improved reliability

Mathematical techniques were investigated, but it was found that due to the degree of subjectivity in data capture and analysis, mathematical models would be difficult to calibrate and therefore the results could be unreliable. Nevertheless, it is estimated that significant savings may be achievable following introduction of SSCM and this is demonstrated in Chapter 5.

In order to facilitate a comprehensive understanding of the objectives of the proposal, the research methodology has been broken down into the following key areas:

- A detailed literature review
- A study of the origins of formal safety analysis
- An overview of the current analysis system, including the background legislation
- Current in-service data capture and analysis systems
- A study of commercial aircraft accidents and incidents, defining accident rates, with particular emphasis on those which have design, reliability, system safety and / or human factors contributors
- A review of case studies illustrating possible flaws in aircraft design or in-service performance analysis
- Surveys of industry professionals to illicit their views on aircraft safety performance

In each case, the origins of source material used will be detailed, with amplifying information contained in a number of appendices. The detailed research work carried out under each of the above headings is described below.

The primary issues to be addressed are:

- The degree of reliance by industry on obsolete, irrelevant or incomplete reliability data when building their safety cases for certification

- The unsatisfactory level of feedback from actual in-service equipment performance in order to validate the safety level assumptions made at the design stage

As a result of this research, recommendations in a number of key areas for possible action by industry will be made, such as:

- A mandatory safety analysis process
- New industry-wide equipment and component reliability databases
- Global aircraft and system event data capture and analysis systems, communicated and made available to the widest possible audience in all sectors of the aviation industry

This thesis addresses all of these issues and, in addition, identifies two further areas of required action:

- Increased training of safety practitioners
- Management-level education of the need for and cost-effectiveness of meaningful and on-going safety analysis.

1.7 STRUCTURE OF THESIS

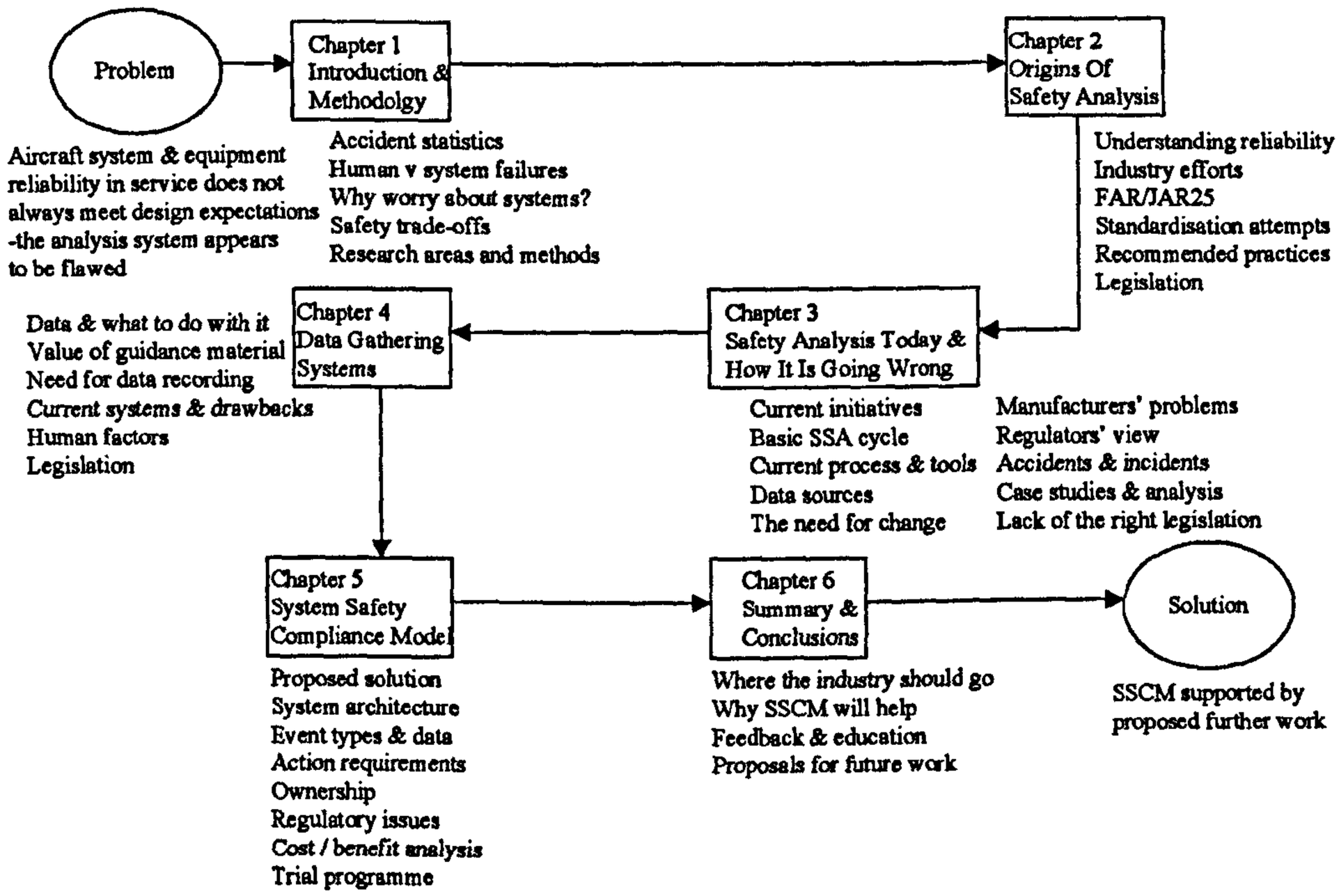


Figure 3 – Thesis Structure

The overall structure and sequence of the thesis is illustrated in figure 2 above, while the content of each chapter is as follows.

Chapter 2 – The Origins Of System Safety Analysis, explains how today's safety analysis process has evolved and how current legislation has been formulated. It also makes it clear that equipment and component reliability is at the heart of all the regulatory requirements and the design team analysis in order to demonstrate the necessary safety levels. It describes the formulation of recommended practices, indicating their shortfalls in terms of legislative requirements and the consequent freedom given to manufacturers with regard to how much or how little of the recommended analysis processes they use.

Chapter 3 – The Safety Analysis Process And How It Is Going Wrong, describes the key tools used by system design analysis teams. It will

demonstrate how complex the process is, and reinforce the view that much of it remains open to interpretation, due to such issues as a lack of the resources required to do the analysis and the absence of supporting legislation. The unsatisfactory nature of much of the basic reliability data, which tends not to be supported by in-service feedback, which is a fundamental issue throughout this thesis, is also highlighted. Finally, the chapter analyses a range of both design analysis and aircraft accident case studies to illustrate the problems being encountered and which provide substantial support for the SSCM proposal.

Chapter 4 – Data Gathering Systems, examines the use of commercially available data gathering systems to collect and analyse commercial aircraft in-service event data, and comments on the usefulness of the data captured and the effectiveness of the analysis. Regulatory guidance material is considered, and is coupled with the standard processes for formulating aircraft maintenance programmes and the associated reliability monitoring requirement. Wider issues discussed include Flight Data Monitoring (FDM), Mandatory Occurrence Reporting (MOR), maintenance error reporting, human factors issues, and the effectiveness of various industry responses. The chapter concludes with a detailed look at the key areas of system safety that need to be addressed, concentrating on clear demonstration of the need for far more accurate and meaningful event data capture and feedback than is currently available.

Chapter 5 – The System Safety Compliance Model (SSCM), introduces the central innovation in the thesis, an incident and event data capture and analysis tool that will provide near real-time assessment of aircraft system reliability and safety performance against certification requirements. The rationale behind the inclusion of additional key data including operating environment considerations is explained. Other main issues discussed include; interfaces with existing systems, the necessary regulatory input, database ownership and implementation, and a cost benefit analysis.

Chapter 6 – Summary and Conclusions, includes a final overview of the key issues and recommendations, including conjecture on the likely overall benefits of SSCM implementation. It also highlights some areas for proposed future work.

CHAPTER TWO – ORIGINS OF SYSTEM SAFETY ANALYSIS

2.0 INTRODUCTION

This chapter explains how today's safety analysis process has evolved and how current legislation has been formulated. It also makes it clear that equipment and component reliability is at the heart of all the regulatory requirements and the design team analysis in order to demonstrate the necessary safety levels. It describes the formulation of recommended practices, indicating their shortfalls in terms of legislative requirements and the consequent freedom given to manufacturers with regard to how much or how little of the recommended analysis processes they use.

2.1 UNDERSTANDING RELIABILITY

"Reliability for any organisation is not a destination – it is a journey." [8]

In essence, the safety analysis process we have today has evolved in an incremental way over several decades, and therefore it is not easy to put an accurate starting point on it. A clearly significant step was the introduction of the US Military-Standard 882 System Safety Programme Requirements, first issued in 1969, and still in common use to this day. Given that aircraft system safety levels must be demonstrated analytically, this approach requires quantification of failure probabilities against the severity of the outcome of that failure. Failure effects on the aircraft are categorised as follows:

- Catastrophic – may cause death or loss of the aircraft
- Hazardous – may cause severe injury, major property damage, or major system damage resulting in mission loss
- Major – may cause minor injury, minor property damage, or minor system damage resulting in delay or loss of availability or mission degradation
- Minor – not serious enough to cause injury or damage, but results in unscheduled maintenance or repair (in addition to delays and frustration for the passengers)

It is generally accepted that the foundation upon which safety performance of any system is built is the component and equipment reliability. Reliability analysis is thus the science of predicting, estimating, or optimising the life distribution of components of systems [9]. However, a number of definitions of reliability have been proposed, such as:

- *"The ability of an item to perform a required function for a stated period of time."* [10]
- *"The duration of failure free performance under stated conditions."* [11]
- *"The allowable number of faults in a given time."* [12]
- *"The inherent characteristic of an item related to its ability to maintain functionability when used as specified."* [13]
- *"It is reliable when the number of breaks during a specified time is at an acceptable level, or if it does not break for a specified period of time."* [14]

Although it is generally accepted today that reliability must be defined in a way that includes statements about acceptable performance under a given set of conditions over a set period of time, the fact that so many definition variations exist simply demonstrates the lack of rigour which can lead to confusion. Out of the various definitions, it can be argued that the following one is more precise and complete, since it clearly states both the need for adequate performance and conditions of use over time:

"The probability of a product (or system) performing its purpose satisfactorily for a specified period of time given specified operating conditions."

In his conference paper *The Evolution of Reliability*, [15] Paul Barringer goes on from this point to list a number of key sub-principles involved in this definition:

- Probability (chances) for survival
- Components, systems, and processes
- Functioning without failure
- Functioning for a given time period
- Duty cycles under the concept of prescribed duty
- Correct operation is a key element for survival

- Design for use in the correct environment

"Designing reliability into the component, system or process is the best practice. Designing for reliability means you must be able to specify the details. If you do not know what you want, how will you ever know if you get it? If you cannot specify what you want, you will be stuck in a take what you get environment and that usually involves high cost and much suffering." [16]

However, a note of caution must be sounded here since there has been and still exists a tendency to think that reliability numbers alone are the answer to understanding system safety performance. As Geoffrey McIntyre says in his book *Patterns In Safety Thinking* [17]:

"Like any estimate, a reliability number has both an expected value (mean) and an estimated variance. The variance is often ill defined and hard to estimate. When it is left unstated, it is tempting to read the offered reliability figure (e.g., r = .999) as a firm promise rather than the midpoint of a range.

Objective data of past system performance reveal ample evidence of systems whose promised level of reliability greatly overestimated the actual reliabilities. Experience also reveals that it is next to impossible to forecast all inevitable circumstances that may lead to a well-designed system to "fail", even given the near boundless creativity of the system engineer."

2.2 THE START OF SAFETY ANALYSIS

It should be made clear at this point, that there seems to be no single breakthrough study of safety analytical processes that can be considered as the benchmark for today's investigation. Whilst many people, such as Harold Urey in his 1934 study of the efficiency of gaseous diffusion cascades [18], and later A D S Carter at Shrivenham College laid the foundations for understanding the fundamentals of reliability, the same cannot be said for the probabilistic approach to system safety analysis. Many experts have spoken in general terms in this area, such as Charles Latino, President of Reliability Center Inc., [19] who was involved in early attempts to rationalise maintenance periods for

manufacturing machinery based on vibration readings taken over time. As a result of this work, they were able to predict component failures and take equipment off-line in time to prevent more catastrophic machine failures. "The benefit was measured in millions of 1970 dollars." [20] Nevertheless, the key point is that the safety analysis process we use today has evolved gradually in an uncoordinated fashion.

The starting point for today's processes for the reliability and safety analysis of aircraft systems was the National Aeronautics and Space Administration (NASA) Apollo moon-landing programme of the 1960s. Having been committed by President Kennedy to a very tight time schedule to achieve a manned landing on the moon "by the end of the decade", NASA quickly recognised that achievement of this ambitious goal would demand a very significant speeding up of the design, build and test effort across the board. Added to this was the fact that the entire Apollo project, including the Saturn V launch vehicle, and the lunar modules, were highly complex systems that were pushing the limits of engineering expertise and know-how; all were brought together in a very high-profile operation. At the time it was quickly recognised that some new method of confirming design safety levels had to be found, and thus the notion of assessing design failure probabilities against acceptable risk levels was initiated. The subsequent evolution of the process is discussed in Chapter 3. However, some specific programmes and events stand out as key milestones, and it may be useful to mention some of them at this stage

2.3 A TEST CASE: THE CONCORDE EXPERIENCE

Safety analysis as applied to commercial aircraft systems, as practised today, has its roots in the Anglo-French Concorde supersonic transport programme that started in the 1960s [21]. It was recognised by the joint manufacturers (the British Aircraft Corporation (BAC), now BAE Systems, and the French Aerospatiale) quite early on in the programme that, due to the advanced nature of the aircraft, far more detailed analytical work needed to be performed than hitherto in order to provide confidence to the overall safety levels of the design.

To help understand and develop the process, the Concorde team drew quite extensively on the experience and methodologies employed by NASA in the United States for various aspects of the space programme. However, the NASA activity was focused on identifying failure modes and effects, and did not extend beyond the basic understanding of failure mechanisms by taking the next step of trying to quantify failure probabilities. As a consequence, discussions were held with the Air Registration Board (later became the Civil Aviation Authority, hereafter referred to as CAA) in the United Kingdom to formulate the specific requirements for the analysis of the Concorde aircraft.

As an example of how these requirements were formulated in these early days, it is worth taking a look at the origin of the 1×10^{-9} probability requirement for the occurrence of a failure with a catastrophic consequence, which is a standard specification in Functional Hazard Assessment requirements for equipment certification. In the late 1950s, the aircraft industry in the United Kingdom was leading the field in the development of automatic landing systems (more widely referred to simply as autoland). The companies involved sought assistance from the CAA in the form of reliability requirements for the development of such systems. Over the years the CAA had accumulated a great deal of statistical data on the causes of landing accidents, and was keen to support this initiative by setting appropriate performance objectives in the form of one of the very first probability requirements.

The CAA data [22] revealed that the contemporary accident rate due to all causes was approximately 1×10^{-6}, i.e. one accident in every one million flying hours. Since contributory causes due to a system failure stood at 1×10^{-7}, the target for new systems was set at a failure rate of less than 1×10^{-7}. In the case of Concorde, it was assumed during the early design stages that there were likely to be a total of approximately 100 system failure conditions across the aircraft that were potentially catastrophic. It was therefore taken as a design aim that the aircraft should be capable of achieving a 10^2 improvement in safety levels, so that each catastrophic failure condition has a probability of occurrence of better than 1×10^{-9}.

BAC formed a Reliability, Safety and Maintainability Group, which in many ways pioneered the basic analysis that is commonplace today. One of the early lessons they learned was to beware of the risk of becoming what was known as *"probability happy"*. This meant that initially the team was perhaps excessively focused on "the numbers game", that is to say on the use of failure probabilities in system reliability studies almost to the exclusion of engineering judgement. The danger in this was the possibility that number manipulation to achieve overall reliability requirements targets could be masking more fundamental questions on systems performance and interaction.

According to an aeronautical engineer and former NTSB investigator [23]: *"The industry needs to be constantly reminded of the past so that they can be ever vigilant in the future. Believe me, as one who makes his living in the environment, I'm acutely aware that neat little 10^{-9} probabilities are not worth (much) if you are on the airplane when the numbers don't work out."*

Interestingly, Concorde Type Certificate Data Sheet No.A45EU, issued by the Department of Transportation at the Federal Aviation Administration, (hereafter referred to as FAA) in January 1979 in the Service Information section, partly addresses the not previously defined issue of safety performance in service:

"Any modification to a system or component that is the subject of special maintenance requirements must be evaluated with respect to reliability in a manner consistent with the Concorde's certification safety analyses, and the airplane's maintenance program must be amended as necessary to ensure the declared level of reliability in service for the modified system or component."

This proves that, even then, there was some recognition of the need to re-visit the original system safety analysis in the light of service experience, although it only refers to modification action rather than the more general monitoring of day-to-day equipment reliability, which, as we shall see later, is crucial to safety success.

2.4 INDUSTRY SPREADS THE WORD

The experience of the Concorde team was fortunately not lost on other major players in the commercial aircraft business. For example, the Boeing 747 and Douglas DC-10 airliner programmes started to follow similar methods of system analysis, as did the Airbus Industries consortium from the early days of their initial programme, the A300. Furthermore, this increasing focus on trying to establish some basic standardised system also came to the attention of the Fokker company in the Netherlands, who sought help in this direction as they entered the twin-jet airliner market with the F.28 Fellowship, which later evolved, into the Fokker 70 and Fokker 100 aircraft series.

2.5 THE EVOLUTION OF FAR / JAR 25

As these moves were developing, in Europe the JAA was establishing a Joint Airworthiness Requirement (JAR) Study Group to review the existing basic regulatory requirement document overlooking this area. First issued in 1974 by the FAA in the United States in the form of a Federal Airworthiness Requirement (FAR), it was entitled: FAR 25 - Airworthiness standards for the certification of multi engine turbine-powered aeroplanes with a maximum take-off weight greater than 5,700 kg (the standard certification categorisation for large commercial aircraft).

Specifically, the JAR Study Group was tasked with reviewing in detail FAR 25 to assist in the formulation and publication of the parallel European JAR 25 requirement. Active members of the study group included representatives from the national airworthiness and certification authorities of the United Kingdom, France, West Germany (as it then was) and the Netherlands, and it was agreed that there should be a system allowing some degree of national variance.

Of particular relevance to system safety, a technical sub-group of the CAA's Design and Construction Group was formed specifically to review the content of FAR 25 (section 25.1309), which was concerned with system reliability, and the effects of failure on aircraft safety. To illustrate the result of this activity, the

key parts of section 25.1309 in both FAR 25 and JAR 25 are summarised in table 1 below.

Section	Description
25.1309.(a)	The equipment, systems, and installations whose functioning is required by the JAR and national operating regulations must be designed to ensure that they perform their intended functions under any foreseeable operating conditions. However, systems used for non-essential services need only comply so far as is necessary to ensure that the installations are neither a source of danger in themselves nor liable to prejudice the proper functioning of any essential service
25.1309.(b)	The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that –
25.1309.(b)(1)	The occurrence of any failure condition which would prevent the continued safe flight and landing of the aircraft is extremely improbable, and
25.1309.(b)(2)	The occurrence of any other failure condition which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions is improbable
25.1309.(c)	Warning information must be provided to alert the crew to unsafe system operating condition, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimise crew errors which would create additional hazards

Table 1 – Key Sections Of FAR / JAR 25

What this work essentially set in place, was the recognition that systems could only be certified on the basis of probability, using in-service data. Although numerical probability requirements were not specified in FAR / JAR 25, they were listed in Advisory Circular Joint (ACJ) publications as a means of defining to industry the levels of reliability expected against different hazard categories to permit certification of the system.

At this stage the FAA also accepted the need for probability numbers to be specified, while the CAA wanted to go a stage further and introduce a code of practice for the aerospace industry on both sides of the Atlantic. Accordingly, a new study group, chaired by the JAA, was established to explore this possibility, with the intent being to issue an Advisory Circular Joint (ACJ) that would go beyond the overall scope of FAR / JAR 25.1309. Regrettably, the industrial representatives in the group could not agree to a single regulated code of practice, officially citing the desire for some flexibility in their analysis methodologies as their reason for rejection. Unofficially, there was a strong feeling from some parts of the industry that they did not like the initiative, seeing it as an attempt to dictate to them how to do their job. Furthermore, it was felt that difficulties with the FAA system, whereby it was a requirement to discuss all such issues in public meetings, would only serve to drag out the process with a danger of a resultant loss of focus. Despite this, the regulatory agencies have done some work to improve their guidance material. A harmonised version of FAR 25.1309 was submitted to the FAA for review in 2001, with the intent of harmonising the FAR and JAR versions, which as has been shown, differ in some respects. Since that time, however, the new European Air Safety Agency (EASA) has started to take over the formulation of air safety requirements from the JAA, and by early 2005 was in the early stages of producing an Implementing Rule (IR) 25, which will eventually replace JAR 25. Regrettably, the indications are that it may not be fully aligned with the FAA 25 requirements, which is considered to be a retrograde step.

2.6 ESTABLISHING A RECOMMENDED PRACTICE

Having thus failed in the attempt to gain industrial acceptance of a standard procedure, it was suggested that the only way ahead was to try for a recommended code of practice, which might be more palatable since it would not be enforceable. The intent was quite clear; to produce a set of guidelines and methods for performing safety assessment to show compliance with FAR/JAR 25.1309. An example, looking at the specific detail of the requirement for an electrical system, is shown at Appendix A.

There is evidence that much of this requirement was not and still is not performed to a satisfactory standard, if at all, but the fact that the methodology for analysing systems was not mandated, meant that there was no incentive for some manufacturers to pay full attention to what they were being asked to do. In particular, sub-paragraphs d(1) and d(2) (part) relating to damage from external sources and undetected failures, are frequently ignored during the course of a system safety analysis, often because they are considered to be either too difficult, too time consuming, or both.

2.7 AEROSPACE RECOMMENDED PRACTICES

In the early 1990s the CAA approached the Society of Automotive Engineers (SAE), a body highly respected for its technical expertise and frequently actioned by the FAA to produce recommended practice and Technical Service Orders (TSO). Therefore, a group known as the S-18 Committee was established to formulate the new documents. This committee included representatives from:

- Aerospatiale
- Allied Signal
- Allison Engines
- Boeing Commercial Aircraft Group
- British Aerospace
- Civil Aviation Authority
- Daimler Benz Aerospace
- Federal Aviation Administration
- Honeywell
- Rockwell Collins
- Rolls-Royce
- SAE

As a result of the establishment of the committee, two Aerospace Recommended Practices (ARP) were issued by the SAE in 1996:

ARP4754 – *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*
ARP4761 – *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

At the time of issue, these ARPs superseded two earlier practices, ARP1834 and ARP926A which contained information about fault and failure analysis. The new ARPs were intended for periodic updates in light of feedback from industry and technological changes, with the first such update of ARP4761 expected to be issued in 2008.

The processes for assessing safety standards of software are contained within standard DO178B (a new version DO178C was in preparation in 2006, but it still will not identify any methods available to assign quantification values to software failures or errors).

In December 2003, the SAE issued a new standard, ARP 5150 *Safety Assessment of Transport Airplanes in Commercial Service*, which addresses the safety assessment of aircraft after delivery and throughout their operational life. It is associated with showing compliance with the regulations, and also with assuring a company that it meets its own internal standards.

John C Dalton [24] of Boeing, who also chairs the relevant SAE committee that formulates these standards, has said:

"You are correct in stating that the present standards are not as good as they should be. Safety is never as good as it should be. That is why we must constantly struggle to advance the art and science of safety assessment. However, ARP4761 *remains the standard for new airplane safety assessment against which all others are measured at this point."*

2.8 THE AIRCRAFT CERTIFICATION AUTHORITIES

The airworthiness certification authorities, as expected, demand the highest possible levels of aircraft and system safety commensurate with achievable

design and manufacture. This is done by specifying the maximum acceptable rates of equipment failure dependent on the severity of the outcome of that failure. In the case of a failure with the potential for a catastrophic effect, i.e. the loss of the aircraft and/or death or serious injury to its occupants, the requirement is that the probability of occurrence is better than 1×10^{-9} failures per million flying hours. Less serious failure effects will have lesser requirements, stepping down to 1×10^{-3} for minor events that have no operational effect on the aircraft and usually result in an unscheduled maintenance activity at the next convenient time on the ground. In military programmes, it used to be traditional to just specify the Mean Time Between Failure (MTBF), or the equipment removal rate per 1,000 flying hours, but the defence ministries are also becoming smarter customers and are tending to fall into line with civil requirements, especially so as more military aircraft are now derivatives of existing civil designs.

FHA NO	SYSTEM FAILURE	FAA/JAR REQUIRED PROBABILITY PER FLT HR	CALCULATED PROBABILITY PER FLT HR	COMPLIANCE WITH FAA/JAR REQUIREMENT
1	Loss of AC bus 1 (in ACPC or CCBP)	1E-3	2.75E-4 (ACPC) 2.76E-4 (CCBP)	Yes
8	Loss of AC bus 4 and AC bus 1 (in ACPC)	1E-5	2.28E-7	Yes
46	Loss of 2 Electrical Management System Control & Display Units (EMS CDU).	1E-7	4.72E-9	Yes
47	Loss of all 4 DC busses (including loss of both batteries).	1E-9	5.34E-11	Yes

Table 2 - Typical Functional Hazard Analysis Table ***(Goodrich Aerospace)***

It is worth noting that in its response to the UK Department for the Environment, Transport and the Regions (DETR) Consultative Document on the Future of Aviation, the Royal Aeronautical Society (RAeS) [25] has called for "International regulation for the safe design and operation of aircraft".

2.9 THE AIRCRAFT AND EQUIPMENT MANUFACTURERS AND THEIR CUSTOMERS

Overall, the aircraft manufacturer's view is that they expect these safety levels from their equipment suppliers at both minimum cost and maximum reliability. Although the trend today is for aircraft manufacturers to increasingly bring equipment suppliers onto their programmes as risk-sharing partners, nevertheless many suppliers retain a natural interest in maximising their profit margins and, in many cases, protecting their "after-market" spares sales and support businesses by not designing equipment that is so reliable that, once in service, returns for repair or overhaul are rare. In other words whilst meeting the safety requirements, they will be looking to strike a balance of what is achievable given the other constraints of development cost, selling price, time to market, manufacturability, repairability and other similar factors.

The aircraft operators want a low purchase price with minimal maintenance activity and thus the lowest possible operating costs. Reliability must be high, and demonstrably so, failure diagnosis simple, removal and replacement time minimal, repair costs and turn-round time low. The reliability and safety performance must extend throughout the long life of the aircraft, for example values well in excess of 100,000 hours airframe life, or 25 plus years in revenue service are not uncommon.

2.10 LEGISLATION

The lack of regulatory guidance regarding the detailed system safety analysis methodology is a very significant problem. The existing legislation framed by the airworthiness authorities to ensure that aircraft systems are fit for purpose and safe, is inadequate. This is primarily because it does not specify in sufficient detail, the optimum processes to be adopted for achieving design safety confidence, but tends to simply require unspecified "analysis." Whilst the specific requirements for system performance, failure effect severity and failure probability are well defined, the required methodology is thus insufficiently defined and policed to ensure adequate adherence. Even the newly established EASA appears thus far to have failed to grasp this issue.

The anticipated issue in 2006 of a new IR 21, to replace the existing JAR 21 Design Standards requirement, appears in its draft form to be relaxing the requirements by making them more generic; this is potentially a major lost opportunity.

The FAA states in Advisory Circular 23.1309-1C Equipment, Systems and Installations in Part 23 Aircraft, that:

"This advisory circular provides guidance and information for an acceptable means, but not the only means, for showing compliance with the requirements of 23.1309. This material is neither mandatory nor regulatory in nature and does not constitute a regulation." Perhaps it should? In chapter 3 the various conflicting views that lead to the posing of this question are discussed.

The authorities response to questions in this regard, is to highlight the need for adequate training of system analysts. However, this may not be true, since most of the safety analysts working in the industry today are highly skilled professional engineers who are generally familiar with the various guidance documents and standards. However, issues such as commercial pressures and lack of resources, continue to harass the safety analyst and all too often result in the line of least resistance being taken. Experience within the aircraft system industry over many years has resulted in the following observations:

- Analysis started too late to adequately impact on design
- Analysis results "tailored" to fit the expectations or design requirements
- Incomplete analysis – the minimum to satisfy the requirement
- Suspect data which may not be supportable – e.g. failure rates
- Limited objectivity in the analysis – the designer does it himself

The result of this may be that a potentially unsafe system enters service.

2.11 THE APPROACH TO SAFETY ANALYSIS

On the basis of the above it seems that the approach to design essentially becomes a risk assessment, trading off reliability and safety requirements

against cost of manufacture, time to market and the need to protect future business such as spares sales. However, the present system followed in both the UK and overseas is too open to misinterpretation, primarily because the aircraft manufacturers themselves are often unclear and not very specific in their programme requirements to suppliers, leaving the door open to the analysis that best suits the need of the supplier, rather than that which best suits the needs of the certification authorities. Indeed, recent moves by the US Department of Defense to delete much analysis as a new programme deliverable, relying instead on the view that the manufacturer is expected to do it anyway, only compounds the problem.

The system further suffers from a lack of direction, in that the few existing guidance standards and documents are either becoming out of date or have no weight because they are not mandatory. Surprisingly, despite some discussions in the 1990s between regulators and industry to try and agree formalisation in this arena, it now seems to be the view of the certification authorities that mandating safety analysis procedures is unnecessary because there are training courses available in the tools and techniques most commonly used [26]. This misses the fundamental point that, while possessing the ability to perform the work correctly is obviously vital, without the support of procedural requirements the use of the hard-won skill of performing robust safety analysis will remain at best variable and at worst completely absent.

To illustrate these points, there are what the author considers to be the three main barriers to system safety analysis; internal company pressures to trade-off robust safety analysis, poorly understood or applied analytical methods, and unsatisfactory regulations. These can be referred to as *The Three Layers of Conflict*, as shown in figure 3 below, which are preventing industry from reaching the desired levels of meaningful analysis.

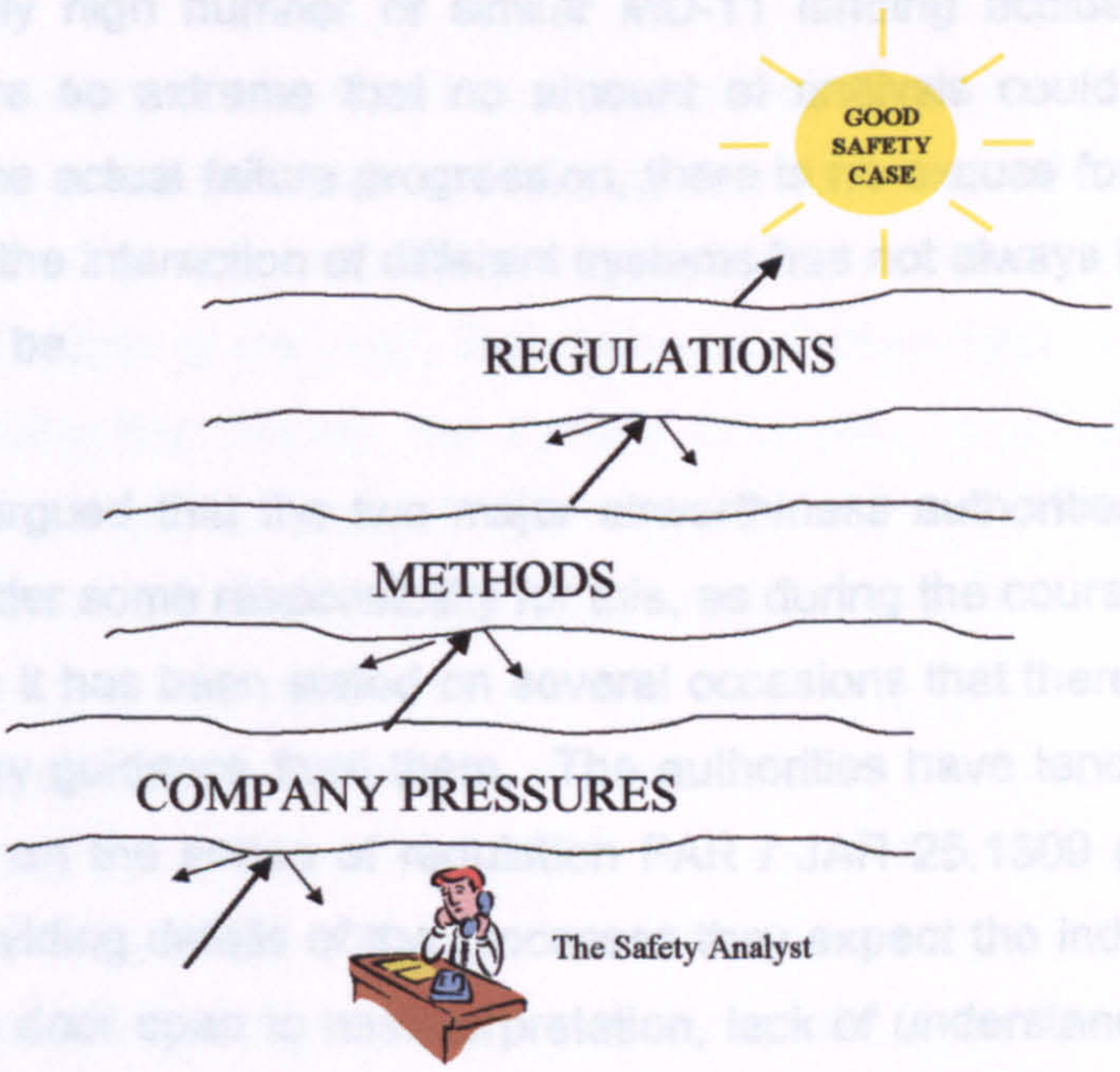


Figure 4 - "The Three Layers Of Conflict"

2.12 DEPTH OF ANALYSIS

It is apparent that in some sections of the aerospace industry, there is a lack of appreciation of both the value of the system analysis process, the point in the equipment life-cycle at which it should be started and the depth to which it should be taken for failure mechanisms to be properly understood. Too often it is the case that failures are analysed by the manufacturer as single events and effects with little consideration for either previous events, or what subsequent chain of events may occur. The more detailed investigation tends to be reactive to events, such as the excellent work done by the Air Accident Investigation Branch (AAIB) on the A340 incident described in Chapter 3.

This raises the issue of how well zonal, cross-system or whole aircraft analysis is performed (see section 3.22 onwards). Recent initiatives to establish extensive combined designer/customer teams during new aircraft development (as, for example, with the Boeing 777 and 787), plus the continued enhancement of computer-aided design and computer simulation of aircraft systems and interfaces, are all useful aids to design refinement. Nevertheless,

while it can be argued that, for instance, the circumstances surrounding the unexpectedly high number of similar MD-11 landing accidents (see section 3.29.4) were so extreme that no amount of analysis could have accurately predicted the actual failure progression, there is no excuse for the fact that the analysis of the interaction of different systems has not always been as thorough as it should be.

It can be argued that the two major airworthiness authorities, FAA and JAA, must shoulder some responsibility for this, as during the course of this research programme it has been stated on several occasions that there is a distinct lack of regulatory guidance from them. The authorities have tended to rely almost exclusively on the sense of regulation FAR / JAR 25.1309 (see section 2.5), without providing details of the processes they expect the industry to use, thus leaving the door open to misinterpretation, lack of understanding, or too much room for flexibility and short-circuiting of analytical processes as a replacement for industry experience.

2.13 OTHER SAFETY PROCESS STUDIES

The regulatory body taking a detailed look at the whole question of safety in aircraft certification is the FAA. The Associate Administrator for Regulation and Certification has conducted a lengthy study of the commercial aircraft certification process, the results of which were published late in 2002 under the title *Commercial Aircraft Certification Process Study: An Evaluation of Selected Aircraft Certification, Operations and Maintenance Processes*. In brief, this document examines:

- Safety assurance processes
- Safety data management
- Maintenance, operations and certification interfaces
- Safety oversight processes

The findings of the study are discussed in Chapter 3.

2.14 SUMMARY

The system safety analysis process has evolved in an incremental way over a considerable number of years. Although some sound efforts have certainly been made to steer the process in a systematic and robust manner, especially through the efforts of the SAE, the continuing lack of focus in this area by the certifying authorities leaves the system exposed. It is time the disparate threads were pulled together into a far more cohesive approach, truly reflecting the capabilities and fallibilities of 21st century aircraft systems.

What is needed is a regulatory confirmation of an acceptable and robust analysis standard, such as ARP 4761, and for a standard such as this to be embedded in regulatory requirement. With the emergence of EASA, whose Implementing Rules are binding on all European Union member States, this provides an excellent opportunity to initiate this cohesion effort.

In the chapters that follow, the reader will be taken through the various methodologies involved in what has become a highly complex analytical process. Due to this complexity and the various side issues involved, it is not possible to present all the material in a sequential way. However, it will all be brought together again to demonstrate both the linkages and the flaws in the current system, at the end of Chapter 4.

CHAPTER THREE – THE SAFETY ANALYSIS PROCESS AND HOW IT IS GOING WRONG

3.0 INTRODUCTION

This chapter describes the key tools used by system design analysis teams. It will demonstrate how complex the process is, and reinforce the view that much of it remains open to interpretation, due to such issues as a lack of the resources required to do the analysis and the absence of supporting legislation. The unsatisfactory nature of much of the basic reliability data, which tends not to be supported by in-service feedback, which is a fundamental issue throughout this thesis, is also highlighted.

Finally, the chapter analyses a range of both design analysis and aircraft accident case studies to illustrate the problems being encountered and which provide substantial support for the SSCM proposal.

3.1 SAFETY TRADE-OFFS

With the global air transport industry going through a period of major expansion, it is inevitable that without change, the occurrence of both human and system-based safety related incidents will increase. Since the travelling public rightly expects the highest possible levels of aircraft safety, this is reflected in regulatory requirements placed on the industry by the airworthiness certification authorities around the world.

The equipment design cycle is a balancing act, trading off the demands of safety against those of performance, cost, weight, manufacturability, supportability, time to market and so on. In addition, looking beyond fatal accidents to less serious events, unscheduled aircraft maintenance, much of which potentially, may result from unsatisfactory system and equipment reliability levels, imposes considerable extra cost and the potential for expensive delays.

Today, increasingly stringent equipment performance and reliability requirements are being specified to the aerospace industry by both certification authorities and operators. The demands of dispatch reliability and operations such as Extended Operations (ETOPS) and Long Range Operations (LROPS), place much emphasis on system configuration and design, resulting in extremely complex analyses of projected reliability and safety performance.

The reality is that aircraft system and equipment reliability in service can fail to meet the design expectations, if not on entry into service, then perhaps later in life. This could result in the certification safety levels being compromised, quite possibly without anyone realising it until something serious goes wrong.

3.2 ORIGINS OF FORMAL SAFETY ANALYSIS

In essence, the safety analysis process we have today has evolved almost piecemeal over several decades and therefore putting an accurate starting point on it, or assigning credit for so doing, is not straightforward. However, some specific programmes and events stand out as key milestones, and these are identified and put into perspective in the overall context of the thesis. The basis of safety analysis lies in equipment reliability with account being taken of the consequences of failure on the continued safe conduct of the flight, as will be explained later, and the way in which an understanding of this has been promulgated is presented and discussed.

The emergence of industry standards, both in terms of reliability and safety targets, and the necessary processes to demonstrate compliance will be described. The way in which the necessary supporting legislation has developed will also demonstrate some of the potential pitfalls in the process as it is carried out today.

3.3 OVERVIEW OF THE CURRENT SYSTEM

A discussion is included of how the current system of safety analysis is specified, including a detailed breakdown of how it is actually being put into practice (with examples), and consideration of the individual methodologies in

order to focus on any shortcomings and difficulties. The strong need to adequately address human factors issues, and the ways in which this is being attempted, are also looked at, as are the regulations covering safety analysis, both current and emerging.

This chapter also indicates those areas where the safety analysis process could result in flawed system design. In the worst cases, this may lead to catastrophic events, but even at the other end of the scale, such design flaws can have, for example, a significant impact on maintenance cost.

3.4 CURRENT INDUSTRY INITIATIVES

Even with today's excellent airline industry safety record (as discussed in Chapter 1), the pressure is still on to reduce the accident rate still further. It was stated by the UK CAA in April 2005, that the world airline fleet is currently running at an accident rate of 1×10^{-8}, which does not justify the perception that we are operating with a comfortable margin over the 10^{-9} requirement for certification of potentially catastrophic failure events. As we have already seen, given the predicted growth in air travel over the next 20 years, unless a significant accident rate reduction can be achieved, it is statistically demonstrable (see Figure 1), that, despite some recent improvements, there could be major aircraft accidents occurring at a frequency which will put a significant strain on the industry's ability to survive in its current form.

In early 1998 the JAA agreed to launch the Joint Safety Strategy Initiative (JSSI). The purpose of JSSI was to devise an agenda to achieve the JAA's stated aim for future flight safety, which is:

"The JAA aims at continuous improvement of its effective safety system leading to further reductions of the annual number of accidents and the annual number of fatalities irrespective of the growth of air traffic".

In order to try and maintain an accident rate of 1×10^{-8}, or better still to improve it against a background of forecast annual traffic growth of 5.1% [27], the main

focus of the JSSI approach is analysis of past accidents, which has led to the identification of an initial list of seven areas for attention;

- Controlled Flight Into Terrain (CFIT) – aircraft which have not suffered any kind of system failure, but which are for example, allowed to fly into high ground due to loss of situational awareness by the flight crew. Most frequently occurs during the approach and landing phase
- Approach and landing – statistically the most dangerous sector of a commercial flight, when either through human error, system failure, or a combination of multiple factors, the aircraft is unsuccessfully brought through its final descent and subsequent landing
- Loss of control – aircraft that have not suffered a system failure, but are allowed to enter irrecoverable flight situations, mainly but not exclusively, due to mishandling. This type of accident may also be caused by control due to an external cause, such as encountering wake turbulence from a preceding aircraft
- Runway incursions – aircraft entering runways or taxiways in direct conflict with other traffic
- Design related issues
- Weather – the effect of poor or rapidly deteriorating weather on the ability of aircraft and their crews to continue with a safe conduct of the flight
- Occupant safety and survivability

What is meant by an aircraft accident? ICAO favours the following definition:

"An occurrence associated with the operation of an aircraft which takes place between the time when any person boards the aircraft with the intention of flight and such time as all persons have disembarked there from, in which:

a) any person suffers death or serious injury while in or upon the aircraft or by direct contact with any part of the aircraft (including any part which has become detached from the aircraft) or by direct exposure to jet blast, except when the death or serious injury is from natural causes, is self-inflicted or is inflicted by other persons or when the death or serious injury is suffered by a stowaway

hiding outside the areas normally available in flight to the passengers and members of the crew of the aircraft, or

b) the aircraft incurs damage or structural failure other than:

(i) engine failure or damage when the damage is limited to the engine, its cowling or accessories

(ii) damage limited to propellers, wing tips, antennae, tyres, brakes, fairings, small dents or punctured holes in the aircraft skin which adversely affects its structural strength, performance or flight characteristics and which would normally require major repair or replacement of the affected component, or

c) the aircraft is missing or is completely inaccessible, or

d) significant damage is caused to the property of the Company or any third party. Significant damage in this respect may be taken to mean any damage caused which may be subject to an insurance claim."

In addition, we should not forget the less serious incidents, since they not only have significant impact on operating economics, but should also be a rich source of information for both operators and manufacturers. ICAO defines an incident as:

"An occurrence other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation."

3.5 A CLOSER FOCUS ON TECHNICAL FAILURES

Many organisations are actively concentrating their efforts on those 75-80% of accidents for which, as has already been stated, the major causal factor was considered to be "human error". Another driver for this focus is coming from the industry regulators, including the FAA, which has stated [28] that:

"Since most aircraft accidents are caused by something other than equipment failures, increasing the reliability of the installed systems to try to improve safety will have little positive effect on reducing aircraft accidents when compared with reducing accidents due to pilot error"

There is a need to investigate whether this is true, or whether the whole issue of aircraft system safety is in fact "an accident waiting to happen"? The industry has become lulled into a false sense of security with the perception that the analytical process must be working, since there has not been a significant number of accidents directly attributable to failures which had not been correctly predicted – either during the design stage or during in-service event monitoring. However, neither assumption is strictly true, as we shall see later. It can thus be argued that something should be done now to improve our system safety analysis processes, in order to minimise the potential for future catastrophic events.

"In a risk mitigation strategy, low reliance on pilot mitigation requires high mitigation by system design; high reliance on pilot mitigation requires high mitigation by pilot training. The increasing rate of introduction of new technologies increases the likelihood of encountering unexpected situations. Threat and error management is critical." [29]

Ten years experience in the field of Integrated Logistic Support (ILS), including reliability, maintainability and safety analysis across a wide range of military and civil aircraft and equipment programmes, has led to the inescapable conclusion that there is an urgent need to rationalise the way these safety analysis procedures are carried out across the industry. A number of attempts have been made in recent years to look at common processes for small areas of ILS activity, since this is a key function addressing not just the ability to support systems, but "supportability" based on the establishment and justification of the required reliability and safety performance levels. However, such attempts have so far only highlighted the different approaches adopted by various aerospace companies. Furthermore, there has been no attempt to co-ordinate these initiatives and pull them together into an overall plan for future systems analyses.

"Very little standardisation currently exists between agencies or even between the directives, regulations, and standards that implement the (system safety) requirement." [30]

3.6 ENGINEERING RESOURCE ISSUES

With the global air transport industry already going through a period of major expansion in the second half of the first decade of the 21st Century, it is inevitable that without change the occurrence of safety related incidents will increase. The industry continues to experience serious shortages of skilled aircraft maintenance engineers, which leads to increased pressure on those who are already in the profession. The situation may be eased somewhat through improvements in system safety performance from new technology, such as "glass cockpits", better on-board diagnostic/prognostic systems, and built-in-test capabilities, all of which, together with training, should aid the engineer to make better informed fault diagnosis and achieve faster and more effective repair of the faulted system or component.

Working against this is the fact that, at present, maintenance is largely being carried out by those who have learned their skills on earlier generations of aircraft and have thus had to transfer their expertise to glass cockpit aircraft. What has yet to be discovered is what will happen once the maintenance organisations are manned by licensed engineers who have only had exposure to the modern aircraft.

The travelling public rightly expects the highest possible levels of aircraft safety (albeit at a price), and this is reflected in regulatory requirements placed on the industry by the airworthiness certification authorities around the world.

Accordingly, the equipment design cycle treads a difficult and complex path, trying to balance the demands of safety with those of performance, cost, weight, manufacturability and supportability. The engineering skills shortage felt by the aircraft operators is just as pronounced in the aircraft and equipment manufacturing industry, none more so than in the areas of design analysis. In

addition, looking beyond fatal accidents to less serious events, unscheduled aircraft maintenance, much of which potentially results from unsatisfactory system and equipment reliability levels, imposes considerable extra cost and unnecessary delays affecting both the company and the passengers.

While there have been and continue to be, some serious attempts to educate engineers with, at least, an overview of the demands of safety analysis, once they have completed that education and returned to their workplace, it is all too often the case that the procedural support they need in order to be fully effective is simply non existent.

The reality is that aircraft system and equipment reliability in service can fail to meet the design expectations if not on entry into service, then perhaps later in life; this could result in the certification safety levels being compromised, quite possibly without anyone realising it until something goes wrong. Indicators such as failure to meet dispatch requirements may be poor predictors of significant system loss in flight due perhaps to the previously unrecognised occurrence of a dormant failure.

"Capital projects are justified by business units with too little budget for both time and money. The businesses expect that 'engineering will find a way...' Engineers do wonders. Engineers do not perform miracles! Projects are justified on a weak foundation and implemented poorly for lack of funding – the homework is usually deficient. The SAE advocates more preliminary design effort to avoid poor implementation of plans that result in unreliable systems. Better homework results in projects that cannot survive the return on investment criteria. In the manufacturing world, the most important tool for reliability is the Pareto distribution based on money (not based on things). Manufacturing quickly teaches that money, time, and successes are key performance indicators. You cannot make on time and on quality deliveries from a low reliability system." [31]

This is a view expressed in a similar way by the National Aerospace Laboratory (NLR) in Holland [32]:

"For most stakeholders (apart from the international regulators) there is no fixed process for decisions on safety measures. Often the decision is made by one person or a board based mainly on 'gut feeling' with multiple input. Some stakeholders perform a separate safety assessment, but this is not common practice."

When in-service event data is collected, confidence levels and the effects of varying operational and environmental scenarios are not always considered or even understood. Thus the concept of in-house reliability databases based on empirical data remains in its infancy. A failure to notice problems, to listen to the equipment maintainers, to seek feedback from all the operators or to learn the lessons of history is commonplace. Associated with this is the fact that once a product enters the in-service Post Design Support (PDS) phase of its life cycle, the original design team disbands or moves onto the next project. Thus over a period of time the corporate knowledge of the product in terms of its design rationale gradually becomes lost.

The industry as a whole needs to recognise the problem that in-service reliability and, hence, safety performance, is not being properly monitored. Aircraft manufacturers, equipment manufacturers and their suppliers, operators and repair organisations should all be prepared to share experiences with each other in the interests of safety. Many will claim that they do so already, but the fact is that take-up of such data sharing initiatives is at best patchy, as we will see later, and needs to be reinforced.

3.7 THE BASIC SYSTEM SAFETY ANALYSIS (SSA) CYCLE

The current system safety analysis process is already highly complex, with many different analytical tools combining to produce an overall safety case, by which the manufacturer can demonstrate to the regulatory authorities that his design satisfies their requirements. What is currently called for is a number of core activities including Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA), Failure Mode and Effects Criticality Analysis (FMEA / FMECA), Common Cause Analysis (CCA), zonal analysis, Preliminary System Safety

Assessment (PSSA), maintenance task analysis, minimum equipment lists, safety case, etc. Manufacturers traditionally perform all, or most, of this activity in-house, most commonly by the system designers. Occasionally the work is contracted out to specialist reliability houses, far removed from the design and production effort.

All this effort is directed towards the completion of a safety case, which is one of a suite of documents that the system and aircraft manufacturers must present to the certification authorities in order to gain approval. To give an indication of the complexity of the documentation demanded, the breakdown of a typical system reliability and safety report is as follows:

SECTION 1 - Introduction, system overview, system boundaries interfaces

SECTION 2 - System description, Line Replaceable Unit (LRU) description & function, system architecture, system logic and control, system redundancy, system interfaces, fault indication

SECTION 3 - Applicable regulations

SECTION 4 - Method of compliance

SECTION 5 - Summary and conclusions

SECTION 6 - Safety Analysis, including single significant failure events, multiple significant failure events, software certification considerations, EMI and lightning tests, design verification analysis and tests, failure rate justification (i.e. the sources used)

SECTION 7 - Periodic ground checks, dormant failures

SECTION 8 - Aircraft Flight Manual (AFM) Requirements

SECTION 9 - Master Minimum Equipment List (MMEL)

SECTION 10 - Document references

Extensive appendices contain all the analytical detail including Functional Hazard Assessment compliance tables, Failure Mode and Effects Analysis tables, Fault Tree Analysis and Functional Block Diagrams. Let us now look at some of the specific analyses in more detail.

3.8 THE CURRENT ANALYSIS PROCESS

It should be noted that in the Safety Requirements Compliance Cycle, there is an apparent disagreement between what is and is not acceptable, depending on whether or not the system being analysed is to be fitted to a single or multi-engine aircraft, with further complexity now coming in with the on-going debate over certification standards for twin and four engine airliners.

The way in which a company should outline its design analysis programme is defined in Military Standard (Mil-Std) 882C System Safety Programme Requirements. That document defines the essential contents of a System Safety Programme Plan (SSPP):

"It shall describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate/control hazards, or reduce the associated risk to an acceptable level throughout the system life cycle."

However, while requiring analytical techniques and formats to be specified by the manufacturer, Mil-Std-882C does not prescribe any preferred methodologies.

3.9 FUNCTIONAL HAZARD ASSESSMENT (FHA)

FHA is the first and potentially the most significant stage in the development of what is and what is not acceptable in terms of the reliability and safety performance of a new aircraft system. Once the initial system requirements and provisional architecture are known, it is the responsibility of the aircraft

manufacturer and the relevant certification authority to review all the predicted system failures and categorise the severity of their effects against the following standard definitions:

Severity	Categorisation	Probability of Occurrence
I	Catastrophic	$< 1 \times 10^{-9}$
II	Hazardous	$< 1 \times 10^{-7}$
III	Major	$< 1 \times 10^{-5}$
IV	Minor	$< 1 \times 10^{-3}$

Table 3 - Failure Severity Categorisations

Thus for each system failure, the manufacturer now has a "target" to reach in order to design and produce a system which will ultimately be certified. Already, the temptation to manipulate component reliability values to achieve the desired top-level probability is in place.

3.10 FAILURE MODES AND EFFECTS ANALYSIS

Central to this activity is the Failure Modes and Effects Analysis (FMEA), and Failure Mode Effects and Criticality Analysis (FMECA), well defined and long established "bottom up" processes for analysing the effects of component failures, and one that is generally performed following the recommendations laid out in US Military Handbook (MIL-HDBK) 1629A. It is absolutely critical to the success of the safety case presented for certification, that the FMEA has been performed thoroughly, preventing any unidentified failure modes appearing at a later date.

One of the key features of FMEA is the identification of so-called dormant and latent failures. A dormant failure is one which has no safety effect on its own and, when it occurs, has no system effect and is undetectable by the flight-crew until a second linked failure occurs. An example might be a lightning-strike protection device such as an electrical contactor designed to open and break a circuit should a lightning strike occur, in order to protect the equipment in the

circuit from an excessive over-current. As the contactor is normally in the closed position to make the circuit, it is possible that over time the current flow may weld the contacts together, thus preventing the contactor from opening to perform its protection function should the aircraft suffer a lightning strike. This initial welding of the contacts thus becomes a dormant failure.

Certification authorities are rightly concerned about the nature of dormant failures, and will require the manufacturer to take one of a number of possible mitigating actions:

1. Demonstrate by analysis that the probability of the dormant failure occurring is so low that it could be considered dormant for the life of the aircraft – most unlikely.
2. Demonstrate by analysis an acceptable time interval during which the failure can be considered to be unlikely to have occurred, at which point some corrective action is taken, such as scheduled maintenance or component replacement.
3. Introduce a built-in test to ensure the failure has not occurred, either at first power-up or possible at intervals during flight. In this case, what was a dormant failure is now referred to as latent.

To get the analysis right for cases 1 and 2, it is essential to correctly identify the second most probable or critical independent failure upon which the dormant failure can have an effect, given that it has occurred. An assessment is then made of the overall impact on both the system and the aircraft as a result of this combination of failures.

Where the analysis shows that there is no effect on either, or that no second failure could be linked to the dormant failure, it is assumed to be dormant for the life of the aircraft. The total expected in-service life of an aircraft could be in the order of 4,000 flying hours a year over 25 years, which equates to 100,000 hours or more, and it is clear that accurate reliability predictions are essential to give confidence over such a long period, (or even for establishing a lesser acceptable period between scheduled maintenance); yet this is one of the hardest things to predict, given the current state of reliability data systems.

Central to adequate and effective address of undesirable failure effects, is the FMECA carried out in the later stages of the analysis. As part of this effort, the predicted probability of a failure event occurring is typically compared with the consequences of its effect and presented in a matrix. The numbers contained within the matrix are unique failure mode identifiers drawn from the FMEA / FMECA analysis. The matrix is a very useful tool for prioritising where the corrective design effort should start, i.e. in the top right hand corner of the matrix, where failures are both most likely to occur and will have the most detrimental effect when they do happen.

Subsequent design effort should then work its way diagonally down the matrix towards bottom left, until a point is reached at which the effort to correct the problem no longer justifies the level of risk it will remove. However, in systems which have already been shown to be compliant with safety requirements, there will be a strong temptation to view any further re-design effort as uneconomical.

3.11 FAULT TREE ANALYSIS (FTA)

The origins of FTA can be traced to a number of parallel efforts in the United States during the 1960s. In one case, as the Minuteman Intercontinental Ballistic Missile (ICBM) design matured, concerns centered on the highly undesirable possibility of an uncommanded launch, and it was recognised that no reliable model existed to satisfactorily and methodically predict the likelihood of such an event. At about the same time Charles Latino of the Reliability Center, was working for a company where they began to employ logic trees, which were used to understand the causes of catastrophic failures. Thus was born Fault Tree Analysis (FTA), which draws on data from FMEA. FTA is a deductive approach which involves graphical enumeration and analysis of the ways in which a system failure can occur and the probability of its occurrence.

This "top down" technique is designed to ensure complete understanding of all the events that can lead to an undesirable system failure. Fault trees are the primary tool used to demonstrate compliance with FHA requirements to the certification authority, and are subject to close scrutiny. However, an

assumption is generally made that the analyst has got his raw data right, i.e. all the possible base events leading to systematic failure have been identified and included on the fault trees. The other problem here relates once again to the failure probability rates which, unless they appear to be outrageously optimistic, will rarely be challenged during the certification review.

From a data analyst's standpoint, the mathematical calculations undertaken in FTA are quite complex. The analysis must consider not only probability rates, but also what is known as "exposure time", i.e. the equipment operating time period being analysed usually being based on the average flight duration. For these reasons, it is universally acceptable (and understandable) for analysts to use various software packages to perform FTA rather than "hand cranking the numbers". The danger here is that in an environment where there are too few skilled analysts, such software is being used routinely by engineers of inadequate skill, training and experience, who may not recognise analysis anomalies should they occur. In this regard, it is worth pointing out that a few years ago a commonly used FTA software package was found to have a programming error, which was leading to incorrect top event probability calculations.

Over reliance on the expediency of commercial software without possessing a basic understanding of the analysis methodology to enable sensible checking to be carried out, can be a serious issue.

Let us look at an example, by referring to a maritime aircraft electrical system issue (discussed in more detail in section 3.29.6). Using FTA, the original prediction for the loss of all four a.c. generators, considered to be a catastrophic event, and therefore having an FHA probability requirement of less than 1×10^{-9}), is shown in Figure 5 below.

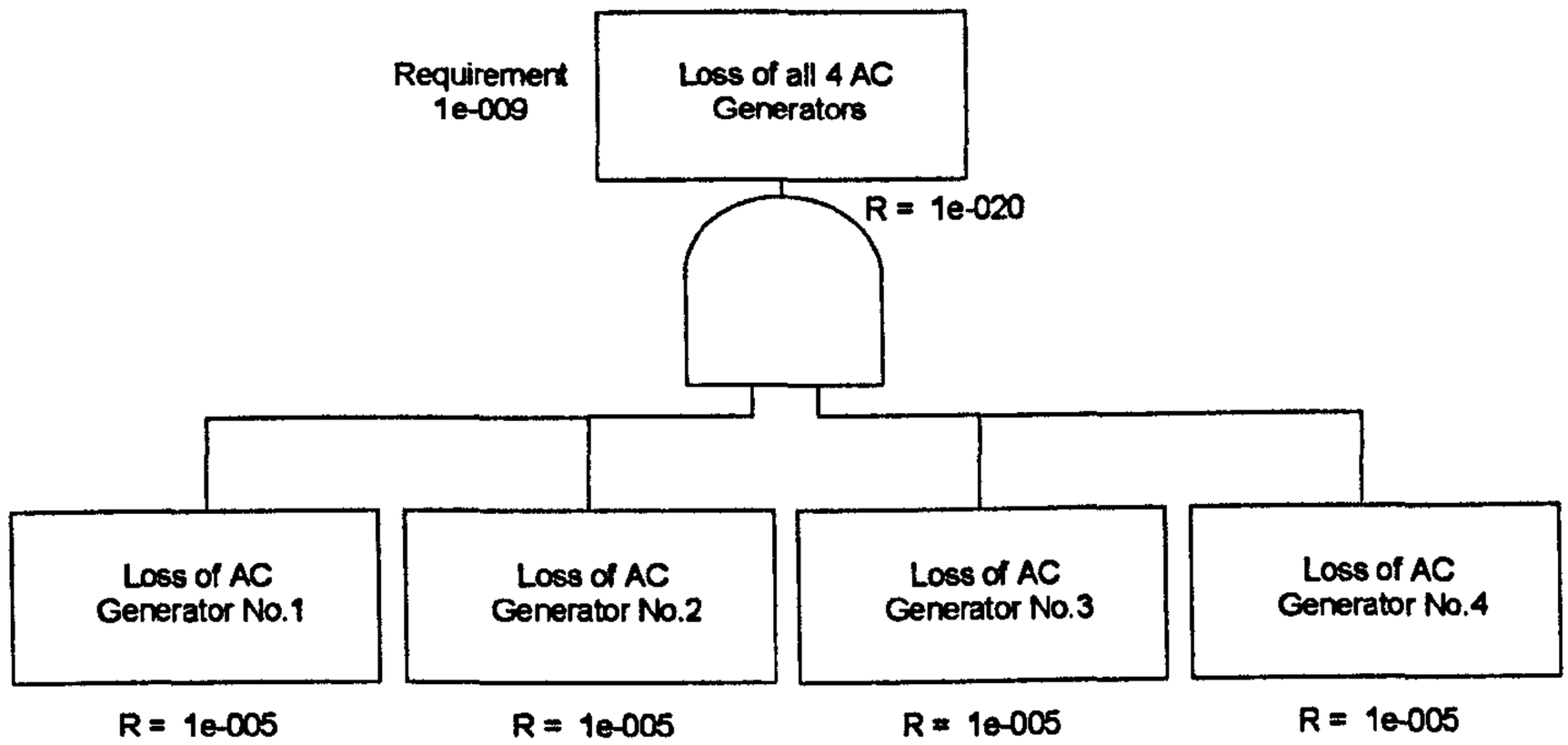


Figure 5 - FTA Analysis Of The Loss Of All Four Generators

It can be seen therefore that, on this basis, the calculated probability (although for simplicity no account is taken here of the exposure time), was approximately 1×10^{-20}, which is well within the compliance requirements.

Now let us look at the two engines, hence two generators, shutdown case. Assuming the remaining two on-line generators still have the same probability of failure as they did when all four engines were running, the fault tree now looks like the one in Figure 6.

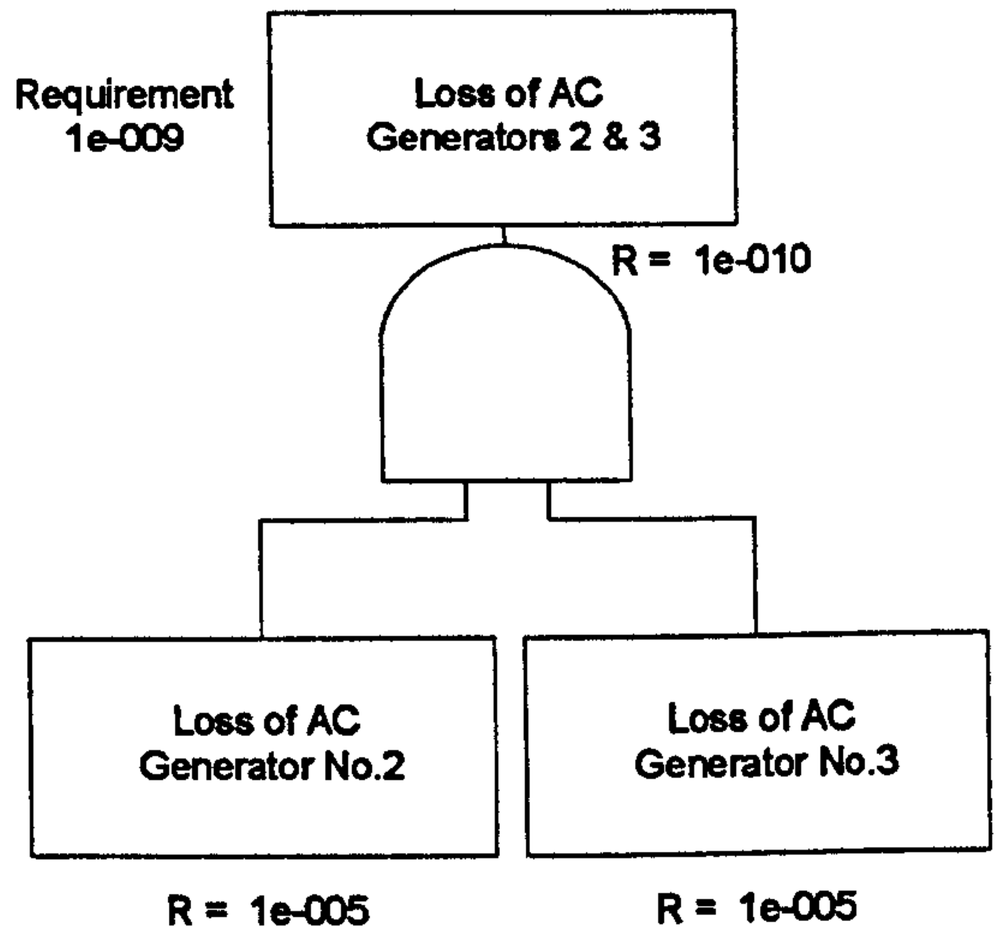


Figure 6 - FTA Analysis Of The Loss Of Two Remaining Generators

This shows that the probability of total generating power loss is still compliant with the FHA requirements at 1×10^{-10}. Now we look again at the same two engines/generators shutdown case, but this time using the alternative two generators, which it should be noticed, have a much higher probability of failure when they are the only two still on-line.

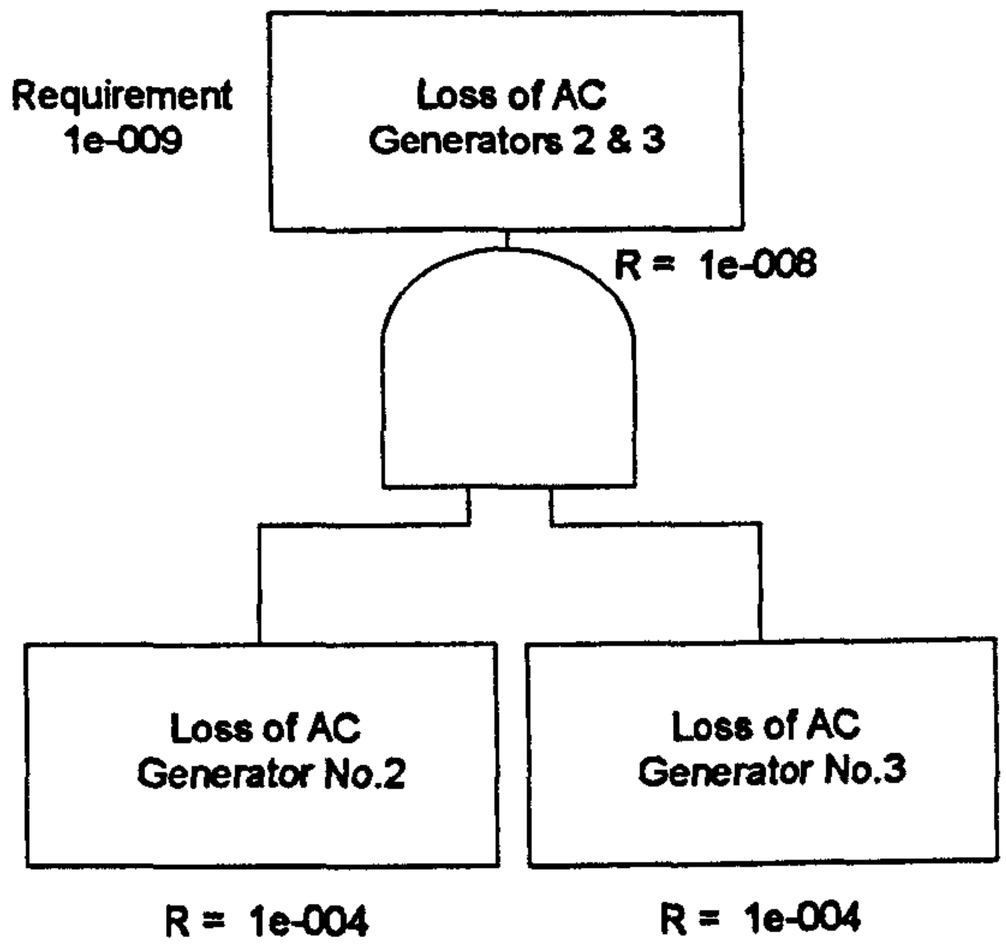


Figure 7 - FTA Analysis Of The Loss Of Two Remaining (Alternative) Generators

In this case, it is evident that the system is no longer compliant with the FHA requirements, since the probability of total system loss is in fact 1 x 10^{-8}, i.e. above the 10^{-9} limit for a catastrophic failure. Challenging the generator manufacturer's original reliability assumptions along these lines has forced a fundamental re-think of strategy, but ultimately, the design process was too far advanced to enable any significant changes to be made.

3.12 ZONAL ANALYSIS

Once all the equipment suppliers have delivered their individual safety cases to the aircraft manufacturer, the latter must conduct a series of analyses of potential system interactions within different sections of the aircraft. This zonal analysis, where major sections of the aircraft are defined to enable assessment of co-located systems, is intended to identify any potential interaction problems, such as routing of independent systems, the possible effect of a failure of one system upon another, the susceptibility of systems and components to damage from an external event, such as a bird-strike, and other similar problems.

The need for zonal analysis was brought into sharp focus by the accident to a United Airlines DC-10 at Sioux City, Iowa some years ago. During the cruise,

the centre engine suffered an uncontained fan failure (actually as a result of maintenance error), but the key point here was that as the failed fan disc exited the engine cowling, it impacted the upper surface of the aircraft's right horizontal stabiliser. This caused major damage to all three of the independent hydraulic systems, since the hydraulic lines were routed adjacent to each other in that zone. As a result, the aircraft lost all flight controls and could only be kept in the air by the use of asymmetric throttling on the remaining two engines. It diverted to Sioux City airport but crashed during a very high-speed landing and killed a significant percentage of those on board. Had zonal analysis been more refined and mandated during the design stage of the DC-10 (which occurred during the early 1970s), it would have been recognised that adjacent routing of the hydraulic lines was not a good idea, and they would have been separated, as Lockheed had in fact done with their competing L-1011 Tristar design.

More recently, an Enhanced Zonal Analysis Procedure (EZAP) has been introduced which brings in more emphasis on wiring systems. This has come about as a result of yet another accident, this time to a Swissair MD-11, which suffered an uncontrollable wiring fire in the area behind the cockpit overhead panel, and subsequently suffered a fatal crash. Developed by an industry team working on behalf of the US Ageing Transport Systems Rulemaking Advisory Committee, EZAP has four stages:

1. For a given aircraft zone, such as the centre section, left wing, tail, etc., the analyst identifies all systems (including wiring systems), structures, components, and any present or possible combustible materials (e.g., fuel vapour, dust particles, contamination)
2. It is determined if the zone contains both wiring and combustible materials
3. If it does, an applicable and effective maintenance task is defined where possible, with an appropriate interval to remove or minimise the build-up of combustible materials in the zone (e.g., a cleaning task to remove dust)
4. An applicable and effective task for inspecting the zone is then defined

For zonal analysis to be effective, it is obviously vital that the analyst has direct access to the aircraft. This allows the determination of what is installed in the zone, access and system interface issues, and other key features such as size and environmental effects. Therein lies the problem with making zonal analysis truly predictive rather than reactive. Effective analysis cannot be completed until the aircraft design, systems layouts, etc., are mature, so if any significant changes are required, they can be extremely difficult, expensive and/or time consuming to affect at a later date.

3.13 RECOMMENDED PRACTICES AND STANDARDS

As mentioned in section 2.7, the guiding documents for safety analysis are SAE standards ARP 4754 and ARP 4761, both originally issued in 1996, as well as Mil-Std-882C, and the FAA System Safety Handbook. Beyond these, it is really left to individual companies to draw up their own safety and reliability analysis procedures, based around the SAE standard structure; no other standard has yet emerged into common use. The military sector has produced a number of guidance documents for industry, which tend to mirror aspects of ARP 4761. These military standards include Mil-Std-882D Department of Defense Standard Practice for System Safety.

3.14 RELIABILITY DATA SOURCES

Information on core reliability data in the form of component failure rates, has historically been available in two universally recognised documents produced by the Reliability Analysis Centre and the Rome Laboratory at Griffiss Air Force Base in the United States and published by the US Department of Defense:

3.14.1 Military Handbook 217 – Reliability Prediction of Electronic Equipment

The Mil-Hdbk-217 handbook contains failure rate models and data for various components used in electronic systems. These include capacitors, connectors, diodes, transistors, relays, switches, etc., and the failure rates listed were based on the best field data that could be obtained at the time of compilation.

Originated in November 1956 as a model for predicting computer failure rates, the first formal issue of Mil-Hdbk-217 was made by the United States Navy in December of the same year. Responsibility for maintaining and updating the document passed to the US Air Force Rome Laboratories in July 1973, and in February 1995 the latest, and as it turned out final issue, Mil-Hdbk-217F Notice 2 was released.

Mil-Hdbk-217 includes the ability to perform a *parts count* analysis or a *part stress* analysis. A parts count analysis provides a simpler reliability figure, and is normally used early in a design when detailed information is not available, or a rough estimate of reliability is all that is required. A part stress analysis takes into account more detailed information regarding the components, and therefore offers a more accurate estimate of failure rate. These functions were included in an early software model made available to industry and known as Milstress.

The basic data was subjected to the testing of various assumptions based on application, operating environment, etc., but the handbook gradually became discredited over time, especially when it was realised just how small some of the component populations analysed were. Indeed Mr Seymour Morris, the point of contact and spokesman for Mil-Hdbk-217 at the Rome Laboratories, has said [33];

"Mil-Hdbk-217 is not intended to predict field reliability and, in general, does not do a very good job at it an absolute sense."

To further illustrate Mil-Hdbk-217's inability to predict component reliability, in 1987 the United States Army conducted a survey [34] of a common design radio that had been supplied by nine different manufacturers, comparing their predicted reliability (all using Mil-Hdbk-217), with their observed reliability in the field.

Manufacturer	MIL-HDBK-217 MTBF	Observed MTBF
1	7247	1160
2	5765	74
3	3500	624
4	2500	2174
5	2500	51
6	2000	1056
7	1600	3612
8	1400	98
9	1000	472

Table 4 - Reliability Assessment *Versus* Reality

The MTBF reliability requirement in the specification was 1,250 hours, with an 80% confidence level. While it should be pointed out that there is likely to be a significant element of human factors events impacting the results, such as mishandling and field damage, nevertheless it is clear that relying on Mil-Hdbk-217 was invalid in this case.

The handbook 217 progressed through a number of revisions and updates until it reached Issue F Notice 2 in February 1995, following which it was withdrawn, due to a lack of funding for further development. Since that time, no replacement has emerged from either the Rome Laboratories or any other official agency. Nevertheless, to this day Mil-Hdbk-217F is still a frequently quoted source of data for electronic parts reliability estimates.

3.14.2 Telcordia

AT&T Bell Labs originally developed the Telcordia reliability prediction model in the 1970s, modifying the equations in Mil-Hdbk-217 to better represent what their equipment was experiencing in the field. The main concepts in Mil-Hdbk-217 and Telcordia are very similar, but Telcordia added the ability to take into account burn-in, field, and laboratory testing. Telcordia also allows the analyst to perform a parts count or part stress analysis, but the model has seen most widespread use outside the aviation industry, mainly in the United States.

3.14.3 Non-Electronic Parts Reliability Database (NPRD)

The NPRD document followed a similar format to Mil-Hdbk-217, and encompassed a very wide range of mechanical and electro-mechanical components, such as actuators, fasteners, springs, valves, etc. Useful though it was for many years as the only generally available tool, it regrettably suffered from the same limitations in the core data that afflicted Hdbk–217, and eventually it was withdrawn from any further update and re-issue following the release of NPRD-95 in 1994. Since the demise of these two US Military documents, a number of others have started to emerge on the scene, some offered as replacements with added functionality. One of the most significant of these is the Bellcore model.

3.14.4 Bellcore

The Bellcore reliability prediction model was developed by AT&T Bell Laboratories in an attempt to better represent their own in-service experience of equipment performance, than had previously been possible with Mil-Hdbk-217. The basic concept was very similar, but Bellcore moved on a stage by taking account of such factors as burn-in and testing and their impact on reliability. This model also included the ability for parts count and parts stress analysis.

3.15 IN-SERVICE RELIABILITY DATA

"In an imperfect world, all hazards may not be identified in this (design analysis) process. Others can and will be identified when the system is exercised through test and operational use. Any occurrence of an accident or incident is (should be) examined critically to determine causes and evaluate effects. The causes and effects could range from something already predicted as possible or even probable under certain conditions, to something entirely new and surprising." [35]

The obvious alternative to using either Mil-Hdbk-217 or NPRD as a source of reliability information is empirical data from actual in-service events. Taken at face value, this would seem to be the most logical and potentially, the most

accurate data source not least because it automatically takes account of changing situations. Not least in this regard are the effects on reliability levels as an aircraft and its systems age.

There are a great many aircraft still in service beyond the 15 year-since-delivery Flight International definition of an ageing aircraft. This situation is not expected to fundamentally change in the medium term at least, so it is perhaps among the most critical factors affecting reliability that need to be understood. However, the whole approach to the gathering and use of empirical data is fraught with difficulty and is discussed in more detail in section 3.19.

3.16 COMMERCIAL SOFTWARE TOOLS

In recent times, the market has seen a proliferation of commercially available software, aimed at simplifying the analysis procedure. This proliferation, while expected, can lead to confusion amongst analysts who may be uncertain about the relative merits of each package. No generally available advice to guide the analyst has been identified.

<table>
<tr><th>Concept Development

Aircraft functions, architectures, requirements</th><th>Preliminary Design

System functions, architectures, requirements</th><th>Detailed Design

Detailed functions, architectures, requirements</th><th>Design Validation & Verification
Tests
Analyses</th></tr>
<tr><td rowspan="2">Aircraft FHA
- Functions
- Hazards
- Effects
- Classifications</td><td>System FHA
- Functions
- Hazards
- Effects
- Classifications</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>PSSAs</td></tr>
<tr><td>Aircraft FTAs

- Qualitative
- Subsystem budgets
- Intersystem dependencies</td><td>System FTAs

- Qualitative
- Subsystem budgets</td><td>System FMEA</td><td>System FTAs

- Quantitative
- Failure rates</td></tr>
<tr><td colspan="3">CCAs</td></tr>
<tr><td>Particular risk analysis</td><td>Common mode analysis</td><td colspan="2">Zonal safety analysis</td></tr>
</table>

Table 5 - The Safety Analysis Process *(ARP4761)*

An alternative version is offered by N Leveson et al in their paper *Demonstration Of A Safety Analysis On A Complex System.* Here it can be seen that more detailed consideration is now being given to, for example, the effects of in-service use on reliability and safety levels. This model is embedded in their *Safeware* analysis system, primarily intended for use in air traffic management, but easily adaptable to any other complex system.

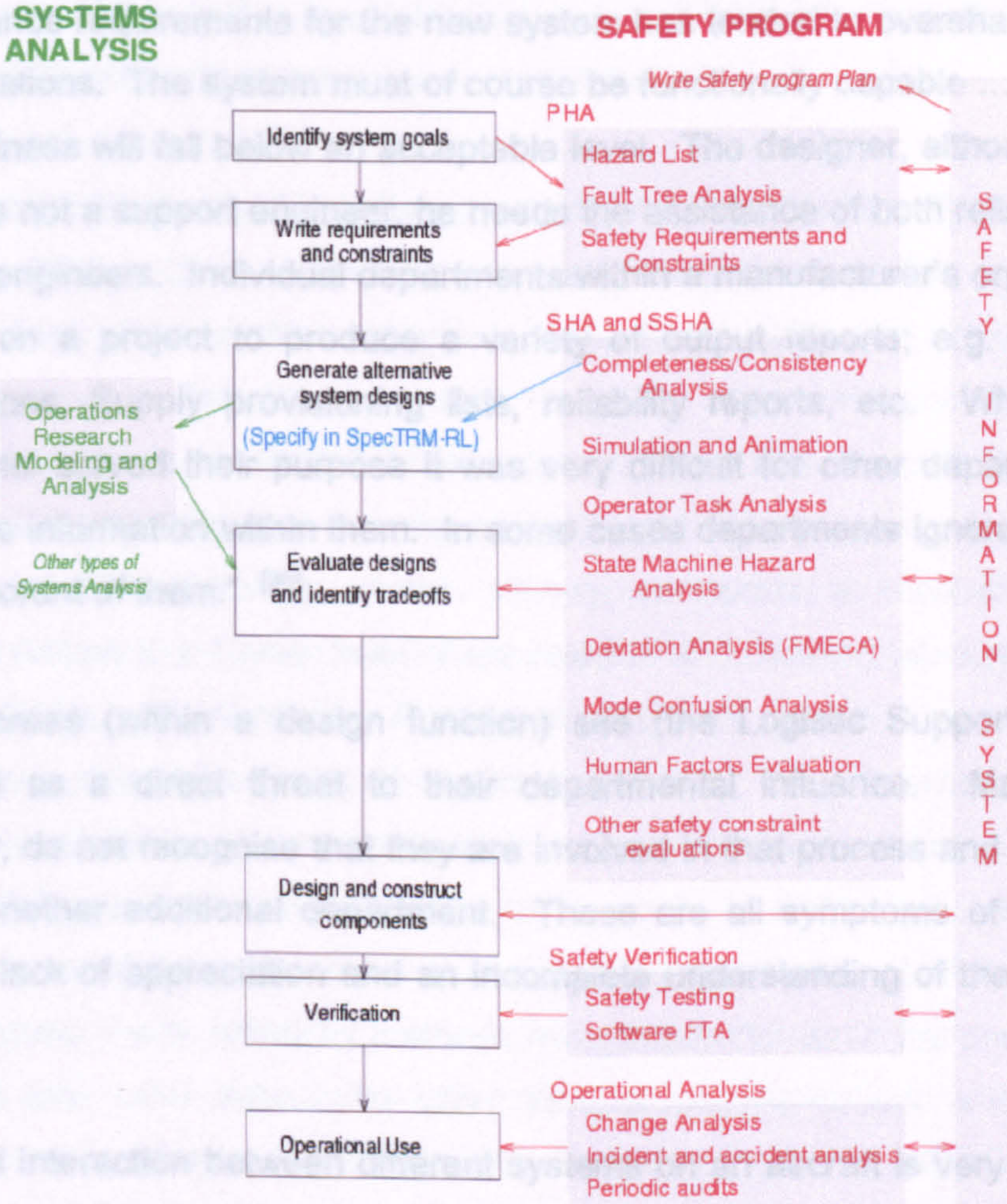


Table 6 – The *Safeware* Safety Analysis Process

3.17 RECOGNISING THE NEED FOR CHANGE

The failings of the FHA system have their roots in a lack of accurate data sources leading to imprecise reliability assessment, the freedom to apply "fiddle factors" to meet the specification and to use reliability figures for equipment running at whatever output the manufacturer chooses, i.e. not necessarily the

"worst case" scenario. Although ARP 4761 recommends independent checking of safety analysis away from the design team, this is not mandatory and therefore is seldom done.

"There are numerous examples where products which appear to satisfy the original functional requirements as intended, fail to do so. The desire to achieve performance requirements for the new system has tended to overshadow other considerations. The system must of course be functionally capable ... if it is not the readiness will fall below an acceptable level. The designer, although highly skilled, is not a support engineer, he needs the assistance of both reliability and support engineers. Individual departments within a manufacturer's organisation worked on a project to produce a variety of output reports; e.g. Technical Publications, Supply provisioning lists, reliability reports, etc. Whilst these documents served their purpose it was very difficult for other departments to utilise the information within them. In some cases departments ignored them or were ignorant of them." [36]

"Some areas (within a design function) see (the Logistic Support Analysis process) as a direct threat to their departmental influence. Many areas however, do not recognise that they are involved in that process and feel that it is just another additional department. These are all symptoms of the same thing, a lack of appreciation and an incomplete understanding of the process." [37]

Potential interaction between different systems on an aircraft is very difficult to do in any case, not least because of the need for a systems integrator who can give his suppliers the earliest possible view of the results of preliminary zonal analysis and other allied processes. Measures of equipment reliability performance during test, development and in-service are variable and frequently inaccurate or even missing altogether, and even when they are present, there tends to be a failure to recognise or understand the limitations of the analysis. Many elements that can impact on system performance are frequently overlooked, such as software reliability, the effect of flight cycles, the operating environment, etc.

Finally and most significantly, it is still common for ILS/reliability/safety analysis to be regarded as a "necessary evil" – a "tick in the box" which can be done retrospectively once the design and testing activity is complete. Resource pressures and a national shortage of experienced ILS/reliability/safety engineers, lead to this attitude becoming more and more prevalent.

In the words of the SAE in their introductory material for the planned *JA1000/1A Reliability Program Standard Implementation Guide:*

"The importance of reliability in design engineering has significantly grown since the early Sixties. Competition has been a primary driver in this growth. The three realities of competition today are: world class quality and reliability, cost-effectiveness, and fast time-to-market. Formerly, companies could effectively compete if they could achieve at least two of these features in their products and product development processes, often at the expense of the third. However, customers today, whether military, aerospace, or commercial, have been sensitized to a higher level of expectation and demand products that are highly reliable, yet affordable. Product development practices are shifting in response to this higher level of expectation. Today, there is seldom time, or necessary resources to extensively test, analyze, and fix to achieve high quality and reliability. It is also true that the rapid growth in technology prevents the accumulation of historical data on the field performance of their products. Unfortunately, some reliability methods have depended upon the availability of historical data, other experiential information, or learning through extensive and time consuming tests. To enable this transition, reliability efforts must be directed toward anticipating problems and designing-in features that assure the achievement of quality and reliability, concurrent with the development process, instead of trying to assess quality and reliability downstream. The gains in time-to-market and cost savings from such an approach can be significant."

"More recent reliability programs tend not to prescribe reliability tasks or methods to be performed by suppliers. Rather, suppliers are considered equal partners in the effort to produce a reliable product and work with the companies in deciding which reliability methods provide most value in achieving objectives. Furthermore, it is not unusual for several design iterations of technologically

different hardware and software to be developed before the final version is incorporated into the production product. Also, the reliability discipline is generally a separate activity from the design discipline in some sectors of the industry."

This same view then spills over into the in-service phase, where minimal monitoring of performance is carried out to check the validity of the analyses that lead to certification. Relying on meeting MTBF targets is the norm, but it is only half the story. MTBF is a measure of a constant failure rate, and its' limitations could be disguised by relying on "reliability growth" in the early years in service. Furthermore, Mean Time Between Unscheduled Removal (MTBUR) is potentially just as important in safety terms, but major aircraft manufacturers do not agree on its' definition.

"Stuff happens. Usage and deployment changes occur – item characteristics are different - reliability predictions versus observed demand rates. Missions change and budget problems constrain usage." [38]

Unfortunately, the certification process allows much of this in many regards. As an example, it is quite permissible for a manufacturer to state how he has derived failure rates by simply stating that he has used standard reliability databases, or the test and in-service data; supporting evidence does not have to be included in the safety case, and is only ever requested by the authorities in the event of an unreasonably low failure rate being claimed.

"The traditional reliability programme approach [39]:

- Customer specifies how reliability will be achieved
- Imposes a sequential product development methodology
- Supplier includes all tasks, relevant or not
- Programme is not product specific
- Imposes a rigid programme, stifling innovation"

3.18 RELIABILITY DATA AVAILABILITY

To help illustrate the difficulties, let us look in more detail at how the Bellcore reliability data model compares with the long-established, but no longer maintained, Mil-Hdbk-217F. The specific requirements of a particular reliability prediction analysis may mean that one model is more applicable than the other. There are many differences between the two models, each of which is briefly described below.

3.18.1 International Recognition and Acceptance

Use of the Bellcore model is still more common in the United States than elsewhere. Although it is slowly growing in popularity internationally, it continues to come up against the general perception, that Mil-Hdbk-217F remains the industry standard tool for reliability prediction analyses.

"Mil-Hdbk-217 is discredited. It only looks at individual components, which only account for 5% of failures. It ignores assembly joints and so on, which account for 95% of failures." [40]

3.18.2 Components Considered

AT&T Bell developed the Bellcore model primarily for commercial equipment, and naturally concentrated on their core business telecommunications equipment. On the other hand Mil-Hdbk-217F had a far broader scope, being geared towards both the military and commercial markets across a wider range of equipment types, and without any specific market focus.

3.18.3 Calculation Methodologies

The basic methodologies of the Bellcore and Mil-Hdbk-217F models are very similar. Nevertheless, when comparing them more closely, it quickly becomes apparent that the Bellcore calculations tend to be more optimistic. In general Bellcore calculations also require fewer part parameters for components.

Hence the calculations performed by Mil-Hdbk-217F are frequently more pessimistic, and generally require more component parameters to achieve an acceptable degree of calculation accuracy.

This does not mean that Bellcore failure rates will always be more accurate, but it does indicate that depending on the components being analysed, it is likely that there will be significant differences in the predicted failure rates produced by the two methods.

3.18.4 Consideration of Test Data

Unlike Mil-Hdbk-217F, the Bellcore model includes the capability of considering component burn-in, laboratory test, and field service data in its calculations. This provides a greater degree of confidence in its predictions, since they tend to be based on historical data, rather than the basic stress methodology used by MIL-HDBK-217F. The burn-in data is also used to quantify expected failure rates in the first year to provide an indication of so-called "infant mortality", i.e. a higher failure rate than can be expected during the "steady state" expected throughout the bulk of the in-service life. However, this shortfall on the part of Mil-Hdbk-217F has been partly addressed by some commercial software packages, which now have the ability to use these additional calculation methods in either model.

3.18.5 *Multiplier*

The Bellcore model calculates failure rates to a value expressed as failures per billion hours, instead of Mil-Hdbk-217's more usual failures per million hours, so this has the potential to be a source of unintentional error in reliability calculations.

3.18.6 Part Types

Each model supports part types that the other does not. For example, Bellcore contains data on batteries, coolers, computer systems, gyroscopes and heaters, none of which are contained within Mil-Hdbk-217. On the other hand, Mil-

Hdbk-217 has data on lasers, printed circuit boards, tubes, etc., which are not in Bellcore. This can result in a tricky situation whereby an analyst may need to refer to both models, with all the inherent difficulties in coping with differing failure rate calculation methodologies, as already mentioned.

3.18.7 Environments

Initially Bellcore only supported three different ground based environments, as it was originally designed for use only by the telecommunications industry. This shortfall has recently started to be addressed by later iterations of the model, which have additional operating environments including Airborne, Commercial and Space. Mil-Hdbk-217 has always offered a variety of different operating environments in air, ground, sea and space, but none of these commercial models offers a range of environmental options that satisfactorily encompass the main air transport operating scenarios.

3.18.8 Quality Levels

Bellcore currently supports four standard quality levels, which are identical for all component types, and are based on generalities concerning the origin and screening of the components. The Mil-Hdbk-217 approach is to use component-dependent quality levels, i.e. levels that differ from one part type to another, rather than having a simple general classification of quality levels.

3.19 THE USE OF EMPIRICAL DATA

Much is written of empirical data and how essential it is in understanding equipment performance, but gathering it and using it effectively is not as easy as it might at first seem. In recent years there have been a great many attempts to establish "industry benchmark" data collection tools, most notably the British Airways BASIS system, but to date none has satisfactorily addressed all the requirements in terms of primary failure cause analysis and feedback to the people who need the information.

3.20 WHAT DATA DO WE MEAN?

As has already been mentioned briefly, it is becoming more common for industry to claim the use of "empirical data" when establishing reliability figures and failure rates for their equipment. This would appear to be the most sensible approach, since it uses data most closely allied to the equipment under analysis rather than relying on a standard reference work which by its very nature makes generalisations. However, there are many pitfalls awaiting the unwary when using such data, and it is absolutely essential for the analyst to precisely understand the data he is coming across.

Let us first consider what is meant by empirical data. The literal meaning is relying on or derived from observation or experiment, or guided by practical experience and not theory. Therein lies the first problem. Too many systems of empirical data retrieval simply gather information from in-service events at operator level, and then not always from every operator. The potentially large amount of valuable data that can come from in-house equipment testing and from the repair and overhaul loop, is all too often either overlooked or is simply not available in a useable form. What do SSPP requirements have to say about empirical data? In Mil-Std-882C, under section 102.2.6 System Safety Data, it is stated that the SSPP shall:

i. "Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned, data
ii. Identify deliverable data by title and number, and means of delivery (e.g. hard copy, electronically, etc.)
iii. Identify non-deliverable system safety data and describe the procedures for accessibility and retention of data of historical value."

Thus a standard does exist for the capturing of in-service data, but there are two major problems with it. Firstly, the programme may be one in which Mil-Std-882C is not specified, and secondly, the requirements as listed above are

far too vague and open to creative interpretation to suit the manufacturer's needs rather than those of the safety of the system.

3.21 PROCESS SUMMARY

The safety assessment process is now very well defined, particular within such references documents as ARP 4761. The basic analytical tools including FHA, FMEA, FMECA, FTA, etc., are well defined and universally understood. Other interfacing procedures are also generally acceptable, and there is a number of on-going industry initiatives aimed at focusing more attention in this area. However, the problem remains the lack of legislation to back them up and require their use. This is now also noticeable in the efforts to establish event-reporting systems to back-up the design analysis.

The problem of over-reliance by design teams and analysts on out-dated or otherwise inappropriate component reliability data lies at the core of many system safety prediction problems. The use of empirical data offers a far more satisfactory approach to reliability assessment, but as yet the availability of the necessary core in-service data to support such a system is still in its infancy.

It is to be hoped that the emergence of agencies such as EASA will help to enforce a wider adoption of the right procedures through legislation. However, in many areas legislation on its own will not work, since the right tools and the back-up support infrastructure are not necessarily all in place.

3.22 HOW IT IS GOING WRONG

Let us summarise what we have outlined so far. A failure to understand the part correct analysis has to play can lead to over-engineered / over-complex systems, ineffective built-in test capability, unexpected operational effects in service and safety margins being reduced unseen (i.e. the dormant failure case mentioned earlier, or a "smart" system re-configuration without an appropriate indication to the flight crew). At best this potentially leads on to expensive and time-consuming equipment re-design or modification, equipment life constraints, extra unscheduled maintenance costs, schedule delays and so on, with an inevitable loss of confidence and raising of costs.

3.23 THE MANUFACTURERS' PROBLEMS

As an example of what can happen, let us take a look at the Airbus A330 and A340 fleets. They are fitted with a common auxiliary electrical power generation system, which suffered a major fall-off in reliability for the very reasons stated above. As a result, the engineering investigation to find the problem, identify the fix and test it, took well over a year. The modified equipment then had to be put into production and embodied across the in-service aircraft fleet, a process which it was predicted, would take a further two years to complete. During all this time, the operators were therefore suffering high unit removal rates, increased maintenance costs and the need for additional spares provisioning, all of which were eroding their already marginal profitability.

Other issues include material or supplier selection, such as financial pressure for the retention of unsatisfactory components, e.g. Kapton wiring. The trade-off of weight / cost / performance / reliability impacts on safety margins – but to what degree is not always clearly understood. Such trade-offs during the design stage generally come under three headings:

- Safety / availability – a balancing act which attempts to ensure the optimum mix of system complexity, redundancy, maintainability and so on, while still achieving acceptable levels of reliability so as to satisfy both the FHA and ultimately the operator
- Safety / cost – here it is a simple economic balance between achieving an acceptable level of failure risk while doing so at minimal cost in terms of both design, test and production effort and system purchase price
- Safety / complexity – closely allied to safety / availability, but also encompassing additional considerations such as maintainability, testability, repairability, weight, and again bringing in cost, development time ("time to market"), etc.

Data errors include a lack of feedback from development and qualification test; in other words, the analysis is rarely re-run. When in-service data is collected, the percentage of the fleet reporting is not always considered, leading to data

distortion. Even at the initial prediction stage, the withdrawal of support for standard reliability data sources such as Mil-HDBK-217F and NPRD95 means that their value, which was always questionable, diminishes even further with time, even though they continue to be heavily utilised. The main problem with MIL-HDBK-217F in particular, was the fact that it looked at relatively small (sometimes very small) populations of individual components, which only accounted for around 5% of the total equipment failures. It ignored the 95% from such areas as assembly joints and so on, and a comparison of MIL-HDBK-217F predictions against actual MTBFs has led to it being generally discredited by reliability specialists. The concept of in-house reliability databases based on empirical data remains in its infancy. A failure to notice problems, to listen to the equipment maintainers, to seek feedback from operators or to learn the lessons of history is rife.

Thus the main areas within the safety analysis cycle that can / do lead to error are as follows:

REQUEST FOR INFORMATION (RFI) STAGE

- Design is extremely immature
- "Guestimates" of reliability levels, based on and frequently over-ruled by, commercial department pressures to win the business

REQUEST FOR QUOTATION (RFQ)

- Preliminary reliability and safety performance estimates still based on immature design
- Use of outdated data sources such as MIL-HDBK-217F, or on expectations from company's experience with other products
- Some consideration of in-service performance of similar equipments, but if the message is not what the commercial people want to hear they may well manipulate the figures after the reliability department has produced them

REQUEST FOR PROPOSAL (RFP)

- Reliability and safety performance guarantees required
- Calculations based on what the customer was told at the RFQ stage and preliminary top-level FMEA rather than a scientific analytical approach.

DEVELOPMENT & TEST

- Development of FHA, FMEA, FMECA, FTA, zonal analysis, CCA, PSSA
- Feedback to design is patchy and messages may be ignored if they are unpalatable or are in the lower number range of the risk analysis
- FMEA and reliability figures are either:
    - Developed by designers without independent checks
    - Developed by ILS / safety analysts / reliability departments without reference back to design
    - Developed by ILS / safety analysts / reliability departments and referred back to design for review, which is frequently extended or overlooked because they are too busy
- Feedback to analysis from test may be patchy or even non-existent.

CERTIFICATION

- Safety Case produced for the certification authorities is rarely subjected to independent checks
- May have been reviewed internally because company procedures require two or more signatures on it, but this process is likely to have involved little more than a token glance at the summary
- Review by the aircraft manufacturer and the authorities will largely be based on trust that the analyst has got it right, and may only question reliability figures that appear to be particularly optimistic. Even then, a justification statement is probably all that will be required.

ENTRY INTO SERVICE

- The Safety Case is now gathering dust on the shelf, with no attempt to revisit it in the light of actual in-service performance to confirm that FHA compliance claims are being met.

3.24 THE FEDERAL AVIATION ADMINISTRATION (FAA) VIEW

It is time for some fundamental changes, and this view is supported by a report issued by the FAA Associate Administrator for Regulation and Certification. Commissioned a year earlier, the *Commercial Airplane Certification Process Study* [41] is subtitled "an evaluation of selected aircraft certification, operations and maintenance processes."

The team that produced the report was led by the FAA, co-chaired by the aviation industry and included other experts from NASA the Department of Defense as well as non-US manufacturers and airworthiness consultants. Their remit was to perform a comprehensive review of the processes and procedures associated with aircraft certification, operations and maintenance, taking as a starting point, the original type certification activities, and then continuing through operational safety and airworthiness procedures. Of particular interest were the content and effectiveness of information paths between certification, operations and maintenance activities, one of the over-riding concerns already examined here.

At the conclusion of their work, the team listed a total of fifteen findings and two observations. They are repeated here in their entirety, with those primary areas of concern already discussed in earlier chapters of this study, highlighted in bold text.

The first four findings were placed under the Airplane Safety Assurance Process heading:

1. *Human factors issues in design, operations and maintenance*. Human performance is still the dominant factor in accidents. The processes

used to determine and validate human responses to failure and methods to include human responses need to be improved. **Design techniques, safety assessments, and regulations do not adequately address the subject of human error in design or in operations and maintenance.**

2. *Correlation of safety assumptions with operations and maintenance practices.* **There is no reliable process to ensure that assumptions made in the safety assessments are valid with respect to operations and maintenance activities**, and that operators are aware of these assumptions when developing their operations and maintenance procedures. In addition, **certification standards may not reflect the actual operating environment.**
3. *Robust safety assessments and design for critical functions.* **A more robust approach to design and a process which challenges the assumptions made in the safety analysis of flight critical functions is necessary in situations where a few failures (2 or 3) could result in a catastrophic event.**
4. *Flight critical systems and structure.* **Processes for identification of safety critical features of the aircraft do not ensure that future alterations, maintenance, repairs, or changes to operational procedures can be made with cognizance of those safety features.**

The next three findings were placed under the Aviation Safety Data Management heading:

5. *Co-ordination of data management systems.* Multiple FAA-sponsored data collection and analysis programmes exist without adequate inter-departmental co-ordination or executive oversight.
6. *Data definition and reporting requirements.* **Basic data definition and reporting requirements are poorly defined relative to the needs of analysis and other uses.**
7. *Identification of accident precursors.* **There is no widely accepted process for analysing service data or events to identify potential accident precursors.**

The next four findings were placed under the *maintenance/operations/certification interfaces* heading:

8. *Capturing the lessons learned from design, manufacturing, maintenance, and operating experience.* **Adequate processes do not exist within the FAA or in most segments of the commercial aviation industry to ensure that the lessons learned from specific experiences in aircraft design, manufacturing, maintenance, and flight operations are captured permanently and made readily available to the aviation industry. The failure to capture and disseminate lessons learned has allowed aircraft accidents to occur for causes similar to those of past accidents.**
9. *Constraints on the sharing of information.* There are constraints present in the aviation industry that have an inhibiting effect on the complete sharing of safety information.
10. *Maintenance and operational safety recommendations and feedback between operators and Original Equipment Manufacturers (OEMs).* There are currently no industry processes or guidance materials available which ensure that; safety related maintenance or operational recommendations developed by the OEM are evaluated by the operator for incorporation into their maintenance or operational programmes, and safety related maintenance or operational procedures developed or modified by the operator are co-ordinated with the OEM to ensure that they do not compromise the type design safety standards of the aircraft and its systems.
11. *Communication and co-ordination between Airplane Certification Service and Flight Standards Service.* The absence of adequate formal business processes between FAA Airplane Certification Service and Flight Standards Service limits effective communications and co-ordination between the two that often results in inadequate communications with the commercial aviation industry.

The next two findings plus one observation were placed under the major repairs and modifications heading:

12. *Classification of repairs and alterations*. The airline industry and aircraft repair organisations do not have a standardised process for classifying repairs or alterations to commercial aircraft as "Major" as prescribed by applicable Federal Aviations Regulations (FARs).
13. *Quality of alterations and repair processes.* **Inconsistencies exist between the safety assessments conducted for the Initial Type Certificate of an aircraft and some of those conducted for subsequent alterations to the aircraft or systems**. Improved FAA and industry oversight of repair and alteration activity is needed to ensure that safety has not been compromised by subsequent repairs and alterations.

Observation 1. *Airworthiness Directive/Service Bulletin information flow to field reference materials.* OEM and operators maintenance manuals, Illustrated Parts Catalogues (IPCs), wiring diagrams, and other documents needed to maintain aircraft in an airworthy condition after incorporation of Service Bulletins (SBs) and Airworthiness Directives (ADs), are not always revised to reflect each aircraft's approved configuration at the time the modifications were implemented.

The final two findings plus one observation were placed under the safety oversight process heading:

14. *People and process for oversight of Designated Engineering Representatives (DERs)*. Consultant DERs have approved designs that were deficient or non-compliant with FAA regulations.
15. *Detection of single point human error.* **Processes to detect and correct errors made by individuals in the design, certification, installation, repair, alteration, and operation of transport aircraft are inconsistent allowing unacceptable errors in critical airworthiness areas.**

Observation 2. *Oversight processes and resources: industry.* Some air carriers do more extensive oversight than others of their in-house and

outsourced flight operations and maintenance activities, with major safety and economic benefits.

A very comprehensive and alarming list of findings, which clearly demonstrates the depth of concern now starting to emerge in at least one of the World's primary certification authorities with regard to overall deficiencies with the current aircraft system safety process. Disappointingly however, the report stops short of making any concrete proposals for change to address these issues which, given the serious nature of the identified shortcomings is hard to understand.

What the report does discuss, albeit extremely briefly, is the need to achieve a change of culture across the industry. It recognises that regulation alone cannot achieve the desired results, and that is of course quite true, but expecting such a large and varied industry to adopt "inter-organisational" cultural changes to facilitate a more open exchange of information" is going to take more than gentle persuasion. The report recognises that the manufacturers, operators and FAA should work together towards achieving co-ordination of initiatives, but what about maintenance organisations, all the manufacturer's system and component suppliers, ground handlers, etc.?

3.25 THE ETOPS & LROPS DEBATE

Let us take a look at one major area of dissention amongst the industry today, extended operations, or ETOPS. The present ETOPS regulations began in the 1980s with new rules governing the design and operation of twin-engined aircraft on long-range routes, and considering the possibility of an engine failure. It stated that there must be a suitable diversion airport within a certain flying time at the one-engine out speed. Today, most Airbus and Boeing wide-bodied Airbus twins are type-certificated to 180 minutes single-engine flying time from a suitable airport, while many narrow-bodies also have certification to 120 minutes.

There are strict rules regarding the modification status and life consumed of on-board equipment for ETOPS missions, and this is reflected in differing Minimum

Equipments Lists (MEL) and in tighter regulations on maintenance activity. Current moves are now pushing ETOPS to 207 minutes, or even 240 minutes, and here the two major manufacturers have a difference of opinion. Airbus believes that the policy of extending ETOPS maximum diversion times to 207 minutes for specified airlines for North Pacific operations is inappropriate until such time as international agreement is reached on applicable standards.

They are concerned [42] because:

"A typical application of the 207-minute authority will be in winter, when ETOPS tracks will take twin-engined aircraft to the north of the Pacific region, in the vicinity of the most remote airfields, where any diversion would probably occur in bad weather conditions and where ground facilities are minimal. In granting the 207-minute authority, the U.S. Federal Aviation Administration has presented no explanation of how safety would be maintained."

"Airbus believes that ETOPS should be formalised in regulations rather than administered through ad hoc policy letters and advisory circulars. ETOPS regulations should be driven by safety and a public review is necessary of the risk management models used. ETOPS rules should be harmonised with international rules, rather than imposed by only the FAA for a select group of airlines. Airbus supports the creation of an industry and government working group to review 207-minute operations."

Furthermore, Long-Range Operations (LROPS) is a newly proposed regulatory concept which addresses all aircraft, irrespective of the number of engines.

"Airbus would like LROPS to embrace flight length, diversion times, and airport weather and equipment. The rules criteria should cover systems design, maintenance and operations practice. Airbus would like to see diversion airfields re-categorised as extreme, demanding and benign, depending upon their integrity."

Note here the emphasis Airbus places on the need for "rules criteria" on system design.

More recently, Boeing and the FAA have been pushing to permit twins to operate under the same rules as three and four-engined aircraft which currently have no limitations on diversion times in the one-engine-out case, due to the obviously higher level of system redundancy. The case they make is that engine reliability is now at such a high level that such restrictions are no longer justified.

3.26 DOES THE INDUSTRY HAVE TOO MUCH FAITH IN RELIABILITY?

The ETOPS / LROPS debate is highly indicative of the way in which much of the industry appears to be developing an over-confidence in the reliability performance of their aircraft systems. What should have been a wake-up call occurred in April 2003, when a United Airlines Boeing 777 on a trans-Pacific flight suffered an engine failure, resulting in an ETOPS diversion reportedly in excess of the 207 minutes currently certificated.

There can be little doubt that, worthy though it is, the current emphasis on improving air safety performance solely by addressing human factors issues on the flight-deck, means ignoring a very significant level of risk inherent in the way we currently design, analyse and maintain our aircraft systems.

3.27 ACCIDENTS AND INCIDENTS

Two main areas of investigation were used to look for evidence of flawed or incomplete safety analysis. Firstly, a study was conducted of all known commercial aircraft major accidents and incidents over the period 2001 to 2005. From this data, an analysis of root causes was carried out, placing particular emphasis on those which had design, reliability, system safety and / or human factors contributors.

Secondly, a number of more detailed case studies were carried out where there was sufficient data available to do so. The results of both these investigations are presented and discussed in section 3.29.

3.28 VARIANCES IN RELIABILITY

The stringent equipment performance and reliability requirements already mentioned as being specified to the aerospace industry by aircraft manufacturers, manifest themselves in a number of key areas. For example, dispatch reliability guarantees for civil systems which five years ago were specified at the 97% level, are now being routinely demanded for new applications at better than 99%. Similarly, the demands of such initiatives as ETOPS certification, places significant demands on system configuration and design, which results in extremely complex analyses of reliability and safety requirements.

The problem is that both aircraft and aircraft system reliability experience in service may fail to meet the analytical expectations of the design stage, intended to support these requirements. For example, an Auxiliary Power Unit (APU) generator was introduced into service in a large passenger aircraft in the 1990s, with a Mean Time Between Failures (MTBF) of 15,000 operating hours being guaranteed by the manufacturer.

Analysis showed that after an apparent very high level of reliability in the early service life, some two years after introduction, levels of both MTBF (and Mean Time Between Unscheduled Removal (MTBUR)), fell away dramatically to levels below that which had been guaranteed. Investigation of units returned for repair revealed a number of failure modes, some of which were occurring far more frequently than originally predicted, while others had not been expected to cause unit failure at all. Extensive – and expensive – modification, testing and fleet embodiment programmes over an extended period of time were required in order to bring reliability levels back up to the required level.

Cases such as this can result in the safety levels required for certification being compromised, quite possibly without anyone realising it until something goes wrong. Examples of this could be either a consistent failure to meet dispatch requirements, or more importantly from a safety standpoint, a significant system loss in flight due perhaps to the unrecognised occurrence of a dormant failure, followed by a second failure which creates a problem for the flight crew.

Certainly lower reliability will inevitably lead to higher direct operating costs for the operator. As an example of this, a modern aircraft Integrated Drive Generator (IDG) has a predicted reliability expressed as an MTBF of 15,000 flight hours. Statistically, this equates to 66.6 removals per million flying hours, which is obviously 67 in practice. Assuming the aircraft flies an average of 4,000 hours a year, this means that each such aircraft (fitted with four generators) in an operator's fleet could expect one unscheduled generator removal per year. A 10% error in the initial reliability prediction for the generator, resulting in a true MTBF of 13,500 hours, would mean that an operator with a fleet of 45 of these aircraft would suffer an increase in annual fleet generator removals from 45 to 53. The average repair cost for an IDG is typically around $60,000; thus the prediction error could be costing the operator an extra $480,000 annually – and this is for just one item of equipment on one aircraft type in their fleet.

Such an error in analysis, albeit by a relatively modest 10%, could also result in the safety requirements for the loss, in this case, of electrical power no longer being achievable.

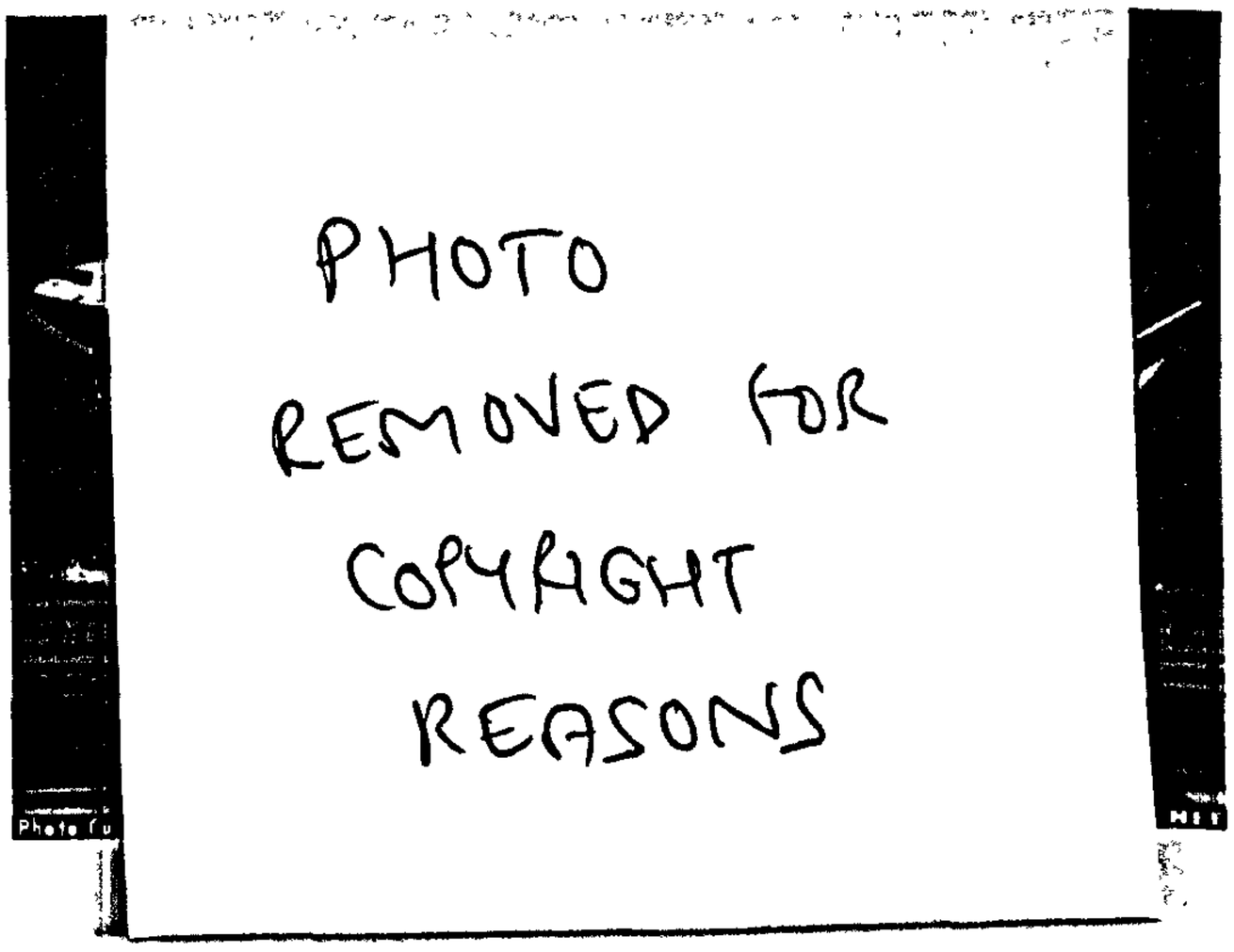
3.29 CASE STUDIES

A number of case studies were analysed in depth to further illustrate this issue of reliability and safety, as follows.

3.29.1 Lauda Air Boeing 767 - Inadvertent in-flight thrust-reverser actuation

On 26 May 1991 a Boeing 767 aircraft operated by Lauda Air, took-off from Bangkok airport en route to Vienna. Fifteen minutes later the aircraft crashed in mountainous terrain with the loss of all on board.

The primary cause of the accident [43] was the uncommanded deployment of the thrust reverser on the left-hand engine, leading to uncontrollable aircraft maneuvers followed by a high-speed descent and structural break-up.



Although the root cause of the thrust reverser deployment was never established, the system was subjected to a detailed analysis of possible failure modes. The accident report prepared by the Aircraft Accident Investigation Committee of the Ministry of Transport and Communications in Thailand states that "this revealed electrical short failure modes in the Directional Control Valve (DCV) that could cause an uncommanded reverser deployment following an opening of the hydraulic isolation valve. Boeing could not provide test data or analysis to determine the extent of thrust reverser movement in response to a momentary hot-short with a voltage greater than 8.2 Vdc, or the ability of the thrust reverser to return to the stowed position after tripping of the circuit breaker associated with the source of the hot-short."

"Other potential hydraulic system failures...were tested. The tests disclosed that uncommanded deployment of the thrust reverser was possible with blockage of the solenoid valve return passage...or total blockage in the return line. The result of this testing indicates that this detail may have been overlooked in the original failure mode and effects analysis."

As a result, the National Transportation Safety Board (NTSB) recommended that the FAA "conduct a safety review of the...Boeing 767 aircraft thrust reverser systems to evaluate electrical and mechanical anomalies and failure modes... The certification review should also determine the adequacy of the thrust reverser system safeguards...to prevent uncommanded thrust reverser extensions."

This clearly raises questions over the ability of Boeing's in-house reliability analysis system to identify some of these anomalies during the design stage.

3.29.2 Boeing 737 – Incidences of uncommanded rudder input

PHOTO REMOVED FOR COPYRIGHT REASONS

On 8 September 1994 a Boeing 737-300 aircraft operated by USAir crashed while maneuvering to land at Pittsburgh Airport. The aircraft entered an uncontrollable descent and hit the ground about six miles east of the airport. The NTSB accident report [44] and resulting Safety Recommendation [45] state; "investigations revealed that during the accident sequence, the rudder deflected rapidly to the left and reached its left aerodynamic blowdown limit shortly thereafter.

Examination of the rudder system revealed that it is possible, in the main rudder Power Control Unit (PCU) of the aircraft (as a result of some combination of tight clearances with the servo valve, thermal effects, particulate matter in the hydraulic fluid, or other unknown factors), the servo valve...could have caused the rudder to move opposite to the direction commanded by rudder pedal input."

"Because this accident and other 737 accidents and incidents raised questions regarding the 737's flight control systems, the FAA initiated a Critical Design Review (CDR) of the 737 flight control systems with emphasis on the roll control and directional flight control systems."

A number of Airworthiness Directives (AD) were issued by the FAA covering a redesign of the PCU servo valve and improved operational procedures and pilot training. The report goes on to say, "however, even with these changes, the 737 series aircrafts remain susceptible to rudder system malfunctions that could be catastrophic.

The Board is also concerned that the limited period of vulnerability to rudder malfunction is based on the assumption that a pilot will perform perfectly and that all aircraft systems will perform normally. For example, according to Boeing's fault tree analysis for the 737-New Generation, the combination of a jammed servo valve with a loss of engine power during take-off would be catastrophic only during a 7-second window from V_1 through lift-off.

However, Boeing's analyses apparently assumed that a pilot would always react immediately and correctly and that the hydraulic pressure limiter would not fail. Such assumptions may not be fully warranted."

"The 737 has a history of rudder system-related anomalies, including numerous instances of jamming." The Safety Board expressed concern that the new features of the redesigned PCU did not address all the previously seen malfunctions, some of which were related to improper maintenance, installation or modification. This concern appeared to have been borne out with two further, thankfully recoverable, instances of "anomalous" 737 rudder deflection in 1999.

"During the initial certification of the 737-100 series, FAA certification officials expressed concern about the aircraft's single-panel, single-actuator rudder system and recognized the possibility of undetected latent failures in the servo valve, thereby negating the system's redundancy." Nevertheless, the system received certification without any requirement for modification.

The report quotes information from Boeing, which indicated that "between 1990 and 1994 (before the USAir accident), there were 187 reported yaw/roll events involving the 737. In comparison, information from Boeing's Douglas Products Division indicates that, over about 75 million flight hours, there had only been

three reported yaw/roll events involving the DC-9/MD-80 series aircraft. Information from Airbus indicates that, over about four million flight hours as of November 1995, there had been only one reported yaw event involving the A320, and that event was caused by a rudder mistrim."

Finally, there was a clear suggestion of design error in the design of the PCU servo valve:

"The servo valve was designed to prevent abnormal flow if the secondary slide bottomed out at its internal stop; however, during the investigation of this accident, it was discovered that parts built within tolerances could be assembled with a resulting tolerance buildup that would allow the abnormal flow to occur if the secondary slide moved to its internal stop. Thus, in addition to the potential for overtravel because of an incorrect chamfer, it became evident that the secondary slide could also be forced into the overtravel range if it became jammed to the primary slide. Normal movement of the primary slide could produce a rudder reversal if a primary to secondary slide jam existed."

Following the USAir accident, Boeing's suppliers re-designed the PCU servo valve twice, completing the activity in 1998. Since incorporation of the new design into the 737 fleet, there have been two recorded instances of rudder-related events with the new valve. One was attributed to maintenance error, but the cause of the second was not established. The obvious question to be asked was to what extent was the new design subjected to safety analysis?

3.29.3 Boeing 717 – main flight deck display failures

During the first year of revenue service by the Boeing 717 aircraft, there were two instances of total loss of the main flight deck displays, one occurring immediately after take-off. These failures forced the crews to resort to standby instrumentation, and resulted in a temporary night-time flying restriction on the fleet until the problem was solved. Investigation [46] traced the fault to the Power Conversion Distribution Unit (PCDU), located in the electrical equipment bay under the flight deck and aft of the nose undercarriage bay.

PHOTO REMOVED FOR COPYRIGHT REASONS

The PCDU was failing due to moisture dripping into it. Making changes to the electrical connectors, fitting a drip-tray over the PCDU, and sealing the flight deck floor cured the problem. From a safety analysis standpoint, it would appear on the face of it that a design flaw may have been missed which allowed ingress of moisture into the PCDU, or the zonal analysis may have been insufficiently robust to recognise the danger.

3.29.4 Boeing (McDonnell-Douglas) MD-11 landing accidents

PHOTO REMOVED FOR COPYRIGHT REASONS

Failure to properly analyse failure progression could result in totally unexpected failure combinations catching an operator by surprise. A possible example of how this could happen might be the two recent instances of heavy landings by

McDonnell-Douglas MD-11 aircraft. In both cases, due to external influences, the landings exceeded the design limitations of the undercarriage assembly. However, whereas it might normally be expected that the undercarriage would break away from the airframe under such conditions, in both these accidents the wing structure failed almost simultaneously and broke away from the fuselage, resulting in the aircraft overturning and coming to rest inverted.

In the case of one of these accidents, (to a FedEx aircraft at Newark), the NTSB report [47] cited "structural integrity requirements" as a related safety issue. The report cites the landing gear certification requirements, which specify that no fire hazard from spilt fuel will result from a main landing gear failure due to overload. Boeing stated that "the MD-11 was designed to allow sacrificial shedding (by use of fuse pins) of the main landing gear assemblies under aft (drag) overload conditions to prevent catastrophic loads being transmitted to the wing box." They were also criticised for not giving adequate consideration to the high vertical load condition during the design process.

The risk of being caught out by unexpected or unanticipated failure events has was best summarised by author Charles Perrow as follows [48]:

"A system in which two or more discrete failures can interact in unexpected ways is described as 'interactively complex.' In many cases, these unexpected interactions can affect supposedly redundant sub-systems. A sufficiently complex system can be expected to have many such unanticipated failure mode interactions, making it vulnerable to normal accidents.

The sub-components of a tightly coupled system have prompt and major impacts on each other. If what happens in one part has little impact on another part, or if everything happens slowly (in particular, slowly on the scale of human thinking times), the system is not described as 'tightly coupled.' Tight coupling also raises the odds that operator intervention will make things worse, since the true nature of the problem may well not be understood correctly.

A normal accident typically involves interactions that are 'not only unexpected, but are incomprehensible for some critical period of time.' The people involved

just don't figure out quickly enough what is really going wrong. A normal accident occurs in a complex system, one that has so many parts that it is likely that something is wrong with more than one of them at any given time. A well-designed complex system will include redundancy, so that each fault by itself does not prevent proper operation. However, unexpected interactions, especially with tight coupling, may lead to system failure."

3.29.5 Alaska Airlines MD-83 horizontal stabiliser failure

On 31 January 2000, an Alaska Airlines McDonnell-Douglas MD-83 suffered a catastrophic accident off the coast of California, when the pilots lost control of pitch attitude in the cruise and during an attempted diversion, the aircraft dived steeply into the Pacific with the loss of all 88 people on board.

The NTSB accident investigation report [49] cited loss of control due to poor maintenance, when a failure to grease the mechanism controlling horizontal stabiliser pitch, caused it to become worn and fail, thus allowing the stabiliser to move outside its normal limits. However, one of the most important points to emerge from the investigation was the fact that the stabiliser control assembly was not designed to be failsafe in this case.

Despite the fact that this was the first recorded such catastrophic failure on the DC-9 / MD-80 /717 series of aircraft, all of which use the same basic design, as a single system without any mechanical back-up for the main structural components, it could be argued that this was an accident waiting to happen.

This fact prompted the NTSB investigators to question whether or not a proven, reliable system can be considered to be "safe enough", purely as a result of its, up until that time, impeccable safety record. There was recognition that a redesign, affecting something like 1,800 aircraft, to introduce some failsafe back-up feature to comply with modern practice, would be very expensive indeed for both Boeing (the present owners of the DC-9 / MD-80 / 717 product line) and the airline operators.

What early indicators might there have been from non-catastrophic stabiliser events, which a global data capture and sharing system might have highlighted? In fact it appears that there were several. Investigators found that the accident aircraft's jackscrew end-play was right at the limit required for replacement, two years before the crash, yet this fact and the reasons for not either carrying out the replacement at that time, or instigating some on-going measurement, were neither required nor recorded. Furthermore, out of all the relevant overhaul facilities visited as part of the investigation, only one used a detailed set of workcards to document each step taken during jackscrew overhaul. This in itself is a serious omission in procedures, and one which leaves a gaping hole in the ability to identify and analysis potential problems in service before a major event can occur.

In today's industry, the design of a system in which a single failure can lead to a catastrophic event is not permitted, and NTSB Director of Aviation Safety John Clark described the fact that so many aircraft are still in potential danger thus:

"It's the unknown which is worrisome. If this one single component fails, it leads to catastrophic failure." He went on to acknowledge that the problem is compounded by the fact that maintenance errors happen and that there continues to be the risk of undetected manufacturing error which can lead to premature fatigue and component failure.

The inference from the NTSB accident report is that they have elected to leave the decision about whether or not to re-design the stabiliser system, up to Boeing. Finally in June 2003, Alaska Airlines admitted responsibility for the accident and Boeing said they would not contest liability over the aircraft's

design. The two companies declared their positions in filings to a San Francisco court where relatives of 17 of the victims are pursuing wrongful death claims.

Safety officials rejected Alaska Airlines' claims that flaws in the aircraft's design and maintenance procedures contributed to the disaster. Attorney Brian Panish said:

"This is believed to be the first time that a major aircraft manufacturer has declared that it would not contest liability in a mass air disaster case. It is a victory for the Plaintiffs because the Boeing Company will now be forced to compensate the families of the victims for their tragic loss."

Finally, and of particular relevance to this thesis, the NTSB also recommended that maintenance facilities overhauling DC-9 / MD-80 / 717 screwjacks should not only be required to record end-play measurements, but also to inform their airline customers.

3.29.6 Maritime Patrol Aircraft Electrical System

A fleet of four-engine military maritime patrol aircraft has recently gone through a major structural and systems upgrade to extend both its operational capabilities and its service life.

As part of that upgrade, the opportunity has been taken to install a new Electrical Power Generating System (EPGS) to cope with an increased power demand from new missions systems. The EPGS is a four-channel system, with an Alternating Current (a.c.) generator mounted on the accessory gearbox of each engine. Although there is some system redundancy in the design, that is to say it is possible for the total electrical power demand on the aircraft to be satisfied with less than full EPGS availability, it is necessary to have a minimum of two generating channels on-line before load-shedding is required by shutting-down non-essential equipment.

The mission profile of the aircraft includes extended duration flights of up to eight to ten hours duration, which can be extended even further by means of air-to-air refueling. In order to conserve fuel and thus extend flight duration, it is

Standard Operating Procedure (SOP) to shut-down the two outboard engines for lengthy periods during long-range patrols. As a result, the EPGS is expected to function as a two-channel rather than a four-channel system for a high proportion of its installed life, thus eroding the designed redundancy safety margins. Although this is a questionable operating scenario when viewed solely from the safety standpoint, it has to be remembered that this is a military aircraft and is operated under circumstances where safety levels while still vitally important, can be and are overridden in the interests of mission capability.

Despite this consideration however, an additional concern has arisen as a result of the EPGS upgrade. When the two outboard engines are shut-down, the a.c. generators on the two remaining engines have to satisfy the total electrical power demand for the aircraft, and since it is not required to carry out any load-shedding, as all mission systems must remain on-line, these two generators are now running at or close to maximum output, and thus maximum speed, oil temperature and so on, for extended periods.

This in itself would not be a problem, provided that the reliability prediction of the generator design assumed a steady-state running condition of maximum output, speed and temperature, as is the case with some manufacturers' analyses. However, in the case of these particular generators, this was not the case at all. This time the reliability prediction assumed a steady-state running condition in the mid-range, i.e. average power output, speed and temperature, which is obviously a far more benign regime for equipment reliability and hence safety performance. In fact, the generator manufacturer's reliability guarantee assumed this benign environment, and when challenged on the two-engines out case, stated that the generator reliability figure under those circumstances would be degraded by a factor of approximately ten.

Thus we are left with a condition where not only are safety margins being deliberately eroded by the operator's SOP, but the situation is being considerably worsened by a consequential drastic worsening of reliability performance in those system channels which are still functioning. More details of the analysis which highlighted this problem were shown in section 3.11 on

Fault Tree Analysis (FTA), but the point is that this was done far too late in the equipment selection and design process to have any effect on the outcome.

Reliability predictions cannot be undertaken on a "one condition suits all" basis. There will always be large variations in reliability due to environment, usage rates, location, and so on. This is a recognised problem, and can be addressed by such tools as sensitivity analysis and the establishment of reliability calculation confidence levels. However, this is a complex and skilled art which is often ignored for the sake of expediency, and in any event, the ability to perform such additional analysis over the full range of possible operating scenarios can be at best minimal.

3.29.7 Airbus A340 Main Undercarriage Failures

Of course, not all design or analysis errors have such extreme consequences, and other examples might include the main undercarriage problems in the early service days of the Airbus A340, culminating in an incident at Heathrow on 6 November 1997 involving a Virgin Atlantic aircraft. The airline was unaware of a similar failure with another carrier, and the accident occurred when the aircraft, which had a landing gear problem on approach to Heathrow Airport, subsequently carried out an emergency landing with the left main landing gear only partially extended. Full deployment of the landing gear was prevented by the unrestrained end of the brake torque rod having become trapped in the keel beam structure within the gear bay, jamming the landing gear in a partially deployed position. The torque pin which had connected the brake torque rod to that wheel brake assembly had disengaged during landing gear retraction after

take off from Los Angeles, allowing the unrestrained rod to pivot freely about the retained end.

The wheel brake assembly design had satisfactorily passed the certification structural torque tests. However, the tests contained no requirement to use a representative axle to reproduce the deflections that occur during aircraft braking in service, and did not require post torque test strip assessment of brake assemblies for resultant evidence of overstressing deformation, which did not produce component failure. Once again, had there been an effective in-service data capture system in place, such as the one proposed in this thesis, it is quite probable that the earlier failure could have alerted other operators to the danger, and forced remedial action prior to the Virgin Atlantic incident.

3.29.8 Commercial Aircraft Fuel Tank Safety

Between 1990 and 2001, there were three commercial aircraft hull loss accidents, which had explosions of fuel tank vapour as their primary cause. These were:

- Philippine Airlines Boeing 737-3Y0 11 May 1990 at Manila Airport. The aircraft was parked in very high ambient air temperatures of around 95 degrees Fahrenheit (35 degrees Celsius), with external air conditioning packs positioned beneath the centre wing fuel tank, which had been running for approximately 30 to 45 minutes. The fuel tank had not been filled since March 9, but probably still contained fuel vapour. Shortly after pushback a large explosion occurred in the centre fuel tank, pushing the cabin floor violently upwards. The wing tanks ruptured, causing the aircraft to burst into flames. The fuel vapour had probably been ignited by damaged wiring.
- TWA8 Flight 800 Boeing 747-131 17 July 1996 over the Atlantic Ocean. The probable cause of this accident, which resulted in the total disintegration of the aircraft in the cruise, was an explosion of the centre wing fuel tank resulting from ignition of the flammable fuel/air mixture in the tank. The ignition source was never determined, but the most likely candidate was a short circuit outside the tank that allowed excessive voltage to enter it through electrical wiring associated with the fuel

quantity indication system. It was stated that contributing factors to the accident were both the design and certification belief that fuel tank explosions could be entirely prevented by precluding all ignition sources, and also the design and certification of the Boeing 747 with heat sources located beneath the tank with no means to reduce any heat transfer into it or to render the fuel vapour in the tank nonflammable.

- Thai Airways Boeing 737-4D7 at Bangkok Airport 3 March 2001. Parked at the gate in an ambient air temperature of 35 degrees Celsius, and again with air conditioning packs located directly beneath the center wing tank which had been running continuously for 40 minutes. Fuel vapour in the centre wing tank probably ignited, causing an explosion and fire, which ultimately gutted the aircraft.

In response to these accidents, the certifying authorities placed the following flammability reduction measure requirements on the aircraft manufacturers; automated cut-off of fuel pumps running dry, improved lightning strike protection and fresh consideration of the routeing and location of high-power wiring harnesses. As a result, it became apparent that most affected aircraft types would require design changes to be carried out, and that these would require mandatory configuration control measures to ensure fleet-wide compliance.

Following the re-design effort, it was required to introduce improved maintenance programmes by December 2005. Unfortunately, while the FAA also required retrospective introduction of these changes, EASA did not, which can result in loss of configuration control across like fleets, and the potential for confused fire safety standards.

3.29.9 Global Aviation Information Network (GAIN) Examples

Two further examples of the potential for learning through the use of more robust procedures have been reported by the GAIN initiative [50].

"Airline B experienced the loss of an engine cowl on one of its aircraft during takeoff. Investigation revealed the cause to be the failure of line maintenance personnel to properly secure the cowl latches following routine engine maintenance, due in part to the lack of color contrast between the latch

recesses and the adjacent cowl livery. Airline B subsequently modified the colour of the latch recesses to facilitate visual recognition of incorrect latch alignment, and amended its line maintenance procedure to include a cross-check of cowl latch security. It also posted an incident report on a safety information sharing system in which it participated and notified other operators of the same equipment participating in the safety information sharing system. Several of these operators subsequently modified their line maintenance procedures and some also modified the latch recess color scheme."

"In the course of a routine inspection, Airline C discovered a cracked engine mounting bolt that could have led to an overstress of the engine mounting and an in-flight loss of the engine. A check of incident reports on a safety information sharing system in which the airline participated revealed that two other operators had experienced the same problem and had concluded that the procedure for engine removal and replacement had the potential to overstress the mounting bolt if the engine was misaligned during replacement. These airlines had devised and adopted a different procedure for engine removal and replacement that avoided the potential problem. Airline C then adopted the new procedure and notified other operators of the same equipment participating in the safety information sharing system of the potential problem."

3.29.10 Study Of Global Aircraft Accident Reports

Using the Aviation Safety Network on-line aircraft accident database as a starting point, every listed commercial and corporate aircraft accident and major incident for the period 2001 to 2005 was analysed for contributory causes (see Appendix B). Conclusions were drawn based on either the results of the post-accident investigation, where that was known, or using engineering judgement based on the available, more limited, evidence presented in the database.

A total of 112 events was subjected to this analysis, taking as a starting point, those that had clear evidence of system or equipment fault as a significant contributory factor, in order to exclude purely human error events. The results of this analysis indicate quite clearly, that over that five year period there have been a number of accidents and incidents which, it can be argued, might have been prevented, or had a lesser impact, if either the original system safety

analysis had been more robust and /or there had been an effective service event data capture system in place.

3.29.10.1 Identified Significant Event Groups

As a result of the analysis, the following event groups were identified from those accident and incident records containing sufficient data to be able to draw conclusions with a reasonable degree of confidence:

a) Maintenance error (22 events)
b) Component failure (20 events)
c) Unpredicted failure mode (8 events)
d) Design fault (4 events)

Looking at each of these categories in more detail, and starting with maintenance error, it was noticeable that two of these (C-130A 17 June 2002 and PB4Y-2 18 July 2002), identified inadequate procedures that failed to take account of either the advanced age of the aircraft concerned, or the unusual environment in which there were operating. These are both major arguments contained within this thesis. Other events cited yet more inadequate procedures, ineffective repairs and/or poor oversight, with five accidents occurring either immediately after the completion of maintenance, or very shortly thereafter.

The two main lessons emerging from this group are; the lack of awareness of the need to review and modify procedures over time as aircraft age and operations change based on in-service feedback and monitoring, and the apparent ease with which maintenance standards and supervisory oversight may fail to adequately defend against progression towards an accident. In both cases, it is argued that better use of in-service event reporting (confidential if required), could have helped prevent some of these events from occurring.

Moving on to component failure, this category is obviously less easy in terms of identifying potential remedies, since it might be argued that all could have been simply the result of a random failure. However, that is not to say that there

would not have been any earlier indications of impending failure, such as performance degradation still within operating limits, or even incorrect maintenance action, which again, an event reporting system might have picked up.

The category of unpredicted failure mode is, on the face of it, more straightforward, since six of the eight identified relate to almost identical events on the same type of aircraft – engine failure on the Cessna Caravan. This single-engined aircraft is fitted with the normally extremely reliable Pratt and Whitney Canada PT-6 turboprop, which has a very long history of service in a number of different applications. However, all but one of the events listed occurred to aircraft operating in fairly challenging operating environments, with the majority occurring shortly after take-off. Given that eight of the 44 engine failures analysed occurred to this one type, it is reasonable to suppose that there may be some aircraft/engine interface problem with the Caravan that has not as yet been identified, and may well be linked to operating scenarios not fully considered during the design analysis process. It is worth noting in this regard, that one African operator of the Caravan (Air Kenya) withdrew its fleet from service in 2004, due to concerns about engine reliability; as yet there appears to have been no publicised response from the manufacturer.

Another case of unidentified failure mode relates to the Fokker F.27 accident on 5 June 2002. This Rolls-Royce Dart engine turbine disc failure had only ever occurred once before, and was still under investigation at the time of this incident. In this case, it is clear that there was effective feedback from the first event, and good reaction to try and address the problem.

Finally the four design fault events. One is the Alaska MD-80 horizontal stabiliser accident already discussed in this chapter. The second was a fuel starvation incident, which occurred to a Virgin Atlantic Airbus A340-600 on 8 February 2005. The problem was traced to a design logic fault in the fuel control computer, causing a failure to transfer fuel automatically between tanks. This event simply reinforces the need to understand that design analysis does not stop at system certification.

The third design error event occurred on 6 March 2002, when a Domier Do.328 turboprop had a partial door opening during the take-off roll, which was safely aborted. The subsequent investigation found that although the airstair and door design was technically compliant with certification requirements, it lacked the necessary integrity to prevent such a hazardous occurrence (a cabin attendant had inadvertently grabbed the inner door handle to restrain herself during the initial acceleration). The recommendation was for a thorough review of the entire door operating mechanism. It would appear that in this case, the original zonal analysis may not have been as thorough as it might have been, but the main lesson here is yet again, the need for incident reporting systems. It would be unreasonable to suppose that this was the first time an attendant had used the door handle as a means of restraint, and surely the potential hazard of so doing must have occurred to those who may have done this before. A confidential reporting system may well have highlighted their concerns and thus prevented earlier action and prevention of this near-accident.

The final design fault accident occurred to a Lockheed-Martin F/A-22 Raptor on 20 December 2004. The aircraft was lost due to the failure of all three rate sensor assemblies, which provide feedback on yaw, roll and pitch status to the Flight Control System (FCS). The pilot had inadvertently triggered the failures during his pre-flight preparations when he shutdown the engines for a maintenance check, believing the FCS was continuously powered by the APU. In fact, the FCS momentarily lost power in this event, and this was linked to a known quirk in the system, which was programmed such that it could interpret a momentary power loss as an instruction to enter test mode, which freezes or latches the unit. Furthermore, the FCS could not warn the pilot that this had occurred. Up to this point in the Raptor flight test programme, the aircraft manufacturer had returned some 20 control units to British Aerospace for investigation of suspected latching events, resulting in a design change and fleetwide embodiment of a new standard unit.

As Alexander Wells puts it in his book *Commercial Aviation Safety* [51]:

"Non-accident safety data, while not substitutes for accident and fatality data, are valuable supplements. If properly collected and maintained, non-accident

data can help identify and estimate the magnitude of safety problems and permit the monitoring of safety programmes."

Perhaps the most interesting statistic to emerge from this study is the percentage of aircraft accidents for which "pilot error" was the primary causal factor. As stated in Chapter 1, conventional wisdom would have us believe that approximately 75% of total loss accidents can be attributed to the human cause. Looking at the 112 events analysed above, it was found that the percentage for human factors contribution is still close to 55%; a significant point.

3.30 CASE STUDY CONCLUSIONS

In each of the case studies described above, it was clear from investigation that there had been fundamental errors in either basic design for safety, safety analysis of design, post-design testing, or combinations of these. The main points from each study are:

- 767 un-commanded thrust-reverser actuation – Incomplete failure mode evaluation of the thrust-reverser system.
- 737 un-commanded rudder movements - Design error in PCU servo valve not found during analysis.
- 717 flight deck display failures – Design flaw permitting moisture ingress plus poor zonal analysis.
- MD-11 landing accidents – Absence of design considerations for undercarriage sacrificial failure in the drag condition.
- MD-83 horizontal stabiliser failure – Single point failure leading to a catastrophic event, not permitted under current certification rules, had been carried across without re-design from the DC-9 aircraft, which was designed in the 1960s before the rule was introduced.
- Maritime patrol aircraft electrical power system reliability – A failure by the generator manufacturer to recognise the potential for drastically reduced equipment reliability when operating under certain standard operating flight conditions.

- A340 main undercarriage failures – Failure to adequately test the undercarriage design using conditions fully representative of those expected on the aircraft in service.
- Fuel tank safety – Failure of different certification authorities to agree on a common approach to implementation of essential safety modifications.
- GAIN examples – The other side of the coin, demonstrating the potential for corrective action to address design anomalies, when data sharing is effective between operators.
- Study of global aircraft accident reports – Statistical confirmation of the need for improved in-service event data capture and analysis, and more robust design safety analysis.

The question that emerges from these cases is, has the industry adequately learned the lessons for the future? If this is not the case, what can be done to make the designer and analyst's life easier to produce less opportunity for such error in their next aircraft programme?

3.31 DEPTH OF ANALYSIS

It is apparent that in some sections of the aerospace industry, there is a lack of appreciation of both the value of the system analysis process, the point in the equipment life-cycle at which it should be started and the depth to which it should be taken in order that failure mechanisms can be properly understood. Too often it is the case that failures are analysed by the manufacturer as single events and effects, with little consideration for the subsequent chain of events that may occur. The more detailed investigation tends to be reactive to events, such as the excellent work done by the Air Accident Investigation Branch (AAIB) on the A340 incident described above.

This raises the issue of how well zonal, cross-system or whole aircraft analysis is performed. Recent initiatives to establish extensive combined designer / customer teams during new aircraft development (as with the Boeing 777 for example), plus the continued enhancement of computer-aided design and computer simulation of aircraft systems and interfaces are all good aids to design refinement. Nevertheless, while it can be argued that for instance, the

circumstances surrounding the MD-11 accidents were so extreme that no amount of analysis could have accurately predicted the actual failure progression, there is no escaping the fact that analysis of the interaction of different systems is not as smart as it needs to be.

To be fair to the manufacturing industry, the airworthiness authorities must shoulder some responsibility for this, as during the course of this research it has been stated on several occasions that there is a distinct lack of regulatory guidance from them. The authorities have tended to rely almost exclusively on the sense of regulation FAR / JAR 25.1309 (see section 2.5), without going into much detail of the processes they expect the industry to use, thus leaving the door open to misinterpretation, lack of understanding, or too much room for flexibility and short-circuiting of analytical processes as a replacement for industry experience, in order to save time and money.

3.32 LEGISLATION

This lack of regulatory guidance is the root of the problem. The existing legislation framed by the airworthiness authorities to ensure that aircraft systems are fit for purpose and safe, is inadequate. Whilst the specific requirements for system performance, failure effect severity, failure probability and so on are well defined, the required methodology is insufficiently defined and policed to ensure adequate adherence. Even the new European Aviation Safety Agency (EASA) appears to have failed so far to grasp this issue [52]; this is potentially a major lost opportunity.

The authorities response to questions in this regard, is to point to the need for adequate training of system analysts; this misses the point. Most of the safety analysts working in the industry today are highly skilled, professional engineers who know their job, and are very familiar with the various guidance documents and standards.

However, issues such as commercial pressures, lack of resources, etc. continue to harass the safety analyst and all too often result in the line of least

resistance being taken. From personal experience within the aircraft system industry, the author can say that this can result in any one or all of the following:

- Analysis started too late to adequately impact on design
- Analysis results "tailored" to fit the expectations or design requirements
- Incomplete analysis – the minimum to satisfy the requirement
- Suspect data which may not be supportable – e.g. failure rates
- No independence in the analysis – the designer does it himself
- A potentially unsafe system enters service

The FAA states in Advisory Circular 23.1309-1C Equipment, Systems and Installations in Part 23 Aircraft, that:

"This advisory circular provides guidance and information for an acceptable means, but not the only means, for showing compliance with the requirements of 23.1309. This material is neither mandatory nor regulatory in nature and does not constitute a regulation." Perhaps it should? In the next chapter the various conflicting views that lead to the posing of this question are discussed.

3.33 SUMMARY

It is clear that despite the good safety levels being enjoyed by the industry, there is little room for complacency, particularly with regard to the projected future growth of air travel. The case studies examined demonstrate that the emergence of human factors as the centre of attention must not be allowed to completely divert attention away from the problems of technical failure. However, even such acknowledged experts as Charles Perrow are still not taking their work far enough. He excludes from his analysis what he calls "final accidents," catastrophic events such as an aircraft breaking up in flight, since, he says, "they are not interesting from an analytical point of view because there is nothing that the operator can do to influence the course of events." This sweeping statement ignores the vital contribution of in-service data capture to the overall effort to ensure safe designs. The legislators must take a clear stance on this issue and ensure that the industry uses the best available processes to produce robust system safety analysis.

CHAPTER FOUR – IN-SERVICE DATA GATHERING SYSTEMS

4.0 INTRODUCTION

This chapter examines the use of commercially available data gathering systems to collect and analyse commercial aircraft in-service event data, and comments on the usefulness of the data captured and the effectiveness of the analysis. Regulatory guidance material is considered, and is coupled with the standard processes for formulating aircraft maintenance programmes and the associated reliability monitoring requirement. Wider issues discussed include Flight Data Monitoring (FDM), Mandatory Occurrence Reporting (MOR), maintenance error reporting, human factors issues, and the effectiveness of various industry responses.

The chapter concludes with a detailed look at the key areas of system safety that need to addressed, concentrating on clear demonstration of the need for far more accurate and meaningful event data capture and feedback than is currently available.

4.1 DATA GATHERING SYSTEMS

"British Airways credit the use of a Flight Data Analysis programme, as part of a safety management system, as reducing their hull losses from 30, in the years 1952 to 1978, to 2, in the period 1978 to 1999." [53]

"Aviation accidents and incidents continue to occur, information sharing is usually anecdotal and not business-as-usual...currently there is no single source of lessons learned/corrective action information for the aviation community." [54]

When in-service event data gathering is done, the most common methodology by which an aircraft or systems manufacturer will capture the data is by use of a Failure Reporting Analysis and Corrective Action System (FRACAS), which gathers event data, deposits it into a database or spreadsheet and then offers the facility to analyse that data for performance, reliability and failure trends.

The system will also add in additional data such as that provided by the repair and overhaul people, while the most developed systems also have a formalised output that requires trend review and corrective action to be taken if necessary.

In more recent times the similar sounding Defect Reporting Analysis and Corrective Action System (DRACAS) has gained favour in some parts of the industry, since it attempts to illustrate a more developed approach to equipment performance analysis than is the case with a system that just looks at failures. Given that an understanding of what is and what is not a true component failure is, perhaps surprisingly, not as widespread as it should be, this opportunity for improved analysis is still not well established.

4.2 HOW RELEVANT IS THE DATA?

"Modern technology has a lot to offer the operating organisations. Better, more comprehensive monitoring of aircraft components, systems and performance coupled with enhanced means of transferring and analysing the recorded data can provide big payback. The reality is that aircraft are being kept in service for longer and their mission requirements are continuously being revised. As a fleet ages so its maintenance costs continue to grow. Concurrently, the pressure to increase maintenance productivity, reduce maintenance manhours and improve aircraft readiness continues to strain the current structure. Better understanding of aircraft actual usage, more accurate and timely information on needed aircraft maintenance and improved tracking of component usage is critical to realising gains in aircraft readiness. Comprehensive aircraft monitoring is the key to this achievement." [55]

Let us now take a closer look at the data that may go into a FRACAS (or DRACAS) system. In the early days of equipment's service life it is likely to be covered by the manufacturer's warranty. For that reason alone, whenever a unit suffers an unscheduled removal from an aircraft, it is virtually certain that the operator will return it to the manufacturer for assessment and repair. Therefore there will be considerable confidence that the manufacturer is getting information about every such event across the whole fleet of aircraft fitted with his equipment, and thus he believes that his resultant reliability calculations will

be as accurate as possible. However, in those early days of fleet build-up when flying hours totals are comparatively low, small changes in the number of equipment arisings can have disproportionate and distorting effects on reliability calculations.

The picture changes considerably however, once the warranty period passes. The operator may elect to repair the equipment himself or contract the work out to a third party, with the result that the flow of data back to the manufacturer becomes at best less than complete, and at worst ceases altogether. This will be especially true of equipment that goes to a third party, since in many cases they will be in direct competition with the manufacturer for repair business and will therefore be highly unlikely to share their shop findings.

Will the manufacturer now recognise the fact that his FRACAS system is no longer seeing 100% of fleet events, or will he simply believe that his equipment is becoming more reliable as time goes on? Unless he recognises the signs, he will continue to analyse reliability using 100% of the total fleet flying hours and far less than 100% of the events. This distortion of the analysis may then get fed back into the design team who get an unjustifiably rosy picture of how the equipment is performing, and then use those incorrect failure rates in the safety analysis of follow-on or upgraded equipment.

An example of this is a recent case involving safety analysis of contactors in an aircraft electrical power distribution system. The manufacturer claimed an extremely low failure rate for his contactors, and when challenged to justify it, stated categorically that the rate had been established by in-service data, and was based on all the units returned to them for repair. What the company's analyst had failed to recognise was that a very significant proportion of contactors failing in service were simply being discarded on failure and replaced with new ones, since it was a far more cost-effective policy than going to the expense of putting them into the repair loop.

Of course it could also be true that the manufacturer's data gathering system is not sufficiently robust to recognise unjustifiably pessimistic analysis, which may then penalise a design because it apparently fails to meet its safety targets.

Such errors can occur when the natural instinct to "worst-case" incomplete data is permitted to cloud the data.

4.3 WHAT TO DO WITH THE DATA

Despite these attempts at gaining a better understanding of how a manufacturer's equipment is performing in the field, all too often the result is a data gathering system without a close-out action loop; in other words what the company really has is a FRA system without the CAS. If the data is not properly analysed and the need for some kind of action goes unrecognised, then potentially damaging and costly impacts on the customers may not be addressed. From the safety analysis perspective, a full and correct understanding of equipment performance, failure mechanisms and trends will not be gathered to be fed back into the design analysis.

The other major problem endemic in many FRACAS systems is the inability to differentiate between an inherent component failure, and an induced (or secondary) failure. Without this understanding through sufficient detail in both repair shop strip reports and the FRACAS system itself, the outcome may be a corrective action that addresses the wrong failure mode. Needless to say, this not only has the potential for generating expensive and ultimately fruitless equipment modification, but also will seriously undermine the value of the reliability data being fed into the analysis of new or improved designs.

Fortunately the SAE, at least, has recognised this poor approach to the monitoring of in-service equipment performance. A new standard ARP 5150 was released in 2003, and is intended to be the international standard for ongoing safety assessment of aircraft in the field.

The fundamental issue is that when analysing a new design, it is vitally important to be certain just how relevant the raw FRACAS input data coming from the field really is. Without that certainty, unjustified beliefs in reliability high-performers may become so entrenched in the organisational psyche that it can come as a major and expensive shock to learn, some years down the line, that all is not well with the operators.

4.4 REGULATORY GUIDANCE

What guidance does the industry receive from regulators or other bodies that might encourage the retrieval, analysis and effective action-taking of empirical data from the in-service fleet? The short answer is "plenty"; but a closer look at what is expected soon reveals significant holes in the guidance.

Implicit in the JAR-OPS regulations concerning aircraft maintenance (contained in Sub-Part M), is the requirement for an operator or his contracted maintenance provider, to have a system to monitor the effectiveness of their maintenance programme. Specifically, JAR-OPS states in section 1.890(a)(4) Maintenance Responsibility:

"An operator should have a system to analyse the effectiveness of the maintenance programme, with regard to spares, established defects, malfunctions and damage, and to amend the maintenance programme (this amendment will involve the approval of the Authority unless the operator has been approved to amend the maintenance programme without direct involvement of the Authority)."

Section 1.910(a) Operator's Aeroplane Maintenance Programme is even more explicit:

"Where an operator wishes to use an aeroplane with the initial operator's aeroplane maintenance programme based upon the Maintenance Review Board Report (MRBR) process, any associated programme for the continuous surveillance of the reliability, or health monitoring of the aeroplane should be considered as part of the aeroplane maintenance programme. Some approved operator's aeroplane maintenance programmes, not developed from the MRB Process, utilise reliability programmes. Such reliability programmes should be considered as a part of the approved maintenance programme. Reliability programmes should be developed for aeroplane maintenance programmes based upon MSG logic or those that include condition monitored components or that do not contain overhaul time periods for all significant system components."

A suggested method of compliance with these requirements was first defined in the JAA's Temporary Guidance Leaflet (TGL) 25, which layed out their vision of an ideal process. Subsequently, the TGL25 principles were absorbed by EASA into guidance material on means of compliance with the regulatory requirements for commercial aircraft maintenance programmes, albeit essentially unchanged. The good news was that this material stated that a reliability programme should be in place for any aircraft whose maintenance programme is defined using Maintenance Steering Group 3 (MSG-3) rules. It is necessary to explain in some detail exactly what that means, in order to illustrate just how complex this whole problem of accurate in-service data gathering has become.

4.5 ORIGINS OF MAINTENANCE STEERING GROUPS

The MSG system has its origins in a United States initiative in the 1960s. Up to that time, there was no standardised, structured procedure for developing scheduled maintenance plans for commercial aircraft, and as a consequence, the tendency was for operators to over-maintain aircraft and systems. The reason for this of course, was that no-one had a clear view of the safety effects of all system failures, because they were not being analysed, so by the "belt and braces" approach, the view was taken that too much maintenance was better than not enough.

This approach was obviously not only very hit and miss with regard to ensuring safety, but was also generating excessive amounts of maintenance man-hours per flying hour, and thus becoming a major financial burden on the airlines. The MSG initiative, lead by representatives of various airlines, decided to start addressing the issue by looking at aircraft engines, and building a process to identify those parts which could cause a major safety problem if they failed, and concentrate on these when constructing the scheduled maintenance programme. In theory therefore, a significant number of other parts could be taken out of the maintenance schedule and in essence, allowed to fail – the so-called condition-based maintenance, generically known as "fit and forget".

4.6 EVOLUTION OF MSG-3

The first major outcome of the initiative was the publication of Handbook MSG *Maintenance Evaluation and Program Development*, which included decision logic and airline/manufacturer procedures for developing scheduled maintenance plans for the then-new Boeing 747, chosen as the vehicle for what came to be known as MSG-1. This laid the basis for the system that is still used today, and which is described below.

The process was further refined to make it non-aircraft type specific, and the resulting MSG-2 *Airline/Manufacturer Maintenance Program Planning Document* was derived in the 1970s to analyse both the Douglas DC-10 and Lockheed L-1011 aircraft. Next, the British and French aircraft industries picked up the process, and the European MSG version was successfully used on the Concorde and Airbus A300 programmes, with the lessons learned from that being fed back into the original US model. An Air Transport Association (ATA) task force reviewed MSG-2 to finally produce today's MSG-3, which included some clarification of the distinction between economics and safety, and more adequate treatment of hidden functional failures. With relatively minor amendments, this is where we are today.

4.6.1 The MSG-3 Process

The MSG-3 process is closely allied to another long-standing model, Reliability Centered Maintenance (RCM), which was formulated many years ago by two United Airlines employees. In an effort to further promote this work, John Moubray gave RCM a wider audience through his book *Reliability Centered Maintenance* published in 1992. RCM is a very thorough audit of equipment and process functionality with the end result usually being a programme of non-destructive testing and usually some procedure changes to avoid catastrophic failure. Moubray said he saw no harm to equipment or processes by using RCM and believed that it was a long and arduous way of developing an effective non-destructive testing plan.

It was quickly taken up by the US Armed Forces and embedded in the present worldwide process, MIL-STD-2173.

MSG-3 itself is originated by the aircraft and system manufacturers, with the results being reviewed by Industry Steering Committees (ISC) Maintenance Review Boards (MRBs) representing regulators, operators, and so on. However, the process does not stop once the MRB is happy, since following entry into service, the operator may wish to modify the scheduled maintenance programme in some way to suit his own particular operating scenario, and the rules allow him so to do, provided that he still follows the same MSG-3 methodology.

The first step is the identification in every system on the aircraft, of those parts which, if they failed, could cause a significant safety problem. This is done by answering the following four questions:

a. Could failure be undetectable or not likely to be detected by the operating crew during normal duties?

b. Could failure affect safety (on ground or in flight), including safety/emergency systems or equipment?

c. Could failure have significant operational impact?

d. Could failure have significant economic impact?

If the answer to any one of these questions is "yes", then the part is termed a Maintenance Significant Item (MSI) or, if it is a structural component a Structurally Significant Item (SSI), and must now be taken through the rest of the analytical process. However, if all four questions have been answered "no", the process stops and no further analysis of the item for maintenance requirements is required. Needless to say, it is vital that this initial selection is accurate, and at the design stage, the information provided to answer the four selection questions comes from the designer's FMEA and / or FMECA.

Following selection SSIs are next taken through a process that asks a further series of questions about the nature of their failure effects, which depending on the responses are categorised as one of the following:

a) Evident / Safety – the effect of the failure is evident to the flight crew and could have major or catastrophic consequences

b) Evident / Operational - the effect of the failure is evident to the flight crew and could curtail operational or have a significant operational impact. Note: Operation is defined as the time during which passengers and crew are onboard for the purpose of flight.

c) Evident / Economic – the effect of the failure is evident to the flight crew but the effects have only an economic impact, e.g. loss or degradation of non-critical and non-operational systems in flight, and corrective maintenance activity back on the ground

d) Hidden / Safety - the effect of the failure is NOT evident to the flight crew and could have major or catastrophic consequences

e) Hidden / Operational - the effect of the failure is NOT evident to the flight crew and could curtail operational or have a significant operational impact

f) Hidden / Economic - the effect of the failure is NOT evident to the flight crew but the effects have only an economic impact, e.g. loss or degradation of non-critical and non-operational systems in flight, and corrective maintenance activity back on the ground

As can readily be seen, categories a) and particularly d) are especially undesirable.

Following categorisation, each MSI is now taken through a final series of questions intended to identify what (if any) scheduled maintenance activity can be applied that will be appropriate and effective in reducing the probability of occurrence of the failure and its consequent effects on the aircraft. Once again, there are a number of options:

1) Is a lubrication / servicing task appropriate and effective?
2) Is an operational / visual check task appropriate and effective?
3) Is an inspection / functional check task appropriate and effective?
4) Is a restoration task appropriate and effective?
5) Is a discard task appropriate and effective?

As soon as "yes" is answered, the process stops and all that is now required is to fully define the nature of the maintenance task, together with a justification statement and a proposed periodicity, (it is acceptable to say "yes" to more than one task). Here too, it can be seen just how vital it is to assess the accuracy of the analysis by learning from in-service feedback, thus giving confidence in the maintenance of safety margins (assuming of course that the original FMEA – FMECA – SSI / MSI task selection trail was correct).

What happens if no maintenance tasks can be identified as appropriate and effective? Here MSG-3 is very unambiguous. In the cases of failures with safety effects, either evident or hidden, it states that re-design is mandatory. In all other cases, i.e. those with operational or economic outcomes, it says that re-design may be desirable.

However, what if there was a fine line in the decision process between whether or not a failure had a safety effect or an operational effect? What part might the original use of non-empirical failure rate data have had to play in that decision? Could all this subsequently be influenced by a commercial decision based on the premise of trading off safety against the economic viability or desirability of what could be an expensive re-design?

Once we enter the in-service phase of the fleet, and aircraft are being maintained by JAR-21 (design authority) and JAR-145 (maintenance) approved organisations, who are allowed within certain limits to design and incorporate their own modifications, just how robust are their systems within the framework of JAR-OPS Sub-Part M and the acceptable means of compliance in ensuring a full understanding of what they are doing in MSG-3 terms?

4.7 MAINTAINABILITY

Of course, no matter how good the MSG-3 work has been, the starting point for effective maintenance to ensure safety levels, has to be a maintainable design. Right back at the beginning of the safety analysis process, maintainability (and repairability) should have been inherent parts of the analysis.

A maintainability prediction provides a solid framework for performing maintainability analyses. Replaceable component data is used to generate maintenance parameters and calculations, including Mean Time to Repair (MTTR), Mean Maintenance Man-hours per Repair (MMH/Repair) and so on. Gaining ever increasing importance is the ability of on-board monitoring, testing and diagnostic systems to isolate and identify an ever increasing percentage of faults to a single replaceable item. Typical requirements for new systems talk of values in the order of 90% plus.

Indeed, new developments in test technology are predicted to see engines and other aircraft components eventually becoming "smart assets" that tell maintenance planners exactly what their condition is, what maintenance they are going to need and when they will need it. Managers will, in turn, plan the most economical schedules for repairing or replacing these smart pieces of equipment, supposedly without the expensive unscheduled removals that happen today. That, at least, is the vision, and many people share it. However, there still are substantial hurdles and questions. Quite apart from the danger of false warnings leading to a high rate of No Fault Found (NFF) removals, what about the skill of the maintenance engineer? There was much talk in the 1980s and 1990s of the need for aircraft operators to remain as "intelligent customers", that is to say, retaining a certain level of systems knowledge and expertise to ensure that in-house maintenance activity, even at line level, remained cost-effective. Even in the cockpit, it has recently been stated that pilots entering the profession today may go through their careers without ever experiencing an engine failure, due to the high levels of reliability now being achieved. If they did suffer a failure, how confident might the pilot feel in coping with the situation?

The relentless drive towards diagnostic and prognostic sophistication may, in many ways, militate against this philosophy, and turn our line engineers especially into little more than licensed "box changers". Indeed it is not just the engineers who may fall into this trap of diminished systems awareness, so vital in order to maintain our flight safety levels and provide the feedback that should be the life-blood of the design and analysis effort.

Take the example of the Air Transat A330 incident in 2001. The aircraft was on a scheduled flight from Canada to Portugal when it suffered a major fuel leak in the supply to the right hand engine, which as a result, flamed out. Some minutes later, the left hand engine also flamed out, primarily because the flight-deck crew system knowledge was insufficient to enable them to accurately identify the fuel system leak problem and take the appropriate corrective action to isolate the leak which was available to them. In the event, the aircraft was able to glide to a successful un-powered landing in the Azores, but nevertheless, the lesson is clear. Not only should flight crews be given additional training in aircraft systems knowledge, but also how safe can a system truly be claimed to be if such an event can be allowed to happen?

Once again we are bringing in several aspects of safety analysis:

- Design analysis that must consider system safe states
- Efficiency of Built-In Test Equipment (BITE)
- Possibility of incorrect actions required by the crew

Poor maintainability design not only impacts directly on maintenance cost per flight hour, but also may lead to incorrect or incomplete corrective action or maintenance being performed either on the flight deck or in the field.

4.8 HOW GOOD IS EASA GUIDANCE MATERIAL

As we have already said, an aircraft operator may elect to repair aircraft and equipment himself or contract the work out to third parties, a decision based not only on financial expediency, but also on a whole host of other issues including his own capabilities in terms of facilities, people skills, experience and so on, repair turn-round times, fleet size, annual hours flown, etc.. The more diversified the maintenance system is, the more likely that the flow of data back to the manufacturer becomes less than satisfactory.

EASA guidance material clearly states that an operator is perfectly at liberty to contract out not only his maintenance, but also the accompanying reliability programme, although he still has a "duty of care" in both cases requiring audit of

his contractor's capabilities on a regular basis. So far so relatively good, but the data trail is now getting very lengthy and unwieldy indeed, and thus like any chain, it is only going to be as strong as its weakest link. It must be remembered that what we are trying to achieve in all this is a clear understanding *by everyone concerned* of just how well equipment and systems are performing in service, in order to:

1) Ensure aircraft safety levels are not being compromised
2) Identify event trends and do something about them
3) Measure the effectiveness of maintenance programmes and corrective actions
4) Prevent re-invention of the wheel by learning the lessons
5) Communicate the results

There are three final chinks in the acceptable means of compliance's armour or, as Professor James Reason says in his well-known work on risks and defences, there are two further ways in which the holes in the defences can line-up to allow, in this case, risk to slip through un-noticed.

Firstly, because the EASA material is for **guidance** only and therefore not mandatory in all its aspects, the distribution of reliability reports is largely left to the judgement of the originating organisation. As a result, it is easy, and perhaps tempting, for some to have minimal distribution of their reports outside their own four walls. Perhaps this is driven by a desire to avoid airing their dirty linen in public, or to avoid any issues with commercial confidentiality as has already been mentioned. In either case, if they are not forced to give reports the widest possible circulation, then obviously they will not do so unless they can see a clear benefit.

Secondly, operators of small aircraft fleets are quite rightly encouraged to tailor their reliability programmes using their own engineering judgement, to ensure that the data they do collect and analyse is appropriate. The main reason for this is that drawing meaningful conclusions from failure trend analysis when you have a fleet of only a handful of aircraft, perhaps of mixed types, and maybe with low annual utilisation, is virtually impossible. But, that should not mean that

their data is not just as important as that coming from those with large fleets. There are lessons to be learned from everyone, not least because of differences in operating scenarios, environmental conditions, utilisation, maintenance programmes and so on. The small players should be encouraged to share their data, while at the same time, the owner of the "central database", be it the aircraft manufacturer, system manufacturer, regulator, or whoever must disseminate the analytical results and recommendations back out to everyone too.

Thirdly, the acceptable means of compliance lists the following sources of data for a reliability programme:

(a) Pilots Reports
(b) Technical Logs
(c) Aircraft Maintenance Access Terminal / On-board Maintenance System readouts
(d) Maintenance Worksheets
(e) Workshop Reports
(f) Reports on Functional Checks
(g) Reports on Special Inspections
(h) Stores Issues/Reports
(i) Air Safety Reports
(j) Reports on Technical Delays and Incidents
(k) Other sources: ETOPS, RVSM, CAT II/III

Laudable though these aims are, there is as yet no system in place with the capability of pulling all these highly disparate strands together to form a cohesive and truly meaningful repository of knowledge.

Finally and encouragingly, the guidance material does talk about the desirability of pooling data with others. Paragraph 9 of the document says:

"In some cases, in order that sufficient data may be analysed it may be desirable to "pool" data: i.e. collate data from a number of operators of the same type of aircraft. For the analysis to be valid, the aircraft concerned, mode of

operation, and maintenance procedures applied must be substantially the same: variations in utilisation between two operators may more than anything, fundamentally corrupt the analysis."

Regrettably, it is the use of such phrases as "may be desirable to pool data" and the clear implication that variations in utilisation may corrupt the analysis, that provides operators with a "get out of jail free" card to enable them to back away from data sharing.

In paragraph 9.4, it goes on to say:

"Where an operator wishes to pool data in this way, the approval of the Authority should be sought prior to any formal agreement being signed between operators."

The logic behind this statement is difficult to understand. Surely there should be no regulatory barriers to data sharing, which can only be for the common good?

Finally, the guidance material ends this section with the statement:

"It is acceptable that the operator participates in a reliability programme managed by the aircraft manufacturer, when the Authority is satisfied that the manufacturer manages a reliability programme which complies with the intent of this leaflet."

Yet again, the wording is hardly designed to give encouragement to any operator who is wavering over the extent of his reliability programme and distribution of his output data and reports.

4.9 RECORDING ACCIDENTS, INCIDENTS AND ERRORS

Apart from reliability programmes, which capture equipment or systemic issues in their purest form, what other information is out there that we need to have access to in order to achieve our goal of fewer accidents, and why should we do

it? Taking the last question first, the premise of what is known as Continuing Airworthiness is laid down by ICAO [56] as follows:

"All of the processes ensuring that, at any time in its life, an aeroplane complies with the technical conditions fixed to the issue of the Certificate of Airworthiness and is in a condition for safe operation."

ICAO also has a view on accident data capture, and is very specific about reporting responsibilities and so on, and rightly so, but the key message here is that all this only relates to major accidents, with a similar process for less serious incidents. Why can we not have a similarly clearly defined process for minor incidents and occurrences, to help prevent the more serious stuff from happening in the future?

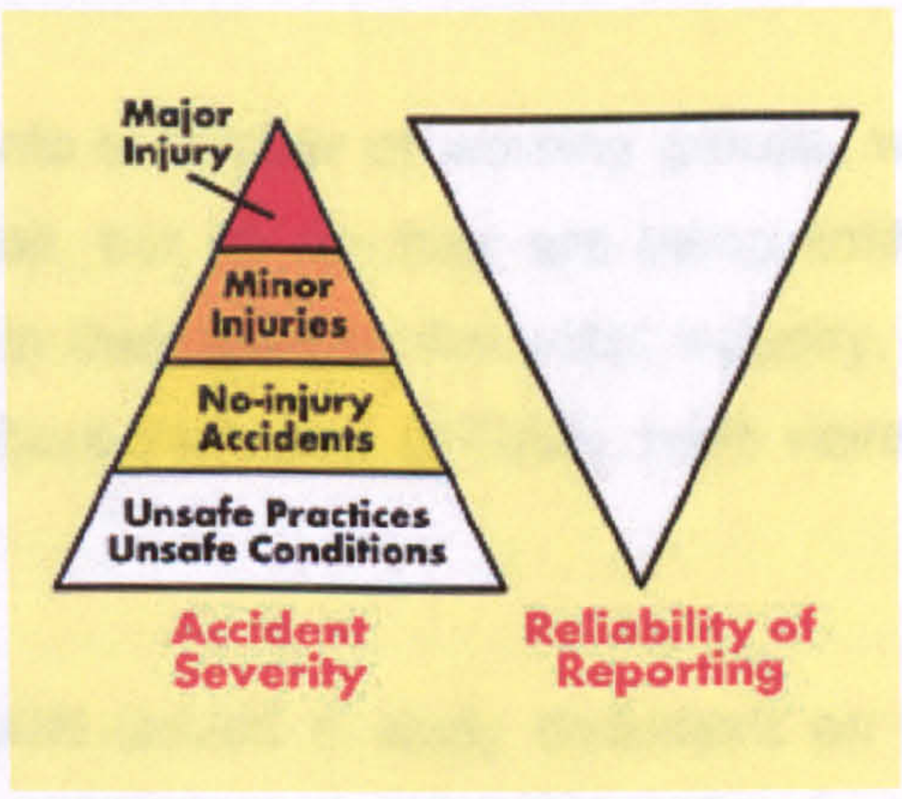


Figure 8 - Heinrich Pyramid ***(R G W Cherry & Associates)***

The Heinrich Pyramid shows that for every major accident or injury, there will be 3-5 less significant accidents, and 7-10 incidents, but there will be at least several hundred (unreported) occurrences. Adopting this pyramid for the air safety information model, an extra layer for aircraft defects can be added.

The inverted pyramid on the right shows the relative amount of information currently made readily available for each type of occurrence. A large number of occurrences are simply not reported, either because the aircraft was not damaged or delayed, and / or because none of the occupants were injured. In the majority of occurrences an unsafe situation does not occur thanks to the

safe design features already discussed, system redundancy and so on. Nevertheless, unreported occurrences may be the start of a process that builds towards a major incident or even a catastrophic accident, especially in those cases were two or more unreported occurrences coincide.

Addressing all these "lesser events" at the bottom of the pyramid should be everybody's goal, but as can be seen, this is the area where reporting is currently at its least reliable. In order to try and overcome this the GAIN was set up in 1996 to promote as the name implies, data sharing through globally accepted and accessible systems. The definition of the initiative states that:

"GAIN promotes and facilitates the voluntary collection and sharing of safety information by and among users in the international aviation community to improve safety"

GAIN is sub-divided into a number of working groups, which are studying the problem in much detail, but so far they are being limited by the amount of interest being shown in their work in the wider industry. Indeed, many airline people when asked about their view of GAIN, have never heard of it! It is the same old story, so far.

In February 2003, GAIN issued a study document on their view of the way forward in this area, entitled *How Information Sharing Contributes to Airline Flight Safety*. The document makes the point very forcibly that "not only does new information from accidents and incidents become available relatively infrequently, but an increasing proportion of accidents arise from causes that have not been previously recognized as significant hazards. Flight safety management is about managing these threats, and the first requirement is to know which threats to address. The necessity of learning from incidents with less serious consequences in order to make changes that reduce the likelihood of more serious incidents or accidents is therefore becoming widely recognised."

"The obvious, and important, benefit of sharing safety related information lies in reducing the risk of an accident through more timely recognition of previously unforeseen threats and ways to address them. While accidents are fortunately

very rare, when they do occur, they impose enormous costs on the airlines involved, not to mention the often tragic consequences to the passengers, airline personnel and third parties directly involved."

It is clear that data sharing can only aid the operators' understanding of what is going on. An airline flying a fleet of say, 50 Being 747s, is sure to have a reasonable "feel" for how well any of the aircraft systems are performing with some level of confidence in the representative nature of the statistics, even without looking outside their own operation. However, the corporate operator of a single 747 flying a low number of hours annually, and operating far removed from other 747 operators, will have great difficulty relating failure events on his aircraft in overall reliability terms that mean anything. The danger of course is that he may not fully recognise the problem and could believe that his MTBF of say 1,000 hours for an item of equipment is acceptable since he only flies 600 hours a year, whereas the rest of the world-wide fleet may be getting MTBFs many times that.

Effort continues to follow-up on operational demonstrations of a number of software packages aimed at promoting data sharing, but to date the interest level and take-up by a significant number of the world airlines is yet to start. Furthermore, the necessary links from the airlines, to and from other bodies such as the aircraft and system manufacturers, maintenance and repair organisations, the regulatory authorities, and so on, are not yet in place. Nevertheless, GAIN has issued a Concept of Operations document for a lessons learned and corrective actions sharing system, and has recently followed this up with studies aiming towards an international standard for safety event descriptor codes, a vital step forward to facilitate data sharing, and one which is addressed in more detail later in this thesis.

4.10 LEARNING FROM MAINTENANCE ERRORS

For initiatives such as GAIN to be effective requires not only widespread co-operation, but also the drawing together of many different data capture and analysis processes. These processes must be easy to use and must be operated in a good safety culture; for good read "just".

There has been much talk over the years of how to define an organisations safety culture, and even today it is still possible to hear people refer to their safety management systems as being "no blame", since that was seen as the right way to go to move away from the bad old days of "blame" cultures, when nobody would ever use an error reporting system (assuming one existed), for fear of retribution.

Blame free is equally wrong, since removal of all threats of action in the case of deliberate or malicious acts is equally devaluing to the error capture need.

One of the best and increasingly common models used today to capture maintenance error events and ensure they are learned from, is Boeing's Maintenance Error Decision Aid (MEDA).

Boeing's philosophy in developing the tool is:

"In most accidents it's the process that's to blame, not the individual worker."

Maintenance errors are thought to contribute to around 15% of aircraft accidents worldwide, and it is therefore vital that we learn from them. It is not simply a case of finding an individual's simple erroneous or negligent act and counseling them, MEDA goes far deeper than this. What we really need to discover is all the underlying contributors to the error, and with particular regard to system safety analysis, find out if there was a fundamental design flaw among those contributors, and if so fix it.

The MEDA methodology follows this logic:

- Identification of a maintenance error event
- Identification of the person or persons responsible
- Interviews to ascertain underlying causes
- Identification of corrective action – this could be manual discrepancies, erroneous maintenance procedures, poor or inappropriate resources –

both human and material – shift patterns, working hours, environmental conditions, and so on

- Implementing corrective action and measuring its effectiveness over time
- Communications all of the above to the widest possible audience

Needless to say, the final point is the one where, as we have already seen, most such systems fall down. Even assuming the operator has ensured that the rest of his team learn about the error and the fix, how about all the other operators of similar equipments? How about the aircraft manufacturer, the system supplier, the regulators; surely they should all be in the communication loop too?

4.11 FLIGHT DATA MONITORING AND OTHER EXISTING DATA RETRIEVAL SYSTEMS

One of the best-known flight data retrieval systems is British Airway's Safety Information System (BASIS), which has been around since 1990.

BASIS consists of a number of different modules as follows:

ASR - Air Safety Reporting. The ASR module is used to process flight crew generated reports of any safety-related incident and was the original BASIS module. There is a built-in risk assessment facility and the system records details of resulting outcomes and actions taken to prevent recurrence. Incidents are categorised using a reference and keyword system with the option of breaking these down further into cause and effect.

AUD - Auditing System. The audit module has been designed to store and analyse details of JAR Ops (Flight Operations, Engineering, Ground Operations) and Health and Safety audits.

CSR - Cabin Safety Reporting. For safety incidents in the cabin such as violent, abusive and/or unsafe passenger behaviour. Although designed, this part of the BASIS system has never been used.

GOR - Ground Found Occurrence Reporting. Reports raised by ground engineers which are related to aircraft safety, analysed in a similar way to ASRs generated by flight crew. As BASIS says, "Engineering Quality would normally be the main user of this system, however, there are great benefits in sharing this type of information with the rest of the airline" and indeed the other operators of similar equipment. Like other modules, GOR produces analysis charts which provide a means of identifying trends.

GHR - Ground Handling Reporting. Events resulting in damage and operational disruption.

HFR - Human Factors Reporting. Aims to facilitate identification of human causal factors behind incidents.

MEI - Maintenance Error Investigations. Identifies what maintenance errors are occurring and more importantly why; i.e. what were the contributory factors. This module derives its data from the already-described Boeing MEDA system, which British Airways helped to develop. Failed processes which should have prevented the incidents are identified. Corrective actions suggested or taken to prevent recurrence at both the local and organisational level are stored for analysis.

SIE - Safety Information Exchange. For system safety, this is one of the key modules, since users extract and send their data quarterly to IATA. The data is de-identified at source and merged into one global database which is then distributed to those users who have contributed data. The merged SIE database is sent out every quarter and contains incidents occurring during the preceding 12 months. Originally supported entirely by the BASIS team, this service is now provided by IATA under the auspices of their Safety Trend Evaluation, Analysis and Data Exchange System (STEADES). This may be partly due to the decision by British Airways in 2003 to sell off BASIS (and its on-line version WinBASIS), as it no longer represented core activity of the airline. This was seen as a concerning development, and it is to be hoped that the new owners, Mercator (part of the Emirates Airlines group), who in September 2005 re-branded the product as Sentinel, will continue the good work. They are

certainly ambitious for the product, aiming to enable direct connection between the aircraft and Sentinel using Gatelink technology, to make "web-based reporting a thing of the past" [57]. Whether this latter aim is the right one is highly debatable, since it apparently assumes that only on-aircraft data capture systems have anything to tell us. This still leaves the issue of data analysis to resolve. In a 2004 conversation with Tom O'Kane, formerly the BASIS manager at British Airways, he mentioned two particular concerns with the system. Firstly there was a large number of unexplained events waiting to be looked at, many of which could potentially hold important messages and secondly, operating environment variations should include consideration of the quality of maintenance, possibly linked to effective maintenance measures of performance as required by JAR Ops. This thesis' SSCM model has the potential to address both these issues.

STEADES is promoted as being the only global safety event database providing analysis of events, with the goal of reducing accident potential and, therefore, costs. It is based on the principles of an open, non-punitive, reporting system that is compatible with other (unidentified) reporting systems. Data loaded into the system is de-identified and analysed internally by IATA. The analysis identifies trends and areas of potential.

Currently over 45 airlines are contributing something in the order of 50,000 records per quarter, with the aim of building up to around 250 airlines over the next four years. STEADES allows daily on-line access to the analysis results through a Safety Data Management & Analysis (SDMA) website, with the facility for ad-hoc analysis requests. In addition, monthly Safety Bulletins, quarterly Safety Trend Analysis Reports and annual Safety Reports are made available to members. The most recent development is the inclusion of a Flight Data Analysis (FDA) module to satisfy the ICAO mandatory requirement for FDA programmes in place with airlines from 1 January 2005.

Promoted as having been designed for use by "anyone collecting incident data (i.e.: ground handlers, air traffic control units, maintenance outfits, regulators, etc.), STEADES currently costs IATA Members $2,500 annually. Future plans for the system include growing membership to 250 airlines by 2008, with the

ultimate aim for STEADES to interact with other systems and become a one-stop shop for safety information.

Again to quote BASIS; "The likelihood is that if one airline has experienced a problem then others will eventually experience the same problem. Hence this is a pro-active method of reviewing air safety incidents, before they happen to you. Even if you have already experienced the same problem, the SIE database is a powerful source of information when trying to convince others that your airline's incident is not an isolated case. Also such a database allows small fleet operators access to safety information from a much larger fleet database."

The first question is, how many airlines have taken up the cause and subscribe to the BASIS/Sentinel/STEADES systems? The second question is, once again, who else sees the data outside the airlines?

Finally, there is the European Co-ordination Centre for Aviation Incident Reporting Systems (ECCAIRS). This initiative was designed to facilitate European Union member states' efforts in collecting and exchanging information on incidents and accidents in civil aviation, through a collaborative network of civil aviation authorities, accident investigation bureaus and others. The intent was to improve and standardise analysis tools and methods for implementation in the 2004 to 2006 time period. However, laudable though this initiative is, it is primarily focused on reportable accident and incident data, and thus the many lower level events which are just as important in understanding reliability and safety performance are unlikely to be addressed.

4.12 HUMAN FACTORS – THE MISSING PART OF THE EQUATION

Almost a mantra today, the term "human factors" has become inextricably linked with the air safety challenge. Of course it is a vital link in the chain of failure events, and must therefore be properly understood and quantified, which is primarily where this problem still rests. To again quote Charles Perrow [58]:

"It is indeed the case that people sometimes do really stupid things, but when most of the accidents in a particular type of system (airplane, chemical plant,

etc.) are blamed on the operator, that is a symptom that the operators may be confronted with an impossible task, that there is a system design problem. In a typical normal accident, the operator's actions may contribute to the problem, or even initiate the sequence of events, but the characteristics of tight coupling and interactive complexity also make their contributions."

4.12.1 A Regulator's View

In May 2001 Hazel Courteney, head of the CAA Human Factors Group presented a paper at a Royal Aeronautical Society (RAeS) safety seminar [59], which gave an interesting insight into the way in which the regulators are now considering human factors in aviation safety. To quote from the introduction:

"It is no longer news to say that crew error is the most common causal factor in aircraft accidents. In fact, human errors would probably account for all but a handful of accidents if the definition were extended to errors in air traffic management, aerodrome support, aircraft maintenance, production, design, organizational management and so on. Human error is our single biggest safety risk. Yet, despite this awareness, and the current high profile of 'human factors' in the industry, the issues remain cloudy, much debated and unresolved."

Although regulations aimed at specifically addressing human factors are still in their infancy, some indicators are already apparent. The JAA has adopted an interim policy entitled *Human Factors Aspects of Flight Deck Design* with particular relevance to projects that introduce novel items to the flight deck. The document continues detailed guidance about what is regarded as novel, including new uses or procedures for existing technology.

Two of the Special Conditions listed in the policy are of especial interest to the safety analyst:

1. "The effects of crew errors in managing systems, including the potential for error, the possible severity of the consequences, and the provision for recognition and recovery from error."

2. The adequacy of feedback, including clear and unambiguous:
    - presentation of information
    - representation of system condition by display of system status
    - indication of failure cases, including aircraft status
    - indication when crew input is not accepted or followed by the system
    - indication of prolonged or severe compensatory action by a system when such action could adversely affect aircraft safety

Consequently, the CAA has gone on to issue a draft regulatory document entitled *Preliminary – Notice of Proposed Amendment 25.310 Human Centred Design* [60]. The central theme of the proposal is that all aspects of an aircraft design should embody a certain level of resistance to human error. The key paragraph states:

"It must be shown by analysis, substantiated where necessary by test, that as far as reasonably practicable all design precautions have been taken to prevent human errors in production, maintenance and operation causing Hazardous or Catastrophic effect. Where the potential cannot realistically be eliminated, then the remaining safety critical tasks should be sufficiently understood and the potential for human error mitigated."

4.12.2 Response From Industry

This far-reaching proposal has the potential to have a major impact on the way in which the aerospace industry currently conducts safety analysis. The initial response to the CAA called for agreement on an Acceptable Means of Compliance, as a result of which the CAA is researching a draft method of Human Hazard Analysis (HHA). The principle will be to systematically identify items where a safety risk could arise from human error, and then demonstrate to the certification authority how the risk has been mitigated. The CAA sees the inclusion of human error base events in system fault tree analysis as the primary tool to achieve this.

To date industry has rarely addressed human factors issues in such analyses. The challenge with this approach is going to be establishing supportable probability of occurrence rates for human factor events. As has already been discussed, we live in a far from ideal world already with regard to obtaining good equipment failure probability data; it is infinitely more difficult to assign realistic probabilities to human factors events.

The problem is that although the identification of the actual events is relatively straightforward, e.g. mis-assembly, incorrect alignment, incorrect procedure, and so on, such events are the result of a combination of factors, including time of day, stress levels, time pressure, resources, distractions, skill level, the list is almost endless.

In the total absence so far of any meaningful guidance in this issue, some system designers are now adopting a philosophy that the risk from human error is always assumed to be less than 1×10^{-9} and therefore can be discounted from the safety assessment. This is a very dangerous path to tread; on what basis was that assumption made? No-one yet has the answer.

4.13 EUROPEAN UNION AND OTHER LEGISLATION

As the European Union (EU) moves increasingly into legislative matters across the member states, movement is particularly evident in the area of transport.

4.13.1 European Aviation Safety Agency

In the autumn of 2002 the European Union officially brought the European Aviation Safety Agency (EASA) into being. What is EASA, and what bearing does it have on the problem of aircraft system safety?

In the 1990s, there was a general agreement between the JAA members that the authority needed a more formal and legally binding status. Accordingly, a working group was set-up, which developed a possible text for a JAA Convention outlining the framework of a formalized air safety agency, and it received an agreement in principle from the JAA Board in 1995. However, it

was not developed any further at that time, as some JAA members felt that co-ordination with the European Union was necessary.

In 1997 the European Union started discussing a proposal from the European Commission for the establishment of a European-based organisation responsible for civil aviation safety. In June 1998 the Council of the EU Transport Ministers accepted the general concept for EASA, and agreed that it will be responsible for rulemaking, certification and standardisation for the application of rules by the national aviation authorities, such as the UK CAA.

The Council asked the European Commission to prepare negotiations for an international convention to establish EASA together with non-EU members. In December 1999 the Council discussed the draft documents for EASA and an alternative concept for an EU Aviation Safety Agency presented by the European Commission. It was decided to explore both concepts further, but in the meantime the European Commission developed and agreed a draft regulation for the creation of EASA, and ultimately the alternative proposal was shelved. As part of the implementation of EASA in 2002, the JAA has developed an Agenda for Change and this is now being implemented step by step into the JAA system.

EASA is now the legislative body for all aviation safety matters within the JAA member states, and over the next ten years or so, EASA Implementing Rules (IR) will gradually replace JARs. Early work by EASA includes airworthiness issues encompassing the question of aircraft and systems safety.

The overall transition programme for EASA to take over the safety regulation functions of the present central JAA will last some 42 months from the September 2003 start up date. This will cover the relevant detail agreements with all the JAA National Aviation Authorities (NAAs) for transfer of specific safety functions to the EASA, any delegated functions to specific NAAs with appropriate expertise, and completion of the preparation and promulgation of the present JARs into relevant EU regulatory material. The EASA Regulation is only binding on the 25 EU member states; it is therefore essential that a method is found for the continued participation of the other non-EU states that are part

of the present JAA. The stated main objectives are to avoid safety gaps, to assure the present safety achievements continue to be built upon, to ensure maximum smoothness in the transition process with particular reference to the impact on Industry, and to ensure that non-EU states continue to participate in Pan-European mechanisms, which provide for co-operation at the highest level on European Aviation Safety.

It has been emphasised that the commitment of the EC to abide by the ICAO Standards is clearly and repeatedly stated in the EASA Regulation. The Member States are acting collectively, using the EC processes, to fulfill their obligations enshrined in international treaties, in particular the Chicago Convention."

EASA themselves, in their formative documents, have stated that:

"The principle of certification of aircraft, organisations and personnel is established. The same principle also applies to third countries, while respecting their rights specified in the applicable international Conventions."

"The essential airworthiness requirements which products and appliances must meet in order to be certified are those contained in Annex 8 to the Chicago Convention, which is annexed to the proposal. The Commission is empowered to adopt, by a committee procedure, any additional rule for application of these requirements."

Thus it can be seen that EASA is focusing immediately on the safety of aircraft and their systems, and this view has been reinforced by the issuing in June 2003, of a draft Consultation Document [61], ultimately leading to a Commission Regulation laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations. The most important statements within this document are:

"The Basic Regulation establishes common essential requirements to provide for a high uniform level of civil aviation safety and environmental protection; it

requires the Commission to adopt the necessary implementing rules to ensure their uniform application; it establishes the "European Aviation Safety Agency" to assist the Commission in the development of such implementing rules;"

"It is necessary to adopt common technical requirements and administrative procedures to ensure the airworthiness and environmental compatibility of aeronautical products, parts and appliances, subject to the Basic Regulation; such requirements and procedures shall specify the conditions to issue, maintain, amend, suspend or revoke the appropriate certificates."

"In adopting measures for the implementation of common essential requirements in the field of airworthiness, the Commission must take care that they reflect the state of the art and the best practices, take into account worldwide aircraft experience and scientific and technical progress."

"The need to ensure uniformity in the application of common airworthiness and environmental requirements for aeronautical products, parts and appliances calls for a common approach and measures to be followed by the competent authorities of the Member States and, where applicable, the Agency in order to assess compliance with these requirements; consequently, the Agency must develop certification specifications, including airworthiness codes and acceptable means of compliance to facilitate the necessary regulatory uniformity."

In any event, it is not expected that any newly formulated EASA legislation will be on the statute books until 2006 at the earliest. As EASA evolves, the JAA will fade away from its legislative status to become an advisory body, much like the national aviation authorities, but as yet, its future is still unclear.

4.13.2 Directive On Occurrence Reporting

In September 2001 a proposal for a Directive of the European Parliament and of the Council on occurrence reporting in civil aviation was published [62]. It was intended as a follow-on to Council Directive 94/56/EC dated 21 November 1994, which established the fundamental principles governing the investigation

of civil aviation accidents and incidents by "facilitating the expeditious holding of investigations."

The 2001 proposal (since adopted), recognised that before an accident occurs, a number of incidents and other deficiencies have shown the existence of safety hazards, and that safety improvement requires a better knowledge of these occurrences to facilitate analysis and trend monitoring in order to initiate correct actions. It said that each EU member state **should** set up mandatory reporting systems, and that occurrences of interest **should** be reported by various categories of personnel working in civil aviation.

However, although it clearly recognised that "the efficiency of detection of potential hazard would be greatly enhanced by the exchange of information", it then went on to back away from legislating the fullest possible dissemination of information. Article 7 of the proposal states:

"Any entity entrusted to regulate civil aviation safety or to investigate civil aviation accidents and incidents within the Community shall have access to information on occurrences collected and exchanged...to enable it to draw the safety lessons from the reported occurrences."

"The Commission may...decide on the release of selected information to...other interested parties. Such decisions..shall be based on the need to:

- provide persons and/or organisations with the information they need...or
- allow the analysis of occurrences by bodies specialised in aviation safety"

"The decision to disseminate information shall be limited to what is strictly required for the purpose of its user. The recipient of information shall in turn commit itself not to disseminate the information further."

Annex 1 of the proposal lists examples of reportable occurrences, and at system level it is especially well written, leaving little scope for omission of almost any event under the proposed mandatory reporting scheme. However,

the damage has been done in article 7, which leaves the limits of the dissemination of information and thus the overall usefulness of the entire proposal to the aviation industry at large. If, as seems likely, the proposal becomes legislation in its current format, it represents a brave attempt, but still a missed opportunity.

In the United States, the FAA issued very similar legislation as Advisory Circular (AC) 120-66B dated 11 November 2002, as part of their Aviation Safety Action Programme.

4.13.3 International Civil Aviation Organisation

In 1999, ICAO proposed changes to strengthen the wording of Annex 6, Chapter 3 of their regulations, which now state that:

– "From 1 January 2002, an operator of an aeroplane of a certified take-off mass in excess of 27000 kg **should** establish and maintain a flight data analysis programme as part of its accident prevention and flight safety programme."

- "From 1 January 2005, an operator of an aeroplane of a maximum certified take-off mass in excess of 27,000 kg **shall** establish and maintain a flight data analysis programme as part of its accident prevention and flight safety programme."

ICAO followed up this encouraging change in the arena of Flight Data Monitoring (FDM), in June 2002 with the adoption of Resolution A33-16: ICAO Global Aviation Safety Plan (GASP). This recognises that improvements in the air accident rate will require new approaches, in particular pro-active and risk analysis based approaches, on the part of all participants in the aviation industry, including ICAO, States, aircraft manufacturers and operators.

Operative clauses 8, 9, 10 and 11 of Resolution A33-16 read as follows:
"8. *Instructs* the Council and Secretary General to participate in efforts by States to improve existing safety database systems and the exchange of safety-related information, and to participate in activities aimed at the development of a

comprehensive data analysis and information dissemination network, taking into account the need to adequately protect privileged information and its sources;

9. Encourages the free communication of safety-related information amongst users of the aviation system, including the reporting of accident and incident data by States to the ICAO Accident/Incident Data Reporting (ADREP) system;

10. Urges all Contracting States to examine and, if necessary, adjust their laws, regulations, and policies to achieve the proper balance among the various elements of accident prevention efforts (e.g. regulation, enforcement, training, and incentives to encourage voluntary reporting) and to encourage increased voluntary reporting of events that could affect aviation safety, and *instructs* ICAO to develop appropriate policies and guidance in this respect; and

11 - Urges all Contracting States to ensure that their aircraft operators, providers of air navigation services and equipment, and maintenance organisations have the necessary procedures and policies for voluntary reporting of events that could affect aviation safety."

A note at the beginning of Annex 13 Chapter 8 reads as follows:

"The objective of these specifications is to promote accident prevention by analysis of accident and incident data and by a prompt exchange of information."

Chapter 8 addresses one of the main aspects of an accident prevention programme, namely, incident reporting systems, database systems, the analysis of safety data, and the exchange of safety information.

To address the need for incident reporting systems, Standard 8.1 in Annex 13 requires States to establish a mandatory incident reporting system to facilitate the collection of information on actual or potential safety deficiencies. In the previous edition of Annex 13, this provision was a Recommended Practice only.

Finally, a new Recommended Practice (8.2) has been introduced concerning the establishment of voluntary incident reporting systems to supplement the mandatory systems.

"The pursuit of aviation safety worldwide requires that safety lessons learned through accident investigation, the analysis of information from incident reports, or by other means, be disseminated as widely as possible."

4.13.4 JAR39 Airworthiness Directives

Advisory Circular Joint 39.3 of JAR39 Airworthiness Directives, discusses the sufficiency of corrective action when addressing defects. The status of this document is quoted as being:

"Not intended to be regarded as binding in specific cases, but, by being used in conjunction with engineering judgement, to aid airworthiness engineers in reaching decisions in the state of technology at the material time."

The document recognises the variation in airworthiness risk levels due to such factors as environmental conditions, variations in material standards, design deficiencies and unforeseen combinations of failures, etc.. It also recognises the need to attempt to monitor conditions tending to increase risk levels. It then goes on to set out a set of guidelines for defect rectification campaigns. However, in addition to its non-binding status, the document simply identifies the overall process for identifying defects, recognising variance and taking corrective action. In other words, it essentially describes the already well-established FRACAS-type system, without giving details of a methodology such as that which is proposed within this thesis.

4.14 SUMMARY OF THE PRESENT SITUATION

The safety assessment process is now very well defined, particular within such references documents as ARP 4761. Other interfacing procedures are also generally acceptable, but the problem remains the lack of legislation to back them up. This is now also noticeable in the efforts to establish event reporting systems to back-up the design analysis.

Hopefully, the emergence of agencies such as EASA will help to force a wider adoption of the right procedures through legislation. However, in many areas

legislation on its own will not work, since the right tools and the back-up support infrastructure are not necessarily all in place.

4.15 AREAS TO BE ADDRESSED FOR ACTION

The International Federation of Airworthiness (IFA) recently published a White Paper entitled *Continuing Airworthiness – The Basic Story* [63]. This attempts to lay out in a clear and concise fashion the continuing airworthiness requirements and control functions and the complex ways in which they all interact. Responsibilities are defined under five main agencies, with their principal areas of concern regarding system safety, highlighted below:

- ICAO – issues international Standards and Recommended Practices (SARPs), and technical guidance publications
- State Regulatory Authority (Agency) – issues aircraft/engine type certificates; requirements for occurrence reporting, analysis and feedback schemes. Approves maintenance/reliability programmes and ageing aircraft and systems programmes. Establishes state occurrence reporting, analysis and feedback schemes. Audits and monitors certification, AOC and Maintenance and Repair Organisation (MRO) standards
- Certified Air Operator / Carrier (Air Operator Certificate [AOC] holder) – establishes maintenance/reliability programmes and occurrence reporting, investigation and follow-up scheme
- Approved Certification Organisation (OEM) – prepares and controls safety assessments and analyses, type certificates and type certificate data sheets. Establishes occurrence reporting, investigation and follow-up scheme (i.e. FRACAS). Issues safety and guidance information for products
- Approved Maintenance Repair Organisation (MRO) – controls maintenance/reliability programmes. Establishes occurrence reporting, investigation and follow-up scheme. Implements ageing aircraft structural and systems programmes

This all clearly shows the level of responsibility for various aspects of the aircraft system safety performance programme. However, it also exposes the holes in both the spread of responsibility and in the current safety legislation.

There can be no "magic bullet" to correct all the issues surrounding aircraft system safety analysis. It is also fair to say that there are many very worthy initiatives under way to try and improve the situation already. Yet still there is a need for a fundamental shift in both the basic analytical methodologies and the "learning from the past" systems the air transport industry currently has in place.

As a result of the situational review carried out in the preceding chapters, a number of areas for action have been highlighted in this chapter. These should be taken simply as – in some of the cases - a first step along a very long road towards the overall aim of maintaining a necessary focus on aircraft system safety issues throughout the system life-cycle. The key issues have been taken further and developed into a detailed proposal for a new process, which is discussed in chapter 5.

By far the most important issues to emerge are:

1. A legislative shortfall which allows the continuation of unsatisfactory safety analysis processes
2. The failure to recognise the need to benchmark reliability databases to replace obsolete references and provide a global safeguard for design safety margins.
3. An absence of clearly defined links between the many initiatives emerging in the arena of in-service event data capture and the equipment and system manufacturers
4. A critical shortage of engineers with the necessary skills and expertise to properly address system safety analysis in all its forms
5. An appalling lack of understanding and appreciation of the need and long-term cost-effectiveness of correct and educated design analysis within many sectors of the manufacturing industry

The proposals are broken down into five main areas, covering:

- The fundamental safety analysis process
- Source data from reliability databases
- Learning the lessons from service experience
- Training our safety practitioners
- Educating the aviation industry at large

4.15.1 A Mandatory Safety Analysis Process

It has been shown that while a fundamentally sound process (ARP4761) already exists for much of the system safety analysis work, the main problem is that the regulatory authorities do not mandate its use. The regulators require demonstration of safety performance by analysis and test for example, but stop short of requiring each step in ARP4761 to be followed.

The most concerning issue here is that this approach allows the manufacturers to perform only as much of the ARP4761 work as they have to in order to demonstrate compliance, and thus see any additional effort, such as independence in the safety assessment process, as an un-necessary "cost plus". Many companies have thus disbanded their traditional reliability and ILS departments who used to perform this work, and either have their design teams (who are not trained safety analysts) do it, or contract it out to specialist ILS / safety analysis companies. While the latter option at least ensures that the people performing the work are familiar with the tools, it does remove the immediacy of not being in the same building as the design, manufacturing and test teams, thus losing the ability to gain a clearer understanding of day-to-day issues and the background to design assumptions and decisions.

So how can these problems be overcome? One solution might be to digitise the FAR / JAR 25.1309 and individual system FHA requirements in a format that can be readily and instantly cross-checked by designers, or better still, the independent analysis team. This would be quicker and potentially more cost-effective in building a safety case that can ensure design compliance both automatically and iteratively.

Perhaps there should be a joint FAR / JAR / EASA safety analysis process requirement as a replacement for ARP4761, issued and mandated by both the FAA and EASA? This might take the form of a straight-forward adoption by EASA and the other agencies of an updated ARP4761. For example, it is known that Airbus is working on a new system based on a starting point of identifying all the aircraft system's *safe* states and then looking at how it might fail, rather than the traditional failure and consequences approach.

4.15.2 Revised Equipment & Component Reliability Databases

It is absolutely essential that the continued use of MIL-HDBK-217F and NPRD 95 (at least) be brought to a halt at the earliest possible date, preferably through legislation. Realistically though, this cannot happen until there is something to replace them. The ideal of course, is empirical data, but until such time as the system described in chapter 5 has been fully implemented, another course of action needs to be found.

The regulators should change the requirements of that section of the safety case that calls for failure rate justification, such that claims for the use of MIL-HDBK-217F and NPRD 95 failure rates alone will not be accepted. Where these sources are claimed, the manufacturer must give justification for not using another more robust database, or empirical data. Only this kind of approach will drive people away from continuing to rely on hopelessly out-dated and inadequate data when performing a preliminary reliability assessment which may well stay with the aircraft for the next thirty years.

4.15.3 Industry-Wide Event Analysis And Lessons Learned Systems

Remember the words of the FAA's *Commercial Airplane Certification Process Study* discussed in the previous chapter;

"Adequate processes do not exist within the FAA or in most segments of the commercial aviation industry to ensure that the lessons learned from specific experiences in aircraft design, manufacturing, maintenance, and flight

operations are captured permanently and made readily available to the aviation industry. The failure to capture and disseminate lessons learned has allowed aircraft accidents to occur for causes similar to those of past accidents."

And:

"There are constraints present in the aviation industry that have an inhibiting effect on the complete sharing of safety information."

Firstly, let us return to the GAIN initiative, and take a detailed look at their action plan [64] as it affects the area of system safety. The plan, which was divided up into a number of main areas, is unfortunately currently stalled due to withdrawal of FAA funding from GAIN. However, those areas of most immediate concern here (and there are many) include:

"1. Foster the use of existing analytical methods and tools and the development of new methods and tools. Sub-tasks include:

- Gather requirements for analytical methods and tools from the aviation user community
- Conduct detailed analysis of the Survey of Analytical Processes and Requirements for Airline Flight Safety Management to refine requirements for analytical methods and tools.
- Define a hierarchy of analytical tools needed for an airline flight safety office.
- Continue to add analytical methods and tools to the GAIN website addressing flight safety, air traffic system safety, airline maintenance safety, and ramp safety.
- Assess the usefulness and usability of existing tools in partnership with the aviation user community
- Work with several airlines at their facilities to gather practical experience in the use of analytical methods and tools with airline data and document lessons learned.

- Partner with several airlines and/or airline organisations to demonstrate the use of data mining or text mining tools for the analysis of safety event reports.
- Facilitate the development of enhanced or new analytical methods and tools
- Explore issues involved in linking and merging data in airline internal safety data bases (e.g. FOQA and ASAP), and identify requirements for new or enhanced tools to support this capability.
- Facilitate the use of analytical tools and services in the aviation community
- Identify and document the appropriate skill set and/or staff mix needed by flight safety offices and/or airline organisations to perform safety analysis.

2. Promote and facilitate the development and implementation of systems to support the global sharing of aviation safety information. Sub-tasks include:

- Facilitate the development of systems to share airline safety event information among trusted groups in near-real time
- Facilitate the on-going work on two systems for exchanging Standard Sharing Reports (SSRs) containing proprietary information on safety events among airline safety managers in near-real time.
- Develop an integrated plan to demonstrate the airline safety event sharing system prototypes and assist the airline safety officers in the monitoring and documentation of the results of the demonstrations.
- Solicit additional airlines to join the prototype sharing systems (alliance members, air carrier and commuter groups, and regional associations).
- Develop standard or operating protocol for sharing airline safety information.
- Facilitate the development of training materials for airline safety officers to improve the usefulness and usability of these sharing systems.
- Promote aviation industry sharing systems
- Identify "automated" aviation safety information sharing activities throughout the world and document approaches used in organising and operating each activity.

- Promote data standardisation among these "automated" aviation safety information sharing activities.
- Facilitate the development of a system to share safety lessons learned and corrective actions within the aviation community
- Gather requirements for a system to share safety lessons learned and corrective actions from target user community, with initial focus on airline flight operations.
- Develop and demonstrate a prototype system for sharing safety lessons learned and corrective actions among airline flight operations.
- Promote and facilitate the voluntary, non-punitive collection and sharing of safety information among the worldwide aviation community
- Identify and increase awareness of current and planned government safety information collection and sharing programmes.
- Promote the establishment of voluntary safety information sharing networks among all users of the aviation system and facilitate the free exchange of information on actual and potential safety deficiencies.
- Identify examples of collaborative processes that airlines and governments have initiated to determine lessons learned from safety information.
- Help reduce legal and organisational barriers that discourage the collection and sharing of safety information
- Encourage government and industry organisations to establish safety management systems that emphasise the importance of non-punitive collection, analysis and sharing of safety information within their organisations."

Let us look closer at one of these GAIN initiatives, which is for a Standard Sharing Report for use in airline Safety Management Systems. This maps the proposed data fields for effective incident capture and analysis and is designed to permit an airline safety officer to determine at a glance if an event report is of interest to a particular issue.

The fields listed are:

- Event Date YYYY/MM DATE

- Aircraft Manufacturer
- Aircraft Model Type - e.g. 737, A320
- Aircraft Master Series Model - e.g. 737-700
- Event Category – a limited list of 10 categories is proposed
- Event Type – a standard comprehensive list covers over 200 events
- System Involved - ATA code
- Phase of Flight - based on CAA standard
- Airport Location - ICAO or IATA codes
- Weather Condition (if pertinent)
- Environment
- Event Description
- Probable Cause
- Corrective Action - Actions taken to reduce future risk
- Recommendations

The more detailed parts of the proposal include:

"Section 145.221 Reports of Failures, Malfunctions, or Defects

Repair stations are required to submit reports of defects or unairworthy conditions to the FAA. The FAA proposes to standardise the type of data reported under the service difficulty reporting system by specifically listing the information required when a repair station submits a report.

Section 145.63(b) states that in cases where filing a report of defects or unairworthy conditions might prejudice the repair station, the repair station shall refer the matter to the Administrator for a determination as to whether a report is necessary. "

One commenter on the proposals stated that it constituted an invasion of privacy. Other commenters opposed including the name and address of the operator in the report, because the report already includes the aircraft registration number, which can be used for obtaining the other information. Another stated that the rule should be expanded to include all part 145 certificated repair stations.

"The estimated safety benefits, being difficult to quantify, are calculated based on what the reduction in accidents needs to be in order to equate the discount costs to the discounted safety benefits. If the safety benefits are half of those discussed in the initial regulatory evaluation (6.9 hull loss accidents will be avoided, including general aviation), then the quantifiable safety benefits of the final proposal will be approximately, $28.5 million in current dollars discounted at 7 percent, over 13 years. On an annual basis (assuming that quantifiable benefits are only one-half of those estimated in the initial regulatory evaluation) an average of 3.4 total accidents will be avoided.

The estimated net cost of compliance after subtracting cost savings with the final amendment will be $22.2 million (net of cost savings) in current dollars, discounted at 7 percent, over 13 years. The most costly requirement, section 145.161, Training Requirements, will result in repair stations incurring discounted costs of $30.5 million. The most cost-saving requirement, the Manufacturer's Service Manual, will result in repair stations saving between $22.8 and $45.5 million discounted.

The final rule is not expected to have a significant impact on international trade nor is it expected to have a significant impact on a substantial number of small firms."

4.15.4 The French View

Some years ago, the French Civil Aviation Authority, Direction Générale de l'Aviation Civile, (DGAC), produced a report entitled *Development of a Methodology for Operational Incident Reporting and Analysis Systems* [65] which examined existing methodologies for incident reporting and data analysis. The report took as its starting point, the perception that there were a lot of databases around the aviation world, being fed with a lot of data, but that data was not being put to effective use, as data alone cannot identify problems. What was needed was a better appreciation of the substantial amount of potentially useful information that incident data can provide and how to process it.

Therefore, the DGAC issued a call for a research study aimed at the development of a methodology for Operational Incident Reporting & Analysis Systems (OIRAS), which resulted in the above report. A number of existing incident databases were reviewed for their effectiveness, and none was found to be entirely satisfactory. The main areas of shortfall were identified as:

- In order to ease data retrieval, there needed to be categorisation of the raw information. This is most problematic with subjective descriptions of an event and its causal factors
- It was impossible to anticipate all possible contingencies, therefore it was also impossible to create an exhaustive list of keywords. Furthermore, since keywords are either present or not present, and can only be combined in a linear fashion, this becomes an unsatisfactory representation of the real situation
- Information is retrieved in the form in which it is entered, so categorisations derived by the analyst defines the output parameters. For example, if there is no "bearing failure" in the database category list, then "bearing failure" can never be found to be a cause of incidents during a database search. Therefore, the safety model which guided the categorisation can only confirm or deny what is already known, nothing new
- A large amount of data is never retrieved once it is entered. Was it relevant in the first place? Of course it was, but the retrieval protocols are not robust or flexible enough to either find that data or recognise its value.
- When a keyword search does identify a case, the analyst usually has to go back to the original report to understand all the details in context
- Once a database grows beyond the memory of the analyst, it becomes a data store, and with consideration of the previous point, potentially important data and lessons are in essence "forgotten".
- The keyword structure acts to bias output reports to fit the established keywords. The danger here is obvious – data which does not fit the keyword structure or other search criteria, may be ignored.

In their report summary, the DGAC team stated that:

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

4.15.5 Other Databases

There are several Internet databases available, either hosted by accident investigation authorities or by independent websites. The NTSB database is by far the best publicly available one since all NTSB investigated accidents and incidents that have occurred since 1983 can be searched (there are over 46,000 records).

The FAA Incident Data System is also available on-line and contains almost 80,000 events that occurred between 1978 and the present time. The search interface is however very basic, and the presentation of the search results is poor. The information on each occurrence is quite detailed, but lacks a description of causal factors.

A major problem with these and other databases, is that they can only be searched separately, there is no cohesion or attempt to make them interface with each other. An initiative attempting to address this problem is the

European Co-ordination Centre for Aviation Incident Reporting Systems (ECCAIRS) project, which aims to integrate information from aviation occurrence reporting systems running in the authorities of the various EU member states. This project started back in 1993 and has not yet been fully implemented.

Similarly concerned with how little is currently being learned from operational feedback, Airbus has, since 1999, been developing a new system intended to learn more from less data. Using data from Air Safety Reports, incident reports and so on, the Airbus "ERASM" model is still undergoing trials and it may be some time yet, if at all, before it results in a commercially available product.

Of course the fundamental difficulties with this whole issue of industry-wide data sharing, remain:

1. Who owns the database?
2. Who pays for it?
3. Who has access to it, both for input and for data analysis?
4. How can the industry as a whole be persuaded to use it?

These points are addressed in Chapter 5.

4.15.6 Flight Data Monitoring

With effect from 1 January 2005, the use of Flight Data Monitoring (FDM) procedures was mandated by the JAA for all European operators of aircraft over 27 tonnes. A parallel programme was introduced in the United States where it is known as Flight Operations Quality Assurance (FOQA). New technologies, such as data fusion techniques to automatically link different data types, and data mining techniques, are making the collection, analysis and presentation of such data more useful.

However, data analysis and therefore monitoring, comes at a cost in terms of finance, infrastructure and manpower resources. The fact that not all airlines

have data monitoring programmes, lends credence to the notion that there is a commonly held concern that the cost benefit of such a programme would be minimal or unquantifiable.

"Evidence is available to prove that airlines which have been using FDM data for 7-14 years now have a lower accident rate than US airlines, and those airlines which have used FDM for more than 14 years, have an accident rate under half that experienced by US carriers." [66]

"In competition for scarce resources within an airline, FDM programmes need to go through the same cost justification process as any other programme. While there are clear and compelling benefits for an FDM programme to identify and reduce operational risks, they are often difficult to quantify. Airlines with FDM have indicated that as they become more familiar with the programme, they have discovered uses of the data that have resulted in extended engine life, more efficient routings, and in saving money in other areas. These improvements, coupled with safety enhancements, have been determined to more than justify the cost of implementing an FDM programme. The one cautionary note is, however, that without the correct management of data quantity and quality, not only will airlines input and receive 'garbage' from their FDM programmes, but they will also possibly jeopardise their relationship with their employees." [67]

4.15.7 Training Safety Practitioners

In the United Kingdom, some independent ILS / reliability companies run short-course training for safety practitioners, and Cranfield University has for many years offered a very popular one week course on the safety assessment of aircraft systems. These initiatives are to be applauded, but they only scratch the surface.

As can be seen, system safety analysis is a complex subject, and that in itself is part of the problem preventing its fuller adoption by industry. It is viewed with suspicion as a "black art", primarily through a lack of understanding not just of the need to perform the activity properly, but also of the benefits it can bring. What is required is a much broader and deeper range of education options to

compliment what we already have, including courses offering Certificate, Diploma and Degree level qualifications for safety professionals. In addition, the Air Transat A330 incident mentioned in section 4.7, and other cases of poor systems understanding, suggest that some kind of system safety overview training for pilots and maintenance engineers would be highly beneficial.

As part of the more detailed safety analysis training, more emphasis needs to be given to moving away from the still common practice of basing reliability figures on the mean. What consideration should be given to variance driven by operational, environmental and ageing factors, not to mention the human interface? How does all this potential for variance in the numbers affect safety requirements compliance, particularly when the system is only marginally compliant when mean figures are used?

There are many potential sources of quantitative variation in analyses. One form is classical variability, which is applicable to first-principle-based problems. Another form is subjective uncertainty, which means that available data or models are not definitive enough to prescribe variability, thereby requiring alternative processes to consider what might be possible.

What is required is an appreciation of the need to combine basic reliability data and physical elements with engineering judgment, while still producing results that are both understood and traceable.

"There is a tendency to misunderstand the role of the PSSA, assuming that it provides positive proof that the proposed design is safe, rather than the intention of the process, which is to say that the design can be safe if the component parts of it are implemented correctly" [68]. Yes, PSSA is vital, but it is just the first step on a long road.

Within manufacturing companies, different engineering discipline teams tend to be isolated from each other, only interfacing once their work packages are complete. This is nonsense of course, and often means that problems are often found either too late in the process to make a difference at all, or too late to make a difference in a cost-effective manner. It is up to the system safety

engineer to provide the day-to-day link with other engineering (and commercial) groups and thus prove that the whole independent element is a legitimate one.

Without the right numbers of safety engineers, who have received the proper level of training, convincing industry to fully adopt this approach is always going to be an uphill struggle.

4.16 EDUCATING THE INDUSTRY

Of course everything that has been proposed up to this point may sound relatively easy, but without "buy in" from the aviation industry, there will not be any motivation for change. Although everyone in the industry says safety comes first, the reality is that safety remains a trade-off, especially in the current climate of extreme financial constraint throughout the world airline industry.

Thus it is vital that attempts to introduce a greater awareness of the system safety issues – in other words instilling a culture of really meaning safety first – must be able to show the benefits to the industry of doing so, or indeed of failing to do so. The case studies discussed earlier, while being extreme in that many of them resulted in catastrophic accidents, nevertheless do show that the aircraft manufacturers in particular, have been forced to spend a considerable amount of time, money and resources, all of which are increasingly scarce in today's cost-conscious world, fixing problems that would not have been there if the design had been correct in the first place. Not only that, but if the problems manifest themselves early on in the equipment's in-service life, the manufacturer also gets hit by the additional cost of warranty claims from the operator who is suffering from the equipment performance fall-down.

Similarly with the airlines and maintenance organisations, increased frequency of both scheduled and unscheduled maintenance due to both initial design flaws and a poor understanding of in-service event issues, will lead at the very least to increased Direct Maintenance Cost (DMC) and thus Direct Operating Cost (DOC).

4.17 SUMMARY

It has been shown that attention needs to be paid to correcting flaws in the fundamental safety analysis process, the use of source data from reliability databases, the way in which we learn the lessons from service experience, how we currently train our safety practitioners and educating the industry in the need for better system safety.

Each of these areas demands its own set of initiatives, but this document goes on to take one major aspect of the procedural problem and develop it in a totally new direction. In order to better understand this, the current safety analysis system is shown in the following sequence of diagrams, which build on each other to illustrate the total system and the flaws currently embedded within it.

4.17.1 The Present Analytical System

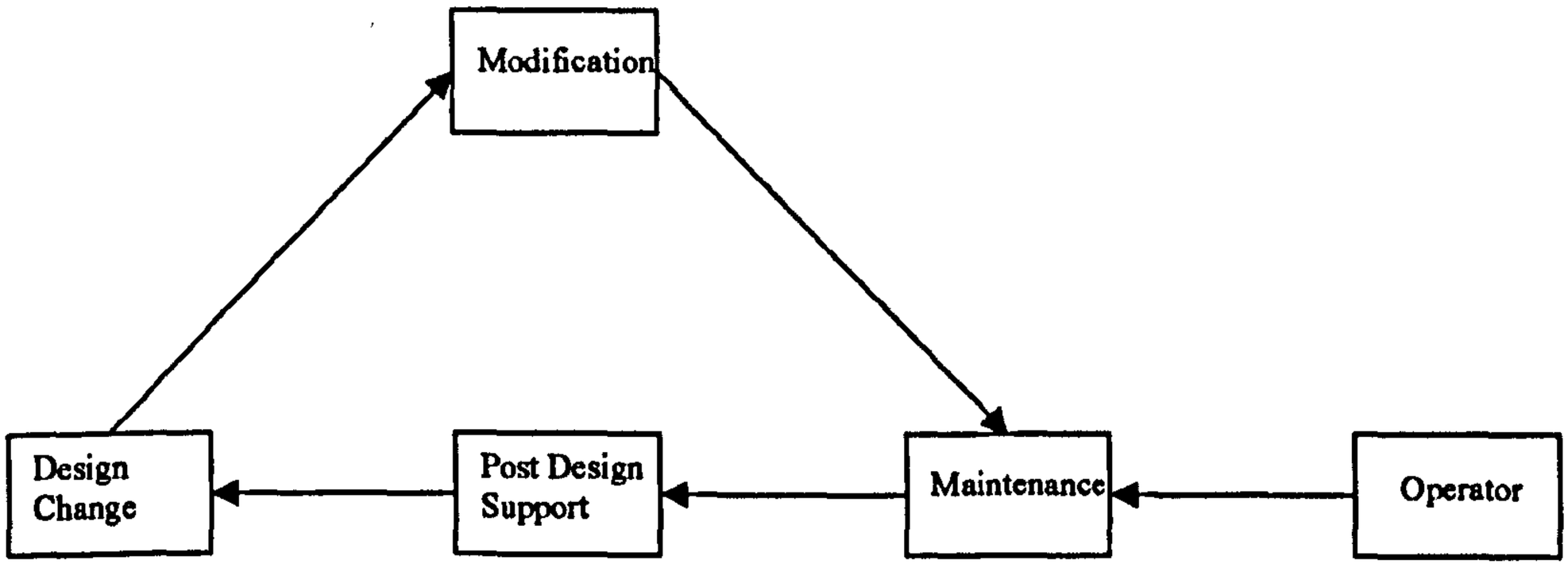


Figure 9 - Post Design Support Basic Model

Figure 9 shows the intent of the basic model, which allows in-service experience of technical performance to be fed back to the originating design team in the OEM, and then acted upon. Event information, either flight data or more usually maintenance data, is fed to the OEM's Post Design Support (PDS) team, which analyses the events, looking for either significant one-off cases where action needs to be taken straight away, or longer-term trends which may

also eventually require correction. Changes identified in this process as being necessary, are passed back to the design team, who will initiate the change, thus resulting in some form of modification to the design that will be passed on to the operator as a product improvement.

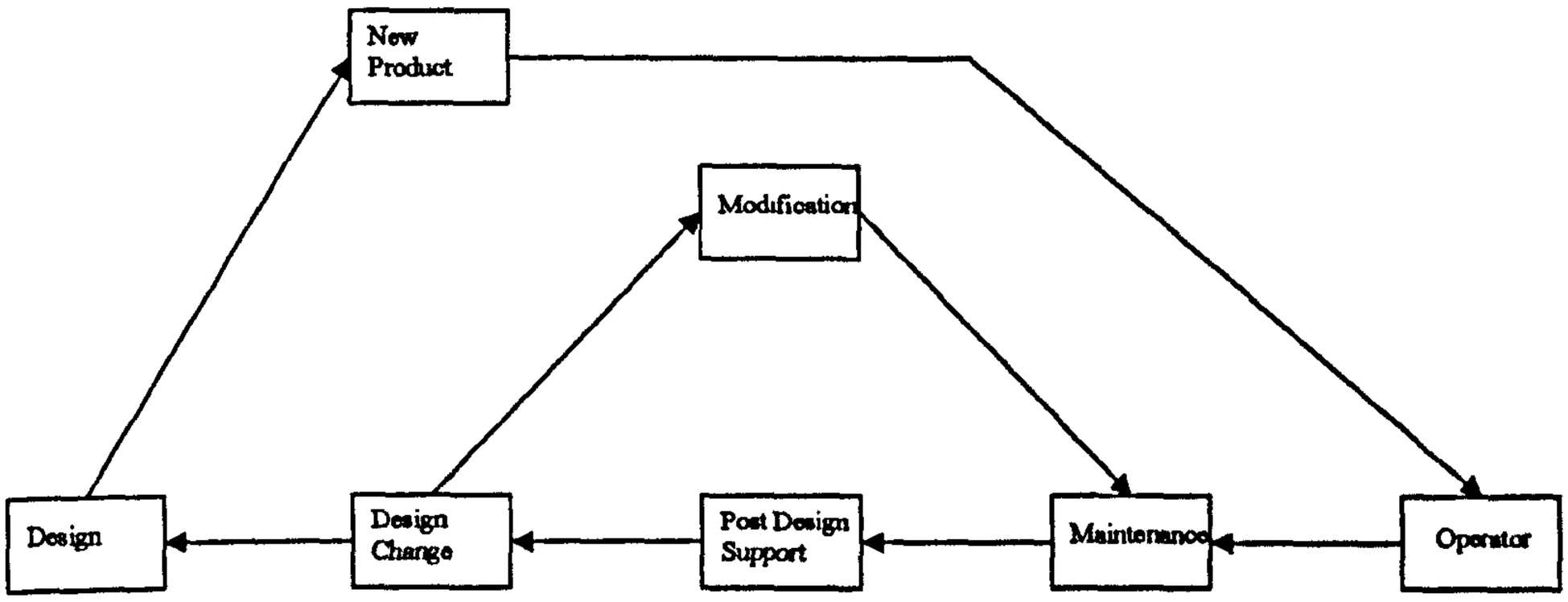


Figure 10 - Post Design Support Lessons Learned

Figure 10 shows the same process but with a significant addition, the lessons-learned loop. This is that part of the overall process which ensures that once modification action has been taken by design to correct an in-service anomaly, that information is also archived in such a way that future designs can retrieve the information to ensure earlier mistakes are not repeated.

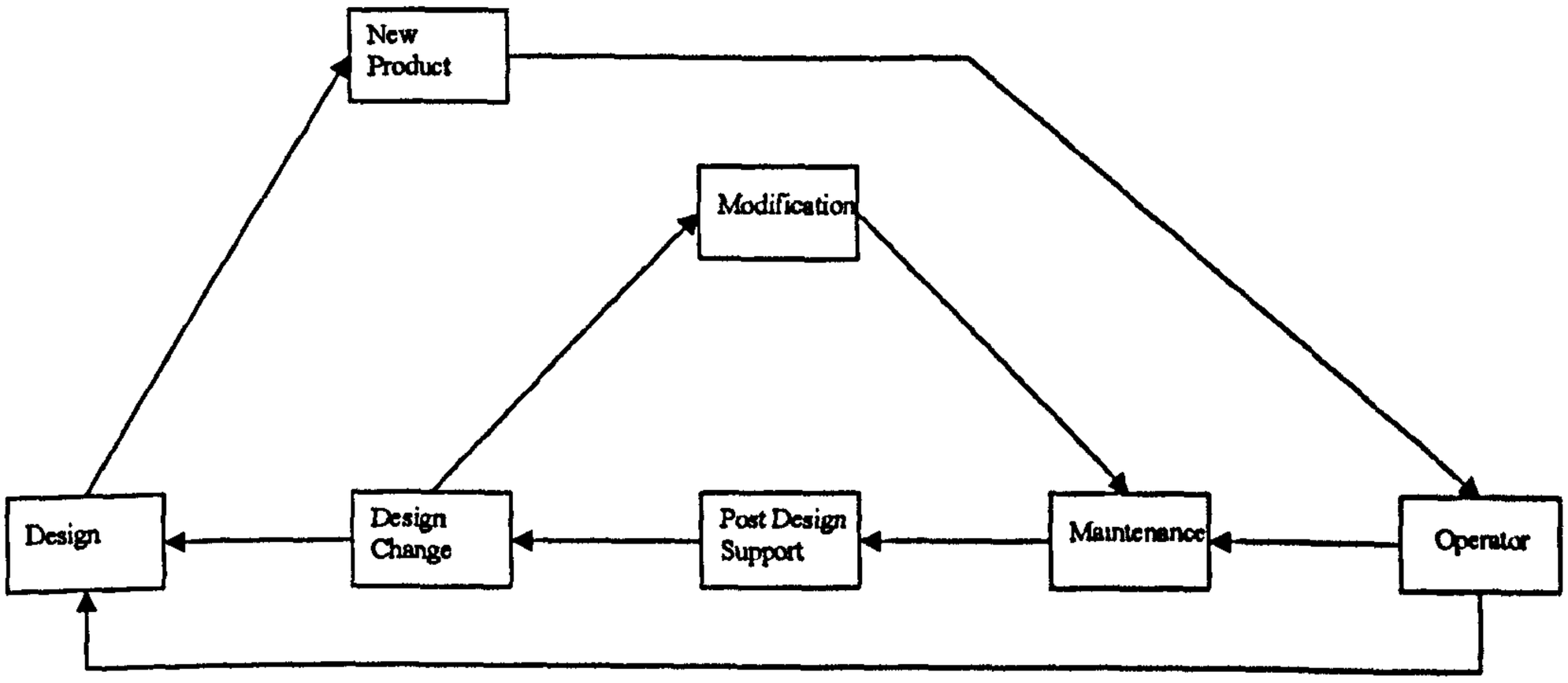


Figure 11 - Operator To Design Link

In Figure 11 a further link is shown, that which allows the design team to learn how well their equipment is performing directly from the operators. This is one

of the critical areas of feedback, which currently is only carried out on an ad hoc basis at any level below that of the prime contractor.

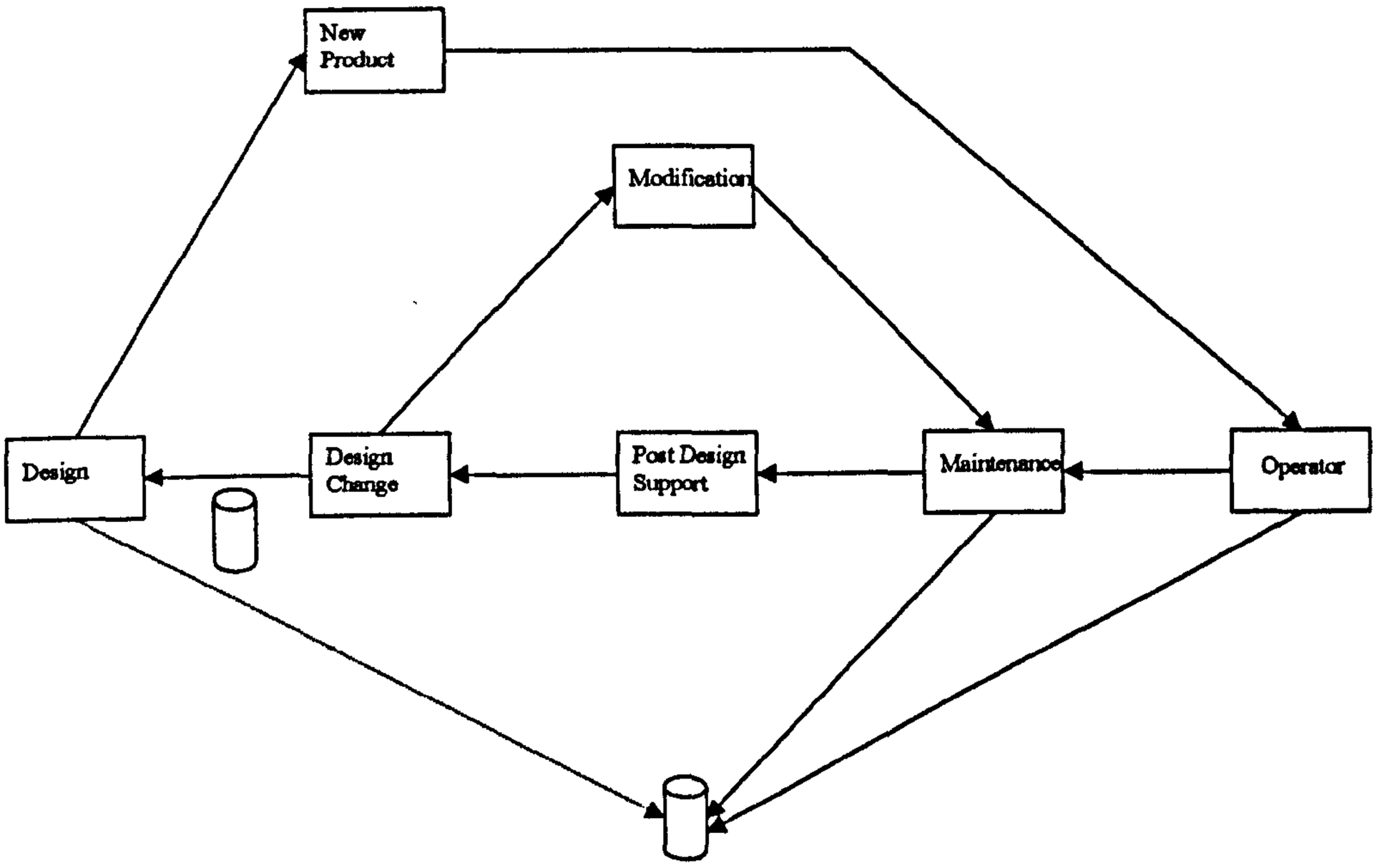


Figure 12 - Event Database Links

Figure 12 introduces two databases to the system. The first one, resident within the PDS domain, receives input from the operator, either from flight operations or maintenance and provides the raw data on which reliability and safety calculations are based. A dotted link is shown to the database from the design team, who should be able to interrogate it for information to influence their current efforts. The second database, hosted within the design area, is the lessons-learned database already mentioned, which also draws information from the PDS system and which can in fact, be the same database if configured correctly.

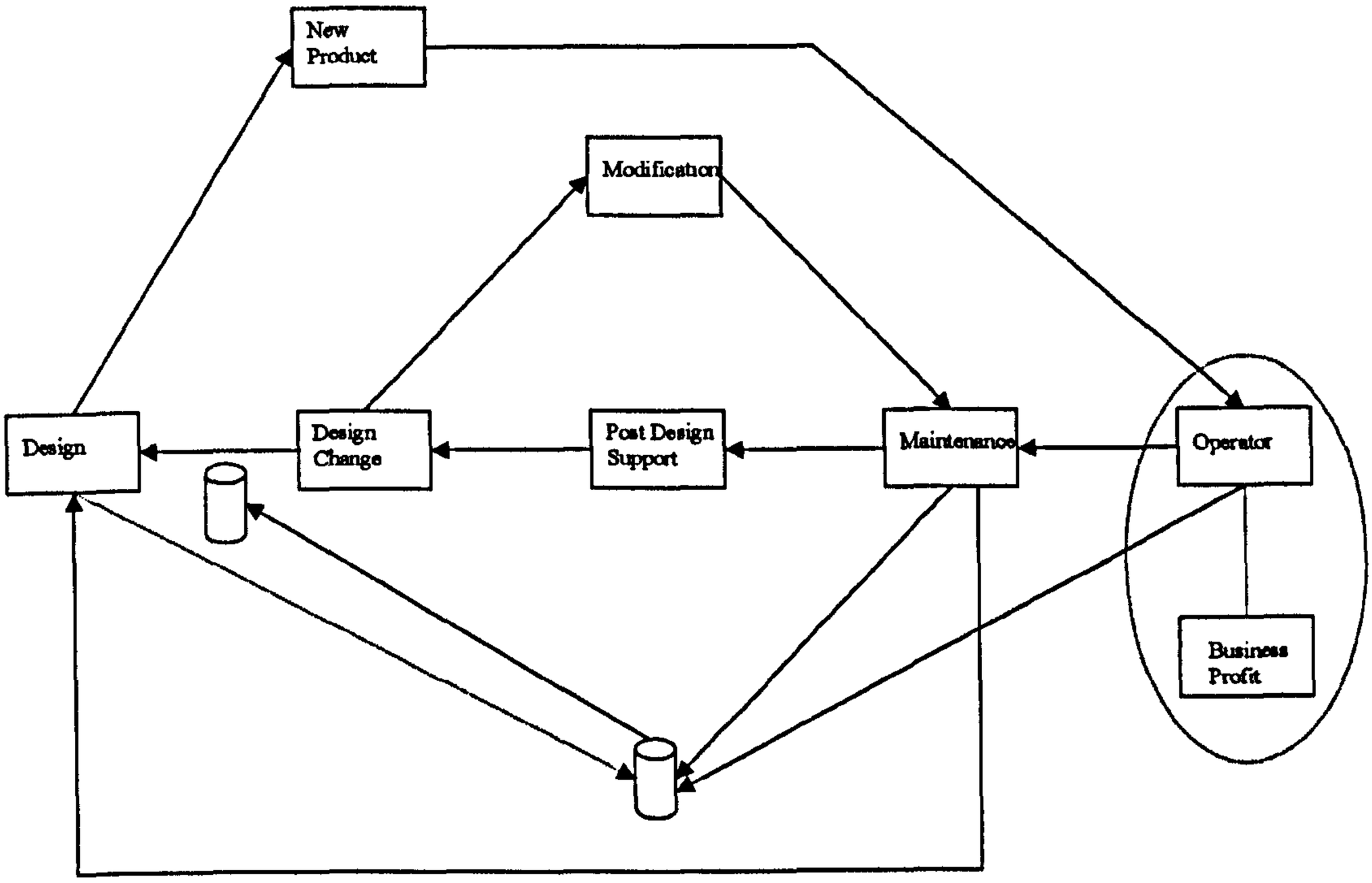


Figure 13 - Closing The Loops

The final part of the process, shown in Figure 13 closes the last required loops to ensure the full and optimum flow of data. Now there are feedback loops directly from maintenance to design and as mentioned in the previous paragraph, from the PDS database to the lessons-learned database.

This diagram also shows the business profit requirement within the operators' domain, since a major key to any new system has to be cost-effectiveness. Cost issues have been seen to be a factor in a number of aircraft accidents, usually through either maintenance of flight operational procedure shortcuts, but financial issues are outside the scope of this thesis and are not addressed.

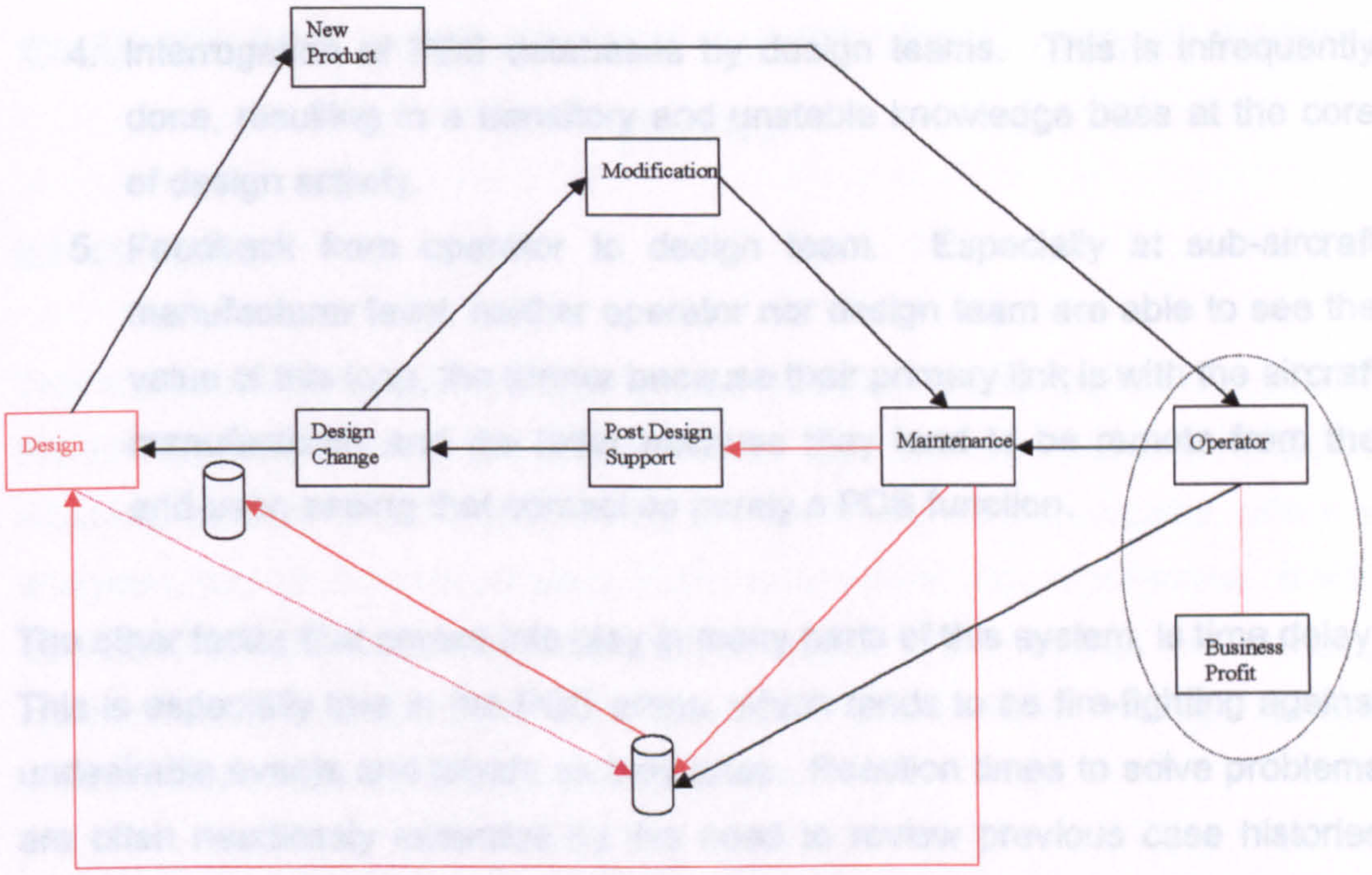


Figure 14 - The Flaws In The System

In Figure 14 flaws in the total system are highlighted in red. There are essentially five such flaws where the present system breaks down and reduces its effectiveness, either because the need is not properly understood, because the regulation does not require it, or because the right tools are simply not available or in place. The new model central to this thesis and shown in the next chapter, addresses each of these flaws:

1. Feedback from maintenance to PDS, particularly so at Tier 1 and Tier 2 supplier level, where the reporting lines are patchy or are filtered by the aircraft manufacturer.
2. Retrieval of event data from maintenance into a PDS analytical database, which even if it exists, may be poorly configured so that not all the data essential to ensure safety compliance is collected.
3. Dataflow from PDS to lessons-learned, often totally absent. Statistics have shown that approximately 80% of human factors errors have their basis in flawed design. "PDS is a block to effective in-service event feedback to design." [69]

4. Interrogation of PDS databases by design teams. This is infrequently done, resulting in a transitory and unstable knowledge base at the core of design activity.
5. Feedback from operator to design team. Especially at sub-aircraft manufacturer level, neither operator nor design team are able to see the value of this loop, the former because their primary link is with the aircraft manufacturer, and the latter because they tend to be remote from the end-user, seeing that contact as purely a PDS function.

The other factor that comes into play in many parts of this system, is time delay. This is especially true in the PDS arena, which tends to be fire-fighting against undesirable events and trends as they arise. Reaction times to solve problems are often needlessly extended by the need to review previous case histories almost "by hand" and re-run reliability and safety calculations over and over again, simply because no central system exists to do this work for them.

In essence then, while the PDS part of the system is probably working reasonably well at aircraft manufacturer level, albeit with unnecessary time delays, below that it is not. The outer loops on the system illustrated above, which are concerned with the speedy and accurate flow of essential data outside PDS, are not working, and the proposal in this thesis will enable that to change.

CHAPTER FIVE – THE SYSTEM SAFETY COMPLIANCE MODEL (SSCM)

5.0 OUTLINE

This chapter introduces the System Safety Compliance Model (SSCM), which is the principal innovation of this thesis. It describes how the system will function, including who can access it, how they will do so, the data it contains, how it is analysed, and the automated alert functions for safety non-compliances. It also considers system ownership, data confidentiality and interface with existing systems. The financial benefits of SSCM are also reviewed through specific case studies to demonstrate potential savings.

5.1 INDUSTRY VIEWS ON THE NEED FOR BETTER DATA

"Detailed information and data about what's going on out there is the lifeblood of any safety management programme" [70]

"If we had the ability to predict and forecast difficulties ahead, many of us would take the necessary steps to avoid the problem in the first place. Information and monitoring is not just about collating data. It also involves building a trusted relationship with customers to accurately understand their operating requirements" [71]

Speaking in September 2004 at the first annual US FAA International Aviation Safety Forum FAA Administrator Virginia Blakey said the five-year timetable for global safety data sharing is "too slow".

"We can do it now, and it needs to happen on an international scale," says Blakey. "We needed it five years ago. The timetable of the next five years is too slow. We need to take another big step, data needs to be shared and integrated so we can see fleet and geographic trends. We can de-identify the data, aggregate it and make it available to everyone via a secure network. Without the overall data we will not see the big trends."

Harro Ranter of the Air Safety Network has taken a very pro-active stance on the issue of air safety data from in-service events [72].

"Preventing accidents from happening and preventing recurrence of accidents that have happened, is a responsibility for everyone in the aviation industry. In order to achieve this goal (air) accident investigation boards issue reports and recommendations in the wake of accidents/incidents, regulating authorities collect data on accidents, incidents, aircraft *Air Safety Information* is limited. All these air safety data/information sources are a key element in the process of preventing accidents since it serves as a raw material for safety studies, trend analysis, monitoring, regulations etc."

"Maybe not directly linked with accident prevention, a manufacturer or prospective buyer may want to investigate the defect and damage history of an aircraft. Similarly, air safety data can be used to claim that a manufacturer knew about certain problems beforehand, because of earlier occurrences. Vast amounts of aviation safety related information are currently available on paper as well as online, free as well as paid and reliable as well as unreliable. It is becoming more and more difficult for aviation professionals to keep track of everything and filter out the reliable and relevant information for his/her organisation."

In the previous chapter, the work of the French DGAC in assessing incident feedback databases was discussed, and the inescapable conclusion was that none of the existing systems was entirely satisfactory.

5.2 PRINCIPLES OF SSCM

At the 5th Eurocontrol Human Factors Workshop in Prague in May 2001, a paper was presented by Jean Paries of the Dedale company, entitled *Feedback from Experience in Aviation – Current Challenges and Industry Initiatives.*

Among the many issues raised by Paries' paper, one stands out as a fundamental principle tying in operational feedback with the original system safety analysis of design.

In the Correction Cycle section of the paper, he states that there should be a "warning function if results are not obtained." This crucial point is the main one currently being missed by the air transport industry as a whole.

In order to address both this and all the other problems outlined in this thesis, the SSCM has been developed. With the exception of the already identified needs for improvements in personnel training and industry awareness, all the other shortfalls in the current safety analysis process are addressed by SSCM.

The basic principles of SSCM are:

- A web-based fully-automated system safety analysis software package maintained by an independent agency, which includes component reliability databases feeding into FMEA, FMECA, RBD, FTA and FHA tools to provide the basis for the safety case required for certification
- Operating environment considerations in reliability data analysis through an automated coding system
- A linked incident data capture system for use by operators, maintenance organisations, and manufacturers. This includes confidential reporting of incidents, as well as the traditional reporting methods previously discussed
- Links to network-based automated spares and maintenance activity systems based on the ATA 2000 E-Business Specification for Materiels Management system for standardised electronic spares demands and progression. Those airlines that have bought into ATA Spec 2000, use the specification to conduct their e-business for a range of material management activities. ATA Spec 2000 describes common data formats for industry to exchange information electronically, allowing airlines and their suppliers to fully automate processes in the areas of: Provisioning, Spares, Procurement, Procurement Planning, Purchase Order Administration and Invoicing, Repair Administration, Reliability Data exchange, Surplus Data, Delivery Configuration and Warranty. Amongst the features utilised by SSCM will be the bar code system for spares and maintenance tasks, which will provide the downloadable link to update parts catalogues and component reliability databases in virtually real-time

- An alert message system which is automatically triggered whenever an aircraft system reliability performance degrades to such an extent that it threatens to jeopardise compliance with the safety levels defined under the FHA procedure. Different alert levels are used depending on the immediacy of the threat, and follow the system used throughout the industry for cockpit warning cue colours and nomenclature.

5.3 SYSTEM FUNDAMENTALS

The overall structure of SSCM is based on the FRACAS system that the author designed, successfully implemented and evolved at TRW Lucas Aerospace in the late 1990s, but taken several stages further with a great deal of new functionality and data input. However, the basic concepts of data capture, data conversion and a lot of the basic analysis tools have been tried, tested and proven in everyday use. This should considerably facilitate the work required for proof of concept testing of the fully developed SSCM.

In order for the new system to be effective, a fundamental change of attitude towards reliability and safety data is required across the air transport industry. Today there are many good efforts underway, with many of them having been highlighted by the DGAC report discussed in chapter 4. Despite this, the critical failings already examined still hamper efforts to make this vital work as effective as possible, and will continue to do so if no change is made.
Therefore, the SSCM system must be:

- Demonstrably cost effective. This is especially critical at the design stage, with the key argument being the long-term benefits of getting the design "right first time" and thus avoiding the potential for lengthy and expensive reliability enhancement modifications post entry into service. This also enables reduction in time to market for new products, thus bringing the manufacturer's revenue stream on-line earlier than might otherwise be the case. It is also key in minimising the operator's direct operating costs through the ability to take correctly informed maintenance and spares provisioning decisions based on accurate input data from events in the field

- A step change in process capability, offering "something new", such as the automated alerting system for adverse safety trends and system safety non-compliance and the comprehensive coding system for accurate data searches and analysis
- Instantly accessible (with appropriate safeguards) at shop floor level to everyone in the business, i.e. component manufacturers and suppliers; equipment manufacturers, suppliers and repair organisations; aircraft manufacturers; aircraft operators including leasing companies; third party aircraft repair organisations; regulatory agencies; industry associations
- Easy to use and as automated as possible to minimise staff training requirements
- Capable of performing instant re-assessment of safety performance down to system level and including consideration of a variety of operating environments and conditions
- The industry standard repository of component reliability data, replacing the present motley collection of outdated and / or inappropriate data sources (this will take time)
- "Centrally" owned by a world-wide recognised industry body or bodies, in order to give it credibility and acceptability right across the aviation industry

5.3.1 System Architecture

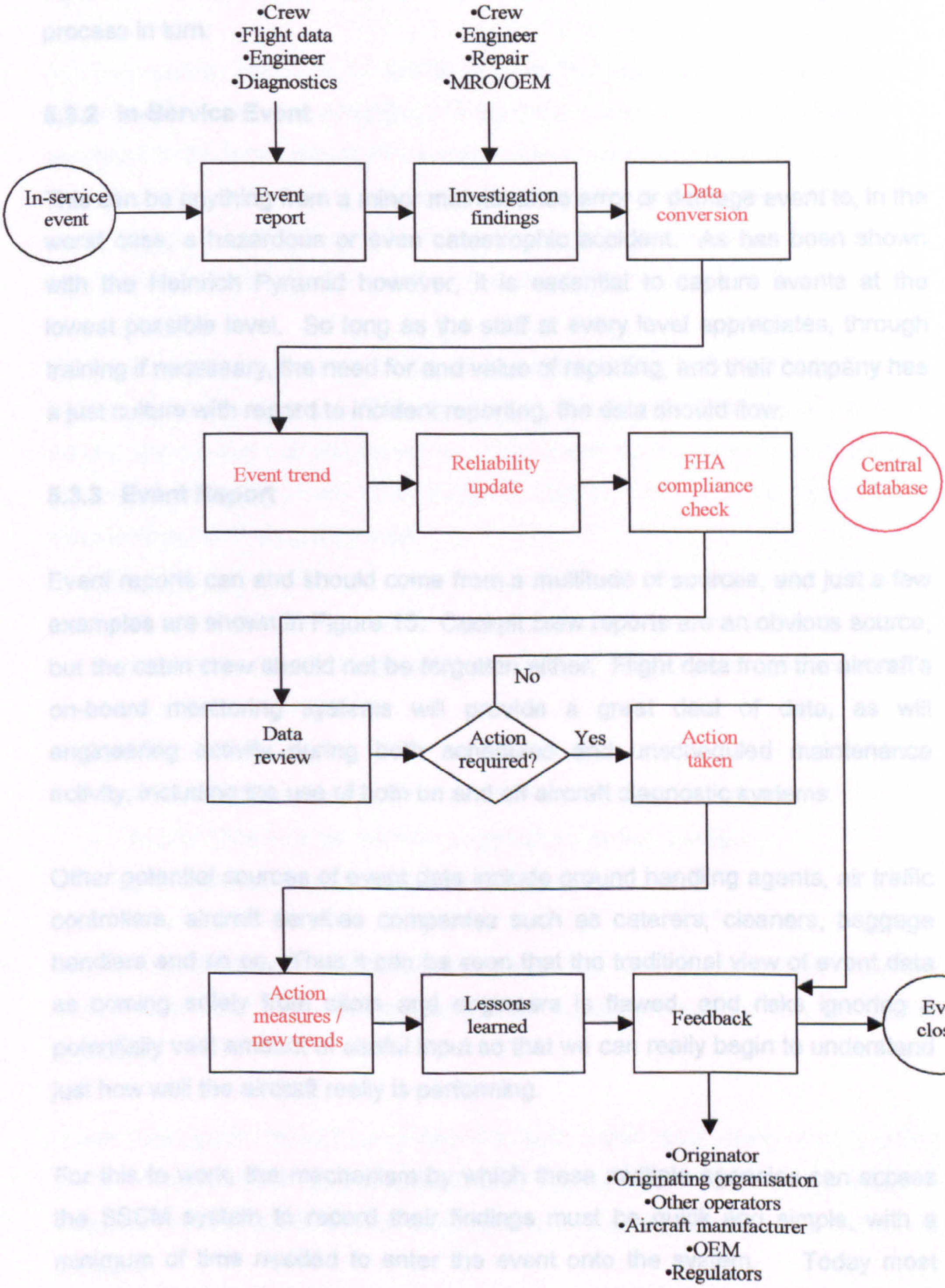


Figure 15 - SSCM Architecture

The steps shown in red in Figure 15, are those that are embedded within the centralised SSCM database. Let us now look at each of the steps in the process in turn:

5.3.2 In-Service Event

This can be anything from a minor maintenance error or damage event to, in the worst case, a hazardous or even catastrophic accident. As has been shown with the Heinrich Pyramid however, it is essential to capture events at the lowest possible level. So long as the staff at every level appreciates, through training if necessary, the need for and value of reporting, and their company has a just culture with regard to incident reporting, the data should flow.

5.3.3 Event Report

Event reports can and should come from a multitude of sources, and just a few examples are shown in Figure 15. Cockpit crew reports are an obvious source, but the cabin crew should not be forgotten either. Flight data from the aircraft's on-board monitoring systems will provide a great deal of data, as will engineering activity during both scheduled and unscheduled maintenance activity, including the use of both on and off aircraft diagnostic systems.

Other potential sources of event data include ground handling agents, air traffic controllers, aircraft services companies such as caterers, cleaners, baggage handlers and so on. Thus it can be seen that the traditional view of event data as coming solely from pilots and engineers is flawed, and risks ignoring a potentially vast amount of useful input so that we can really begin to understand just how well the aircraft really is performing.

For this to work, the mechanism by which these multiple agencies can access the SSCM system to record their findings must be quick and simple, with a minimum of time needed to enter the event onto the system. Today most airline and support employees are never far from an on-line computer, and this is the way into SSCM. Paper-based systems are far less effective, not least

because they require relatively complex procedures for collection and distribution.

Another solution might be for SSCM to draw the raw event data from existing systems. This has the advantage of possibly being rather more palatable to operators in the initial stages of implementation, than being asked to introduce a new data capture system at all levels. However, in the longer term it would still be preferable for SSCM to replace as many existing systems as possible, and thus become the initial point of entry for incident information.

Once an event has occurred, the information required by SSCM must be balanced between being sufficiently detailed to be analytically robust, and not so time-consuming that the person inputting it will become bored and eventually not bother reporting at all. The minimum data for non-technical personnel at this initiating point should include:

- An automatically generated unique numerical event identifier to provide traceability right through to closure, and common for all agencies having an input into that event
- Date of the event
- Person entering the event
- Aircraft type and tail number, registration, or fleet number
- Brief free-text description of the event

Aircraft identification to individual airframe level is essential to ensure recurrent faults, which may be airframe, rather than equipment related can be readily identified.

Event description should be a free-text field rather than using a drop-down menu of event types (as some databases do), since the latter option leads to inappropriate entries and also limits options to the choices made by the menu designer.

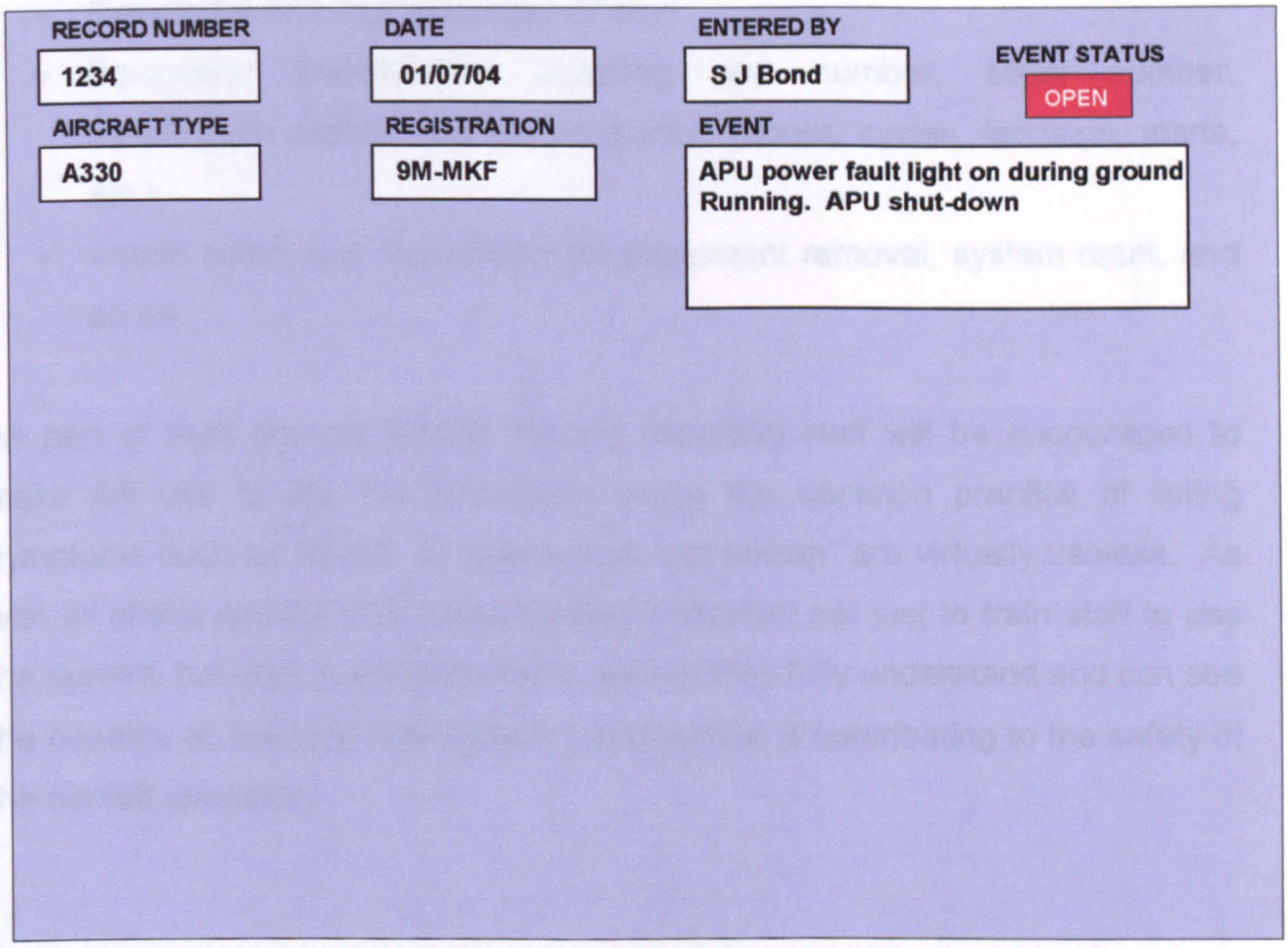


Figure 16 - Event Report Screen

Figure 16 shows the format of the basic database screen used to generate the event, using the fields already described. In the top right hand corner there is an Event Status field, which defaults to "Open" as soon as an event is input.

Data from an actual in-service event has been entered to provide an indication of how the data appears, and in the later stages, how it is combined with investigation information to provide the required input for corrective action and reliability monitoring purposes.

Flight crew and engineers' reports will of necessity be more detailed, and depending on the nature of the event, will require data input into some or all of the following additional fields:

- Technical log number or other unique identifier
- Operating environment (this information ultimately feeds into the environmental coding system described in section 5.4)

- Symptoms and fault diagnosis (if any)
- Equipment identification including part number, serial number, modification status, and life consumed (hours, cycles, landings, starts, etc.)
- Action taken, e.g. the reason for equipment removal, system reset, and so on

As part of their pre-use SSCM training, inputting staff will be encouraged to make full use of the free-text fields, since the common practice of listing symptoms such as "failed" or even worse "not known" are virtually useless. As with all of this activity, it is fundamentally important not just to train staff to use the system, but also to **educate** them, so that they fully understand and can see the benefits of, learning how system performance is contributing to the safety of the aircraft operation.

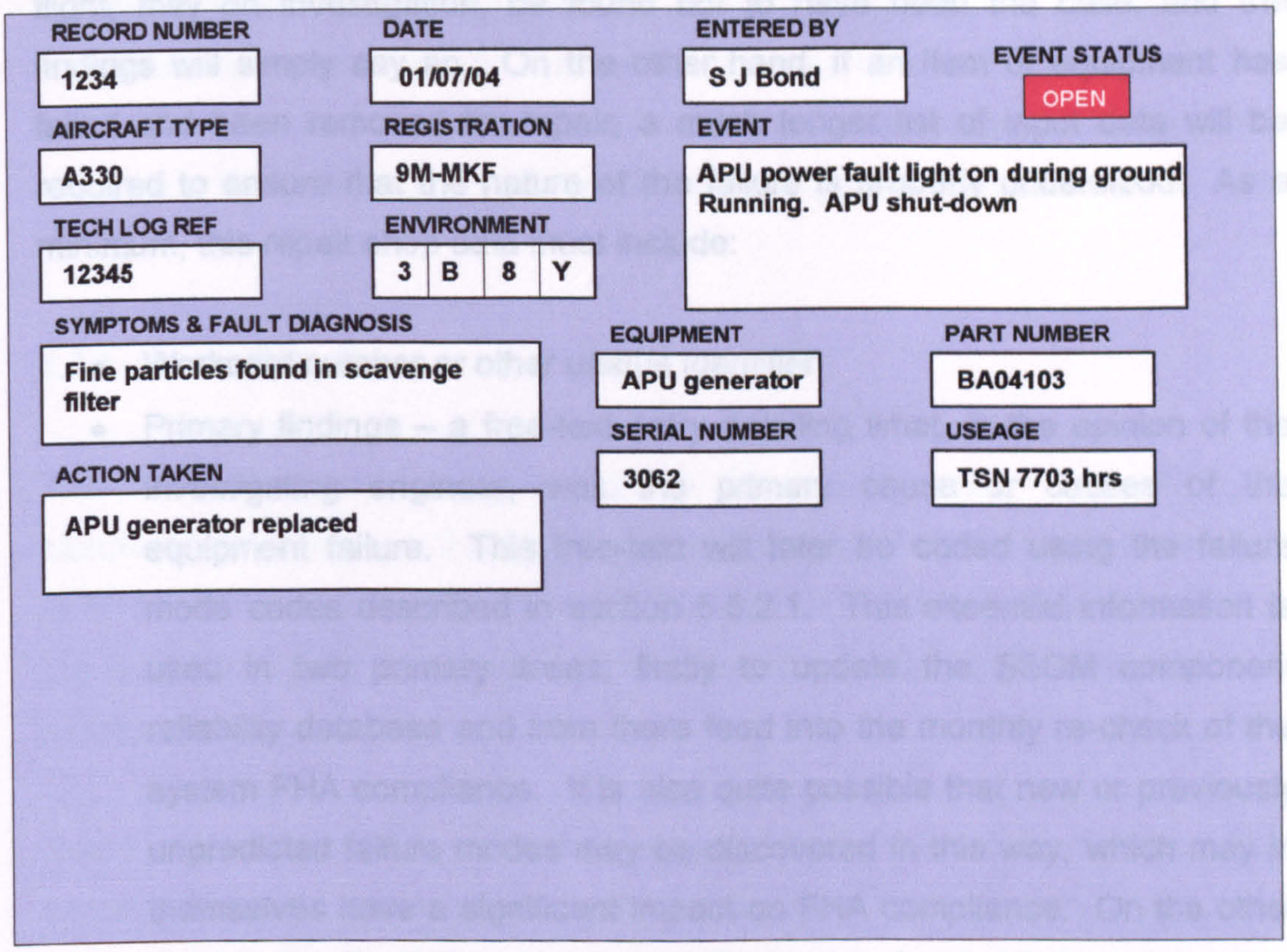


Figure 17 - Enhanced Event Report Screen

Additional details may also be automatically entered by virtue of the location of the workstation used to make the entry. This will include location and reporting operator / company.

In each screen example illustrated, it can be assumed that all the additional fields will be present, but "grayed out" to deny access as appropriate. They have been omitted here simply for reasons of clarity.

5.3.4 Investigation Findings

As a result of the event report being raised, an "open entry" status will be flagged on the SSCM system. This status will remain until such time as the Event Closure field has been completed (see below).

The nature of the findings will obviously vary depending on the type of event. For example, a report of a suspected operating parameter exceedance during

flight, may on investigation, be found not to have been the case, and the findings will simply say so. On the other hand, if an item of equipment has failed and been removed for repair, a much longer list of input data will be required to ensure that the nature of the failure is properly understood. As a minimum, this repair shop data must include:

- Workcard number or other unique identifier
- Primary findings – a free-text entry detailing what, in the opinion of the investigating engineer, was the primary cause or causes of the equipment failure. This free-text will later be coded using the failure mode codes described in section 5.5.2.1. This essential information is used in two primary areas; firstly to update the SSCM component reliability database and from there feed into the monthly re-check of the system FHA compliance. It is also quite possible that new or previously unpredicted failure modes may be discovered in this way, which may in themselves have a significant impact on FHA compliance. On the other hand, a No Fault Found entry can be used to feedback into such areas as fault diagnosis procedures and on-aircraft BITE
- Secondary findings – a free-text entry detailing any other problems the engineer may have found that he / she considered occurred as a result of the primary failure cause, e.g., secondary damage. This is used for enhancing the understanding of failure effects as recorded in the original equipment FMEA and FMECA
- Action taken – what work did the engineer perform to correct the problems found. This is a brief summary of repair, overhaul, upgrade or modification and test

5.3.5 Data Conversion

At this point, the central SSCM database has sufficient information to start data coding under the various headings described in this chapter. One other vital piece of information is still required before reliability and safety levels can be analysed, and that is the aircraft fleet flying hours data. All the major aircraft manufacturers (Airbus, Boeing, Bombardier, Embraer, etc), already issue fleet flying hours, landings and dispatch reliability data on a regular basis, so it will be

a simple matter for them to upload the same data into SSCM. However, the manufacturers have to rely on the operators providing them with their own fleet data, and this can be patchy. Thus there is an unavoidable data lag in this area, so a full flying hours data upload can only be expected, at best, each month.

5.3.6 Event Trends

The database is now equipped with all the data it requires to perform the standard trend analyses of equipment reliability, based on the usual parameters of MTBF, MTBUR and NFF. Trend charts can be instantly updated, but due to the flying hours data lag already mentioned, will normally only be reviewed on a monthly basis.

Trend charts should be produced using a moving 12-month dataset. This ensures topicality, and avoids the risk of masking trends by looking at too much data, as is the case with those systems that chart all events from entry into service to date.

5.3.7 Reliability Update

As the event trend analysis is updated, so too is component reliability. This is why component part number information is so important during the event data entry phase, in order to provide the link to the reliability database, which also takes account of varying environments to produce a range of failure probability estimates, as was the case which such obsolete systems as NPRD.

5.3.8 FHA Compliance Check

Once the component reliability database has been updated, system manufacturers FMEA / FMECA and FTA, which are all embedded within SSCM as part of the safety case deliverables to the certification authorities, can also be recalculated to ensure FHA compliance.

5.3.9 Data Review

There is now a full set of updated information that can be reviewed as necessary depending on a number of requirements and triggers including:

- FHA non-compliance alert
- Removal rate alert levels
- Modification or other corrective action effectivity checks
- Maintenance effectivity checks
- Other regular Measures Of Performance (MOP)

Appropriate bodies through multi-skilled forums of interested parties will carry out data reviews. For example, a system manufacturer might convene a monthly Reliability Trend Review Team (RTRT), that looks at all the current performance levels for their equipment, picking out adverse trends for discussion and either allocating responsibility for new corrective actions, or looking at the progress of previously established actions. Recommended attendees at an RTRT include the data analysis team (usually part of ILS), customer / product support, design, production, test, repair and overhaul, quality and, commercial departments. The results of data reviews must be summarised on SSCM.

5.3.10 Action Required

What has the data review body decided to do? It may be that no action is actually required, in which case there will be a justification statement, otherwise one of the following statements may be input:

- Modification or re-design - to enhance reliability and safety levels, vulnerability to incorrect operation or maintenance, etc.
- Change to operating procedure – procedures are being followed correctly but are inappropriate
- Change to maintenance procedure – procedures are being followed correctly but are inappropriate

- Training – to correct incorrect operating or maintenance practice, repeated error, etc.
- More data required – referred back to the originator or repair organisation
- Further trend measurement required – non-urgent and trends are erratic or require a longer period to become clear

Whichever of these cases is selected, a brief summary of the actual action proposed must also be included, together with the proposed timescales for implementation and references to the detailed written reports and recommendations.

5.3.11 Action Taken

At some stage following identification of the required action, this field will record what was actually achieved, such as:

- Modification or re-design implemented – including identification of modification category, embodiment policy and completion date across the aircraft fleet, introduction point into new production and so on
- Change to operating procedure implemented with effect from a certain date
- Change to maintenance procedure implemented with effect from a certain date
- Training programme (new or modified) introduced and all effected staff trained
- More data received from originator or repair organization and further action taken (as appropriate)
- Further trend measurement carried out and further action taken (as appropriate)

RECORD NUMBER: 1234
DATE: 01/07/04
ENTERED BY: S J Bond
EVENT STATUS: OPEN
AIRCRAFT TYPE: A330
REGISTRATION: 9M-MKF
EVENT: APU power fault light on during ground Running. APU shut-down
TECH LOG REF: 12345
ENVIRONMENT: 3 | B | 8 | Y
SYMPTOMS & FAULT DIAGNOSIS: Fine particles found in scavenge filter
EQUIPMENT: APU generator
PART NUMBER: BA04103
SERIAL NUMBER: 3062
USEAGE: TSN 7703 hrs
ACTION TAKEN: APU generator replaced
WORKCARD NUMBER: G8690
PRIMARY FINDINGS: Fractured main rotor tags, leading to open circuit
SECONDARY FINDINGS: Movement of oil transfer tube. ME stator damaged
ACTION TAKEN: Main rotor and ME stator replaced. Unit flushed and tested, satisfactory
FAILURE TYPE: F
FAILURE MODE: MRL
EVENT CODE: C | 1 | X | F
SAFETY ALERT: NO

Figure 18 - Complete SSCM Data Entry Screen

5.3.12 Action Measures / New Trends

Now that some appropriate action has been taken, the next step is to ensure that it has had the desired effect. A number of questions requiring a simple Yes / No / NA toggle selection on the database are posed to provide the necessary confidence. The NA (Not Applicable) option is necessary for use in those cases where some action has been taken without any safety alert first being triggered.

- Have all the identified actions been completed?
- Have adverse downward reliability trends been reversed consistently across the fleet?
- Has the trend reversal occurred and / or reliability stabilised for the last 3 months?
- Have safety compliance levels been re-established at all operators?
- Have safety compliance levels stabilised for the last 3 months?

A "No" answer to any one of the questions automatically locks-out the ability to select event closure, and requires further action to be taken.

5.3.13 Lessons Learned

All manufacturers should have some form of "lessons learned database", and many do. The intent is to ensure that bad decisions or mistakes made during design are not put back into the next generation of equipment. The lessons learned section of SSCM is a field that receives automatic data input as earlier fields are completed. What the enquirer will find here for downloading into his own lessons learned system are:

- Event description
- Primary findings
- Action taken

5.3.14 Feedback

It is now essential that as a minimum, the same information provided under the lessons learned heading above, is also feedback to all the parties involved in the event, from the originator onwards. Individual company communication mechanisms need to be in place and effective to ensure this happens since without effective feedback loops, event-reporting rates would slow down and could eventually either stop altogether, or only consist of the more dramatic occurrences.

This information flow will not stop at the front door of the organisation involved however, and will continue on to all other interested agencies, such as other operators of the same equipment, the aircraft manufacturer, the OEM and the regulators.

One way in which the ease of feedback data flow can be enhanced will be through the part number system already embedded in SSCM for the reliability database. A straightforward linking of part numbers to standard supplier designators will allow automatic messaging to the supplier that there is a

problem with those parts associated with adverse trends through the FHA compliance alert system.

5.3.15 Event Closure

This field requires a simple confirmatory message that all actions have been completed and that the five Action Measures / New Trends questions have all been answered "yes". The "open entry" event status is then unlocked and the event can be closed, completing the SSCM cycle.

5.4 ENVIRONMENTAL CODING

As has already been discussed, a major failing in current safety analysis processes, is the lack of appreciation of the impact of varying operating environments on equipment reliability. In general terms, the aircraft manufacturer will specify a "typical" flight profile and operating scenario for the system designers to feed into their analytical model, and while there is obviously room for sensitivity analysis to vary some of the parameters, that is about as far as it goes.

A recent example of how this lack of clear understanding can cause problems is the teething problems experienced by airlines introducing the Bombardier CRJ700 and CRJ900 regional jets into service. Reliability has been markedly down from expectations, and Jeff Mihalic, General Manager Customer Service at Bombardier, has said [73]:

"The problems are operator-specific. The aircraft is not mature yet and how it is deployed is key. Addressing operator-specific issues in the short term can have big benefits for fleet-wide reliability."

The problem of course is the tremendous complexity of analysing system performance under all possible permutations of flight profile, operating environment, geographical location, and so on. For example, the Airbus A320 series of airliners currently fly with around 80 different operators in almost every

corner of the World, with average flight times varying between 30 minutes and possibly six hours (in the case of the A319CJ variant).

SSCM facilitates an easier analysis of these variables by the use of a four-figure code that is assigned to each failure event. The coding system considers four environmental parameters and allocates an alpha/numeric identifier under each heading, as shown below.

Geographical Location	**Code**
Temperate	1
Tropical	2
Sub-tropical	3
Arid	4
Cold	5
Marine	6
Operating Cycle	
< 1 cycle per day	A
1-2 cycles per day	B
3-6 cycles per day	C
> 6 cycles per day	D
Daily Utilisation	
< 3 hours	6
3-7 hours	7
8-12 hours	8
> 12 hours	9
Annual Utilisation	
< 100 flying / operating hours	T
100-500 flying / operating hours	U
500-1,000 flying / operating hours	V
1,000-2,000 flying / operating hours	W
2,000-4,000 flying / operating hours	X
> 4,000 flying / operating hours	Y
> 12 hours	Z

Table 7 - Environmental Coding System

Use of this system will enable instant recognition of a wide range of operating environment factors which when combined with other event data, will assist in focusing in on the causal factors leading to a downturn in system reliability performance.

5.5 EVENT AND INCIDENT DATA CAPTURE AND ANALYSIS

Fundamental to the success of SSCM is its widespread use throughout all sections of the industry, and many other systems have tried and failed at this stage. The are five main reasons for this:

1. The company being asked to supply the data does not have a fully-developed safety culture. Without this there will always be reluctance on the part of the employees to use a data capture system effectively.
2. The proposed system is either difficult to access, difficult to use, or the data asked for is either too complex or over-simplified.
3. Data is considered proprietary and thus not to be shared. This is particularly true of repair organisations competing with each other for business.
4. There are no resources available to look after the system and carry out the analysis tasks.
5. There is no effective regulatory pressure to do so.

How can these problems be addressed? Some can indeed by answered by SSCM, while others require adoption of some of the other points raised earlier, in particular, the need to better educate the aviation industry about the need for, and benefits of through-life safety analysis. We are not yet smart enough in maximising use of the powerful analytical tools at our disposal.

The organisation operating and maintaining the system must have no direct interest in the outcome other than the sharing of safety information. The system must be owned and maintained by an independent non-regulatory organisation with no vested interest in the content of the data and information stored in the database. An example of a qualifying government organisation would be NASA. A commercial organisation outside the aviation industry and specializing in information processing and/or Web application hosting would also qualify.

With the decreasing cost of hard drive storage media, constraints on system capacity are not likely. Nonetheless, the system must be capable of storing one million records plus attachments, and the system must be capable of indexing

and searching all the data stored within the system and linked to data owner systems.

The first step in integrating dissimilar data into a sharing system involves identifying data fields that are common among the different safety event reporting systems. Once the common fields are identified, the fields are reviewed for relevance, based on the information needs of the user. Such relevant fields may include make/model, airport name, phase of flight or type of event. Once the relevant fields are established, a map is generated mapping the common fields among the dissimilar data sources to create a virtual subset of data. The next step is to organize the data within the mapped framework so that the information can be conveniently manipulated. This process involves converting the data from dissimilar systems into a common standardised format.

Another consideration when implementing a system is to examine the various approaches to collecting the data. One method uses on-line discussion forums or electronic bulletin boards. A more complex approach requires periodic extraction of data from multiple, disparate, event management systems and merging the data into a central repository. An emerging approach includes the use of the Internet to network several airline flight safety event management systems by mapping individual data fields within each of them to a virtual repository that is available to all members." [74]

5.5.1 Company Culture

Correcting an organisation's inappropriate safety culture obviously cannot be done overnight, but demonstrating to management the potential cost savings of being able to fully understand how equipment performance might be improved is a good start. This can then be followed up by standard industrial initiatives such as Total Quality Management (TQM), embracing the ideals of employee empowerment to help everyone understand the part they can play in improving performance.

Company's face ever-increasing financial pressure and this is frequently highlighted as a reason for not introducing a new process. The key is to demonstrate to the doubters, the potential benefits to them of adopting SSCM. One answer is to point out the extra maintenance burden of incorrect reliability assessment, as was shown in section 3.28. Lower reliability will always lead to higher direct operating costs, and the example discussed resulted in an increased annual cost to the operator of $480,000 annually for just one item of equipment.

This figure pales into comparison with the effect on the operator of a catastrophic accident. The industry has stated that the average cost of such an event is something in excess of $3 million for every passenger killed. No company can afford this, and even if they can, the effect of an accident on their public image and hence commercial viability, is extremely serious.

5.5.2 Ease Of Use

Designing a data capture and analysis system which is user-friendly enough that people will actually get into the habit of using it every time they should, is a fine balancing act between quick and easy data input and meaningful analysis output. For example, some repair shop systems have moved away from allowing "free text" entry by the engineer of what he found when he performed the work, to giving him a menu of "finding codes" from which to select that which closest fits his actual findings. The great danger here is that the tendency rapidly develops to always use the same one or two codes that are easiest to remember quickly, and which may not be a true reflection of the fault. Even worse, is having a vague "general" finding code, where the coder has run out of ideas during the building of the menu. This is meaningless and should be avoided at all costs.

As the DGCA said (see section 4.15.4), data categorisation is essential to ease data retrieval, but "this is most problematic with subjective descriptions of an event and its causal factors", since "it was impossible to anticipate all possible contingencies, therefore it was also impossible to create an exhaustive list of keywords."

5.5.2.1 Failure Mode Codes

What is needed is a combination of free text and data categorisation. The SSCM database allows for free text entry by the originator, which is translated into a pre-determined two or three-letter fault code by the receiving data analyst. Thus generalised searches can be made on the codes, and more detailed searches can be made when required by looking for word strings in the free text field.

When drawing up the failure mode code dictionary, a balance must be struck between having sufficient breakdown of failure modes to enable quick homing in on problem areas during data searches, while not making the dictionary so large that it becomes unwieldy with individual codes which become overly specific in failure detail.

In the examples in table 8 below, it can be seen that the majority of the codes contain sufficient detail for failure identification and thus trend analysis purposes. On the other hand, room is still left for "one-offs" or other difficult to categorise events, through the use of more generic codes such as MF for a Manufacturing Fault, which could be for example, a problem with a poor-quality batch of components, or the breakdown of a production process for some non-design related reason.

Failure Mode Code	Description
ACF	Auxiliary connector failure
ADJ	Out of adjustment
BC	Bad communication
BF	Bearing failure
BOS	Bearing outer race spinning
BRF	Banding ring failure
BSM	Brush solder melted
BWC	Brush wear check failure
CAS	Chassis assembly damage
CBF	Clutch bearing failure
CBS	Clutch bearing separation
CC	Casting cracked
CE	Clutch examination failure
CF	Customer fault (induced damage or failure)
CIR	Customer incorrect repair

Failure Mode Code	Description
CMS	Contaminated motor section
CPT	Component part failure
CTP	CT lead power failure
CUS	Chassis unserviceable
DCF	DC/DC converter failure
DIO	Diode failure
DLD	Diode lead damaged
DLS	Diode lead sheared
DPI	Diode pack disintegration
DV	Damage various (not categorised elsewhere)
EB	Earth bonding failure
EO	External overload/Extended operation
EV	Excessive vibration
FIL	Filter fault
FS	Failed stator
HMF	Hit module failure
IPN	Incorrect part number reported (by software)
IRS	Inner race spooling
LF	Logic fault
LL	Lack of lubrication / low oil level
MBF	Multiple board failure
MD	Minor damage
MER	Main exciter rotor failure
MES	Main exciter stator failure
MF	Manufacturing fault
MOD	Modification
MRD	Main rotor damage
MRL	Main rotor leads damaged
MRO	Main rotor open circuit
MSB	Motor section burnt
MSW	Main stator winding failure
NCD	Non confirmed defect

Table 8 - Example Failure Mode Code List

The Customer Incorrect Repair (CIR) code is also very significant. This demonstrates the SSCM ability to identify and enable searches against human factors criteria. A CIR can be due to a variety of reasons, including maintenance error (which in itself may have multiple causal contributors), or incorrect procedures, any one of which can be expanded in the free-text sections.

5.5.2.2 Event Codes

A further coding system is also used for categorising each event being reported. In this case, SSCM first identifies the source of the data, followed by the type of event, basic action taken and subsequent findings identifiers. This is the core of the SSCM system, and will ultimately become a very extensive and detailed list. For clarity it is shown separately in Appendix C.

This a very comprehensive range of eventualities that can be covered to give a clear and precise overall picture of; who found the problem and under what circumstances, what initial action was taken to recover from the effects of the event, and what close-out action was subsequently carried out. The codes list follows a logical sequence:

1) Data source - identification of the origin of the event report. Options include flight crew reports, flight data, on-board monitoring systems, 1st and 2nd line engineering reports, MRO or Depot level repair, and technical or regulatory post-event investigations.
2) Event category – identification of the basic nature of the event. Options include fault indication (a failure may not be apparent), failure (where such is clear), parameter exceedance (where a fault indication or failure has not apparently occurred), scheduled maintenance, and unscheduled maintenance.
3) Action taken – identification of what was done to clear that single event. Options vary depending on the input data under the first two categories, but include none (where no action was required), system reset, on-aircraft maintenance, repair, replace, overhaul and other.
4) Findings – the results of the post action investigation. Options include confirmed fault, induced fault, monitor (where further clarification or measurement over time is desirable), no fault found, condition / status report, and human factor event.

In all cases, the basic event codes are used to facilitate both data input and database searches, but are backed up by free-text narrative. As SSCM

evolves, other categories will undoubtedly develop, and this code list should be seen as a first iteration to enable the system to become established.

An important addition here though, is the identification of human factors events under their own sub-code. Over a period of time, this will enable the quantification of some human factors events, which is the current great difficulty with accurate forecasting of human factors impact on system safety performance.

5.5.2.3 Understanding Failure Types

One of the key issues is the definition and use of the differentiation between confirmed failures and induced failures. Even today this is not well understood, and is certainly misused within much of the aviation industry, yet it is fundamental to understanding the contributory causal factors in a failure to ensure the proper corrective action is taken.

For example, let us consider again, an aircraft electrical power generating system. A generator failure occurs during normal operations, and on inspection back in the repair shop, is found to have suffered a main rotor windings disconnection. Assuming there are no other mitigating circumstances, which is unlikely, this becomes a clear case of an inherent failure of the unit, for which the generator manufacturer must take responsibility and identify whether or not this could be considered to be a "one-off" event, or one which is part of a trend requiring remedial action. Such a failure in the SSCM database would therefore be classified as a confirmed failure and coded F.

Another generator fails and is found to have suffered a short circuit due to contamination by metallic debris in the oil. The generator shares its oil with the engine gearbox on which it is mounted, and examination of the debris composition shows that it has come from a gearbox component rather than from anything within the generator itself. This is clearly a case of the generator failure having been caused by some external event, for which the manufacturer cannot be held liable. In this case the SSCM database would classify this as an induced failure, and allocate the code I to it.

This is a vital differentiation for two reasons. Firstly, in the case of a warranty claim, identification of primary responsibility for the failure is obviously essential. Secondly, and more importantly from the point of view of reliability and safety performance, confirmed failures (F) are counted towards the calculation of MTBF, while both confirmed AND induced failures are counted towards the calculation of MTBUR. When downloading event data from SSCM into the component reliability database, only MTBF-related events must be considered. However, both MTBF and MTBUR events are necessary for the re-assessment of FHA compliance levels.

In fact, aircraft manufacturers address this issue in different ways, which can and does lead to confusion over what is and what is not an accountable failure. Gaining clarity of understanding and a common approach across the industry will be vital.

5.5.3 Proprietary Data

As has already been mentioned, one of the problems in getting operator buy-in to a data retrieval system such as this, has been their concern over "airing their dirty linen in public", that is to say, many are worried about their events and the action they take, being in the public domain. Even more important is the potential for liability, should the subsequent engineering investigation indicate that the operator, whether by accident or design, had done something wrong. Thus data confidentiality, or "de-sensitising" is very important in order to gain acceptance of and confidence in, SSCM.

However, the simple expedient of removing all originator information from incoming data, removes at a stroke, the ability to address one of the great problem areas with current safety analysis, the understanding of the effects of different operating environments, (see section 5.4). It also prevents an easy communication route back to the originator for feedback of the results of trend analysis and investigation, an absolutely vital part of the whole system. Some existing databases use the IATA two or three-letter operator code system,

where for example, easyJet translates as EZY, to facilitate data searches, but this does not make the data confidential.

There are two possible solutions for SSCM to adopt. The simplest is to continue to use the IATA codes, but hide that data field in the publicly-accessible database, which would still allow the database owners to perform meaningful analysis and provide feedback, but which would somewhat degrade the value of the data to visitors.

The alternative is to use a new set of confidential operator (and other organisation) codes, visible to website visitors but de-identified, which would help the identification of operator-specific issues (especially in conjunction with the environmental codes), without the ability to point the finger at anyone. This is the system that SSCM proposes to use.

In parallel, other data that can identify the originator, such as aircraft tail numbers for example, will also be contained in hidden database fields. Access to the hidden fields will be granted to those agencies that need to know this detail, in particular the aircraft and systems manufacturers and the regulatory authorities.

5.5.4 Lack Of Resource

Here again, the argument about the fight for survival under the daily commercial pressures will be used as a reason for not implementing SSCM, and of course the potential cost savings as already shown, are the main response to that. It cannot be denied that, depending on the size of the organisation and its current structure, there may be a requirement for a dedicated resource to set up and manage their end of the SSCM system. In other cases, particularly in the larger companies, there will already be for example, a reliability team, who can transfer much of their current disparate systems into SSCM, which may well actually bring a saving in resource requirements.

Procedures must be put in place, including confidential reporting systems if they are not already established. Staff must be educated about the need for SSCM

and trained to use it, terminals must be set-up, review bodies identified for the monthly meetings, and so on. All this takes time and money and ties up people, so the business case must be robust and take the longer-term view with clear identification of benefit.

5.5.5 Lack Of Regulation

The regulatory authorities continue to move away from audit and in many cases basic legislation, and are driving hard towards the principle of self-regulation by the industry. Not least among the problems is the poor state of the existing legislation intended to ensure that aircraft systems are fit for purpose and safe. So far, the messages emerging from EASA seem to indicate that they too, have failed to recognise the issue.

EASA should therefore be encouraged to require implementation of SSCM, phased in across the European industry over a period of five years. At the same time, ARP4761 must be moved from being a recommended practice, to being a regulatory requirement, although it will need considerable amendment and upgrading in the medium term to increase its effectiveness. It is believed that these initiatives will be able to demonstrate the benefits of SSCM in a fairly short period of time, such that the other major world regulatory agencies, including the FAA, Transport Canada and so on, will take notice and follow suit.

As long as the industry is able to pick and choose what it does with regard to safety analysis, the situation will not change. Legislation is vital.

5.6 MAINTENANCE AND SPARES DATA CAPTURE

The increasing adoption of maintenance documentation and materiel supply standards ATA 1000 and ATA Spec 2000, provides the opportunity for SSCM to capitalise on already established systems for easier parts tracking. The introduction of standard text formats, and Common Source DataBases (CSDB) has vastly improved the communications systems between OEMs, MROs, aircraft manufacturers and operators.

ATA Spec 2000 has defined common data formats for electronic data exchange, and this capability is heavily utilised for automated spares provisioning. A link between ATA Spec 2000 and SSCM will allow instant updating of component useage rates, and this can be input to the parts catalogues and component reliability databases in virtually real-time. This means that not only will unscheduled component replacements be captured via the normal SSCM event report system, but so too will scheduled replacements of lifed items for overhaul.

This capability closes the loop for full understanding of component performance, and allows the continuous assessment of the validity of both reliability estimates and replacement period recommendations for lifed items.

As with the entire SSCM system, getting the maximum benefit from the ATA Spec 2000 link will take time. The ATA model is not yet in widespread use, but is growing rapidly, and now is the time to maximize its benefits by paralleling with SSCM. Together over a period of time, they will build into a co-ordinated and effective system that will finally enable the obsolete Mil-Hdbk-217F, NPRD 95 and other databases to be pensioned off completely.

5.7 SAFETY PERFORMANCE ALERTS

For ensuring aircraft systems are both designed to and are performing in a safe manner to acceptable levels, this is the core section of SSCM. This is the first time that a capability has existed for virtually instant, automated and continuous assessment and re-assessment of safety compliance, coupled with a warning system to every interested party when things start to wrong, and before they can potentially lead to an accident.

At the initial design stage, system safety analysis, primarily in the form of FMECA and FTA, is embedded within SSCM, and uses the parts reliability database as the source of its core data. Due to the automated alert system built into SSCM, it is therefore evident that even at this early stage, any non-compliance with FHA requirements will automatically be highlighted and require the design team to revisit their system. Additionally, should the design analyst

select a part that does not appear in the database, this too will trigger an alert, which can only be cleared by means of an acceptable justification statement by the design team, such as:

- New part with no in-service history – reliability estimate based on comparison with similar equipments, or on prototype test results
- Insufficient data for confidence in the database – estimate to be validated by testing

Following entry into service, any degradation in safety levels, within the trend parameters detailed below, are automatically triggered to both the aircraft manufacturer and the system OEM simultaneously. However, allowing SSCM to do this on an event-by-event basis, even if it were possible to receive daily flying hours updates for an entire aircraft fleet (which it is not), would be unwise, since daily variations and unexpected operational changes, could result in short-term wild swings in reliability which might trigger spurious alerts.

For the alert system to be effective, the automatic compliance check will therefore be performed on a monthly basis, following upload of the aircraft fleet flying hours data from the aircraft manufacturers (see section 5.3.8).

FHA compliance level	**Trend analysis results**	**Alert colour / type**	**Action taken**	**Close-out requirement**
Catastrophic $<1x10^{-9}$	Declining reliability over three consecutive months, but still at or in excess of certificated compliance levels	Cyan - advisory	Manufacturer required to comment within 30 days	Reliability reverts to previous levels for three consecutive months
	Declining reliability over three consecutive months, still compliant, but below certificated	Amber – caution	All operators advised. Manufacturer required to advise proposed corrective action within	Reliability reverts to previous levels within three months and remains there for three further

FHA compliance level	**Trend analysis results**	**Alert colour / type**	**Action taken**	**Close-out requirement**
	compliance levels		10 days	consecutive months
	Non-compliant	Red - warning	Regulators and all operators advised. Manufacturer required to advise proposed corrective action within 5 days	Compliance achieved within two months and regains previous levels within a further three consecutive months
Hazardous $<1x10^{-7}$	Declining reliability over three consecutive months, but still at or in excess of certificated compliance levels	Cyan - advisory	Manufacturer required to comment within 30 days	Reliability reverts to previous levels for three consecutive months
Hazardous $<1x10^{-7}$ (continued)	Declining reliability over three consecutive months, still compliant, but below certificated compliance levels	Amber – caution	All operators advised. Manufacturer required to advise proposed corrective action within 10 days	Reliability reverts to previous levels within three months and remains there for three further consecutive months
	Non-compliant	Red - warning	Regulators and all operators advised. Manufacturer required to advise proposed corrective action within 5 days	Compliance achieved within two months and regains previous levels within a further three consecutive months
Major $<1x10^{-5}$	Declining reliability over three consecutive months, but	Cyan - advisory	Manufacturer advised and asked to comment	Reliability reverts to previous levels for three

FHA compliance level	Trend analysis results	Alert colour / type	Action taken	Close-out requirement
	still at or in excess of certificated compliance levels			consecutive months
	Declining reliability over three consecutive months, still compliant, but below certificated compliance levels	Amber – caution	All operators advised. Manufacturer required to advise proposed corrective action within 30 days	Reliability reverts to previous levels within three months and remains there for three further consecutive months
	Non-compliant	Red - warning	Regulators and all operators advised. Manufacturer required to advise proposed corrective action within 10 days	Compliance achieved within two months and regains previous levels within a further three consecutive months
Minor $<1x10^{-3}$	Declining reliability over three consecutive months, but still at or in excess of certificated compliance levels	Cyan - advisory	Manufacturer advised and asked to comment	Reliability reverts to previous levels for three consecutive months
Minor $<1x10^{-3}$ (continued)	Declining reliability over three consecutive months, still compliant, but below	Amber – caution	All operators advised. Manufacturer required to advise proposed corrective	Reliability reverts to previous levels within three months and remains there for three

FHA compliance level	Trend analysis results	Alert colour / type	Action taken	Close-out requirement
	certificated compliance levels		action within 30 days	further consecutive months
	Non-compliant	Red - warning	Regulators and all operators advised. Manufacturer required to advise proposed corrective action within 20 days	Compliance achieved within two months and regains previous levels within a further three consecutive months

Table 9 - Safety Performance Alert Matrix

In order to assist early understanding and familiarity with this aspect of SSCM, it has been decided to use an alert colour and descriptor method based on that found in on-board aircraft systems such as Engine Indication and Crew Alerting System (EICAS). This system uses colour codes as attention getters, which require different levels of reaction as the hazard level increases. Thus a cyan colour indicates an advisory level, which may or may not require some action to be taken, amber indicates caution, and red indicates a warning. The degree of action required is decided by reference to the standard FHA compliance levels of catastrophic, hazardous, major and minor.

The SSCM software will automatically trigger these alerts, which will stay "live" on the system until the designated necessary close-out action has been completed. Visibility of this activity will be clear to all concerned parties, including the regulators.

Thus system safety analysis performed at the design stage, is continually assessed for accuracy throughout its in-service life. Any significant downward trends in reliability and hence safety levels are immediately brought to the attention of the regulators, the aircraft and systems manufacturers, and the operators, all of whom will continue to have on-line visibility of progress towards a resumption of FHA compliance.

5.8 SSCM OWNERSHIP AND ACCESS

Obviously, for SSCM to be both acceptable and accessible, it must be "owned" and maintained by a recognised and respected international aviation body. This initially suggests two choices, IATA or ICAO.

As previously discussed, IATA is already in the early stages of running its STEADES programme, and SSCM is a logical extension of this activity, bringing considerably enhanced benefits and greatly expanding the usefulness of the existing STEADES system. This is the preferred option for SSCM.

The alternative is ICAO under the umbrella of the SARPs system. However, as standards and recommended practices, SARPs do not necessarily have the weight required to drive SSCM into the industry to the extent needed for it to become effective in improving safety levels.

A further option would be for the aircraft manufacturers to take responsibility and ownership of the system, and if necessary, pay the operators for their data. This option is certainly the view of the former manager of the BASIS system.

In summary:

1. Who owns the database? IATA as an extension of STEADES, ICAO under the SARPs umbrella, or the major aircraft manufacturers.
2. Who has access to it, both for input and for data analysis? Input – every operator, aircraft manufacturer, OEM, repair organisation, military? Analysis – detailed analysis and feedback of full database by IATA. Manufacturers allowed access to those items for which they have responsibility by tying part number with supplier codes. Other items can be searched for current reliability performance by part number only.
3. How can the industry as a whole be persuaded to use it? By demonstration of cost benefit of getting reliability and safety right at the design stage and by identifying the need for corrective action before

trends start to hurt. Look at the current cost of fixing all the small events and continually re-inventing the wheel.

5.9 IMPLEMENTATION

Having established SSCM functionality requirements and drawn up a draft system architecture, the next step will be to plan a road-map to full implementation. As has already been suggested, it is proposed that IATA adopts SSCM as an additional function to STEADES, but many other links are also required, not least to other existing "satellite" systems such as ATA Spec 2000 and the existing proprietary data capture software packages such as Sentinel.

The principles steps in the implementation road-map will be:

1. Present SSCM principles to major interested parties, including IATA, ICAO, Flight Safety Foundation (FSF), GAIN, IFA, aircraft manufacturers, CAA, JAA, EASA, FAA and a selected groups of representative worldwide airlines
2. Set-up an industry working-group to refine system requirements and identify the system "owner"
3. Identify linking systems and agencies
4. Draft legislative requirements
5. Database design
6. Detail network system design, costs and timescales for introduction
7. Prototype system tests
8. Commence upload of existing data from other systems
9. Identify participants in initial trials
10. Install system for trial
11. User training
12. One year trial and report
13. Review system and refine as required
14. Full-scale promotion and implementation
15. Feedback and review
16. Introduction of legislation

17. On-going review and feedback

Participants in the one-year development trial should include at least one:

- Industry body, such as ATA, IATA, ICAO, etc.
- International safety agency, such as FSF, GAIN, IFA
- National carrier
- Low-cost carrier
- Charter carrier
- Fractional ownership company, such as NetJets
- Sole-user business aircraft operator
- Military air arm
- MRO
- Aircraft manufacturer
- Tier 1 aircraft system supplier, i.e. one which interfaces directly with the aircraft manufacturer
- Tier 2 aircraft system supplier, i.e. one which does not have a direct interface with the aircraft manufacturer
- Component supplier
- Existing in-service data system company – although this is likely to be difficult given that SSCM is designed to replace their system
- Regulator
- SAE
- Reliability and safety analysis specialists

It is anticipated that the overall timescale to full implementation at step 14 could take up to five years, with perhaps a further two before legislation could reasonably be expected to be in place.

5.10 DATA READ-ACROSS FROM EXISTING SYSTEMS

Although SSCM is intended to eventually replace a whole host of existing systems, this will not be at the expense of the vast amount of valuable data already embedded within them. There are three principle areas to consider

here, reliability databases, other in-service data monitoring systems and the overall database software compatibility.

5.10.1 Reliability Databases

Starting a new reliability database from scratch is obviously undesirable, for the simple reason that it will take a very long time indeed to build up sufficient data to start being useful. Therefore it is essential that the maximum possible use is made of the many years data contained in the existing databases.

However, as has been shown, many of these contain much data that is either hopelessly inadequate, out of date or just simply wrong, and deciding which data to use and which to reject will not be an easy task. Ideally of course, it would be nice to think that an existing compatible database could simply be linked electronically to SSCM, but the reality is that there is very little chance of any of them having sufficiently robust and trustworthy data for this to be permitted. Therefore, a small working group of reliability consultants and other experts in the field will be established to draft the procedure for the task of data identification for upload.

Ultimately, but certainly well before the SSCM trial period commences, incorporation of existing parts databases will gradually start as they are sense checked for relevance and currency. As SSCM starts adding to this data, sense checks will be carried out to ensure compatibility and that no sudden trend changes indicate a data mismatch. Some way into the implementation process, a point will be reached at which the old database has yielded all its useful data. Then a recommendation can then be made to the SSCM Working Group to "switch it off", provided of course, that the change over to the new system has been clearly signalled to every user of the old database.

5.10.2 Other In-Service Data Monitoring Systems

In many ways, this will be a similar process to that just described for reliability databases, with the important exception that many – even most - of these

monitoring systems will continue after the introduction of SSCM. They will however, feed into and be able to retrieve data from, the new system.

Once again, a working group will identify desirable data sources and make recommendations for either direct upload into SSCM or database links.

5.10.3 SSCM Database Software

Obviously at an early stage, the choice of which proprietary database software package to use as the framework for SSCM must be made. In view of the potential for the system to ultimately become very large indeed, with a high data storage requirement, the answer will lie in the use of linked or relational databases.

Work will need to be done to assess the probability of error within the chosen database software itself, and this error-proneness will be the deciding factor in the final selection. In order to address this properly, it is proposed that an established reliability software consultant company would be contracted to design the database using their expertise to select the most appropriate software to run under all Microsoft Windows Operating Systems.

5.11 FUNDING

Until such time as the first four steps in the implementation road-map have been completed, the detailed funding requirements cannot be identified. The question remains though, who is going to be expected to pay for it?

Apart from the need to educate the industry about the need for the system to ensure longer-term maximum take-up by users, some key players can be expected to be potential sponsors during the early stages. Perhaps initial investigation, design, trial and set-up costs might be financed by the initial working group (including of course the eventual system owner), with further support coming from other interested parties including aircraft manufacturers and tier I system suppliers. The annual running costs will be levied equally

across all users through the usual commercial mechanisms of licences and annual renewal charges.

Based on earlier work in industry, it is estimated that the initial database design and formatting, contracted out to an established reliability database specialist will cost in the order of $8,000 - $10,000.

5.12 REGULATORY ISSUES

Finally therefore, we come back to the question of regulation. For SSCM to be acceptable to the industry, it must of course go hand-in-glove with legislation, whether that comes from EASA or some other body. In an environment already controlled by far more legislation than any other transport industry, there will undoubtedly be resistance. Nevertheless, the need for more stringent legislation in the whole area of aircraft system safety analysis and on-going in-service monitoring has been amply demonstrated, but how can the regulators be persuaded?

Currently, the exact role of EASA within the continued airworthiness domain remains unknown. It is time for IATA, ICAO or one of the existing legislating organisations to make the case for an SSCM-type system direct to the EASA rule-makers.

5.13 WILL IT WORK? – CASE STUDY

In order to demonstrate the potential effectives of SSCM, let us look at another case study. In late 1999 through to the middle of 2000, the BAE Advanced TurboProp (ATP) airliner fleet began to suffer a sudden alarming increase in the removal rate of its engine-mounted AC generators. Over a period of several months, generators were failing on engine start-up on a regular basis, ultimately doing so at the rate of almost once a week.

It soon became apparent to the OEM, who was receiving the generators for repair, that just one operator was suffering the problem. Furthermore, every

single generator returned was found on investigation to have failed due to some unknown external cause.

However, the investigation by the OEM's repair shop was severely hampered by the poor quality data coming from the operator, who quite evidently had no system for capturing aircraft event information. For example, documentation accompanying the equipment on return was sparse in terms of meaningful information, with statements such as "Not Known" in proliferation. Furthermore, although attempts to get additional information directly were made by both the OEM and the aircraft manufacturer, it was simply a case that no meaningful data gathering existed within the airline.

Meanwhile, the operator continued to try and understand the nature of the problem, primarily through the use of on-the-spot discussion as each failure occurred, and by reliance on engineering memory to tie in with previous events. One highly significant point, which did finally come to the OEM's attention, was the fact that all the failures were occurring on just one aeroplane in the fleet, something not properly recorded by the operator. A sequence of uncoordinated, almost desperate engineering fixes were tried, which included combinations of engine changes, swapping generators over from one side of the aircraft to the other, and so on.

Eventually, the source of the problem was found through detailed investigation by the aircraft manufacturer, which included extensive searches through uncoordinated engineering records and pilot reports at the operator. This revealed that for some time prior to the start of the sequence of apparent generator failures, crews had been suffering from unexplained ground power connection problems with the same aircraft, but in the absence of a robust audit trail of information, these problem indicators were missed. Thus the link between aircrew reports and apparently unrelated engineering actions on "failing" main generators was never made, and the actual failure mode, which was ground power overload damage to the main generator windings took far longer to identify than it should.

The elapsed time from the realisation that a significant problem occurred to the final discovery and repair of the cause, took almost six months. This was obviously very costly for all parties concerned, not least the airline who had to frequently take the aircraft out of service or seriously delay its dispatch. Had the airline had SSCM in place, it is highly probable that, with regular and coordinated data analysis, the following sequence would have occurred:

1. Increasing incidences of ground power problems seen, related to one particular aircraft. This in itself would have lead to an early engineering investigation and the discovery of a faulty ground power control unit.
2. Even if point 1 had not yet on its own brought about an investigation, incoming data revealing a sudden spate of generator changes on the same aircraft, at the same phase of operation, i.e. on the ground before flight, would certainly have done so.
3. Trend analysis would easily have triggered the requirement to take action far sooner than actually occurred, and this would have resulted in the early realisation of the link between the 1 and 2, facilitating a much quicker resolution of the problem.

It is estimated that in this case, SSCM would have saved approximately three months of investigation manhours and in the order of seven or eight generator replacements and repairs. Each repair on its own cost the airline approximately $60,000. This case, although thankfully not as extreme as the Alaskan MD-80 discussed earlier, shows remarkable similarities in a failure to recognise the need for robust procedures for data capture. Both cases would thus have benefited from SSCM.

5.14 WILL IT WORK? – CURRENT SYSTEM FLAWS

In Chapter 4, the current analytical system was described and illustrated and the five fundamental flaws which act to significantly reduce its effectives, were shown to be:

1. Feedback from maintenance to PDS.

2. Retrieval of event data from maintenance into a PDS analytical database.
3. Dataflow from PDS to lessons-learned.
4. Interrogation of PDS databases by design teams.
5. Feedback from operator to design team.

The automated, linked database nature of SSCM, which covers all areas of the system from operator right back to. component reliability databases, will mean that all these flaws are corrected, indeed items 1, 2 3 and 5 in the list above are embedded as automatic functions within SSCM. The only required human action item is number 4, but the very fact that the model will become the main driver for corrective action and that events will require action before they can be closed off, can only serve to keep design teams alert to the information available to them to reduce their workload and shorten development and modification timescales and cost.

5.15 ANALYSIS OF THE BENEFITS OF SSCM

So, apart from the overall aims and objectives of the SSCM system, how can the benefits be measured? The answer comes in five parts;

1. An overview of the cost of an accident or major incident to the industry
2. The results of two surveys of air transport industry students attending the MSc Air Transport Management and Air Safety Management programmes at City University
3. Conclusions drawn from a survey of airline flight safety personnel, carried out by GAIN during their 2003 World Conference in Rome
4. Direct quotes drawn from students coursework for the MSc module on Safety Analysis and Statistics
5. Estimation of possible time and cost savings in a specific case study

5.15.1 The Cost Of An Accident

The cost of a hull loss accident to the air transport industry is huge. The figure below shows just how expensive it is in real terms, showing the combined

annual cost of the aircraft loss and the accident liability to the world airline industry.

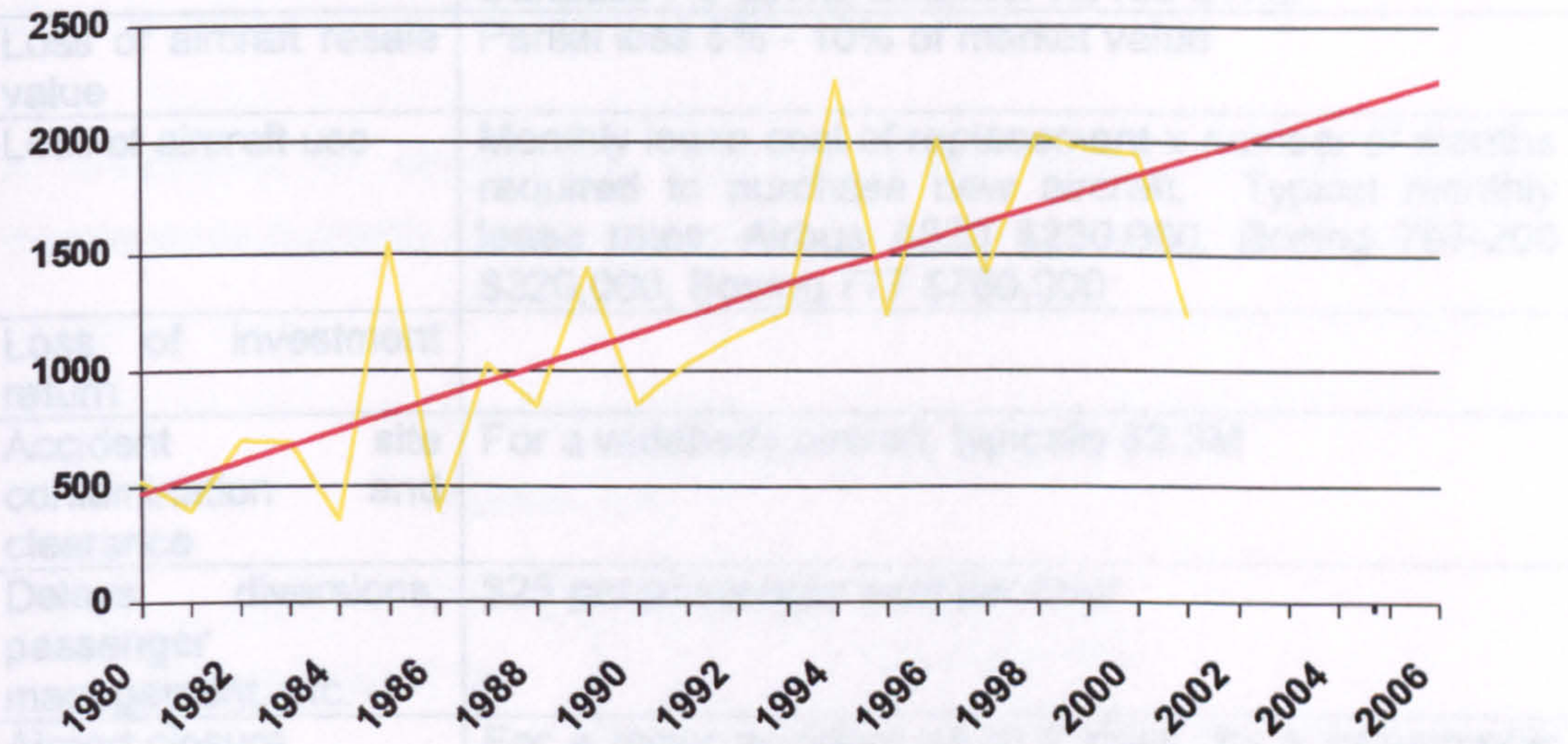


Figure 19 - Hull and Liability Costs 1980 - 2002

Two years ago, the National Aerospace Laboratory in the Netherlands, in association with Airclaims in the UK, produced a document [75] which analyses the cost benefits of effective safety measures to the air transport industry. Their work shows that the average cost to the industry of a catastrophic hull loss accident is now $3.05 million for every passenger killed.

Beneath that stark figure lies a very detailed breakdown of the various cost elements incurred by the industry in the case of such an event, or indeed when a lesser incident occurs, and these bring into sharp focus the potential savings that SSCM can be expected to bring. These cost elements are shown in table 10 below.

COST ELEMENT	AVERAGE COST
Aircraft physical damage	Minor accident 15% of value, catastrophic 100%. Example new –build aircraft costs; Airbus A3250 $56M, Boeing 747-400 $185M, Canadair RJ $27M, Embraer RJ135 $17M
Loss of aircraft resale value	Partial loss 5% - 10% of market value
Loss of aircraft use	Monthly lease cost of replacement x number of months required to purchase new aircraft. Typical monthly lease rates; Airbus A320 $230,000, Boeing 757-200 $320,000, Boeing 777 $760,000
Loss of investment return	
Accident site contamination and clearance	For a widebody aircraft, typically $2.3M
Delays, diversions, passenger management, etc.	$25 per passenger seat per hour
Airport closure	For a minor accident up to 2 days, for a catastrophic accident up to 5 days
Passenger and crew deaths and / or injuries	$3.05M each
Loss of staff investment, training, etc	Training cost of a replacement pilot $55,000
Loss of cargo and / or baggage	Baggage may be up to $52,000
Search and rescue costs, plus emergency services	Average $693,000
Airline immediate response activities	Average $3.4M
Accident investigation	Minimum $2.4M
Third party damage	As for passengers
Loss of investment income	To insurers on monies paid out
Increased cost of insurance	Loss of 20% discount
Loss of income	Passengers avoid the airline
Loss of reputation	Felt by both the airline and the aircraft manufacturer
Loss of company value	Share price decline
Social costs	Road closures, delays, loss of power, and so on
Loss to society	Loss of tax, personal skills, etc
Emergency remedial actions	Airworthiness Directives, modifications, etc
Legal costs	Fines, punitive damages, criminal proceedings

Table 10 - Cost Elements Of An Aircraft Accident Or Incident

Once again, we find similar indicators of cost benefits when looking at the potential for a reduction in the levels of unscheduled maintenance brought about by early or unexpected system failures.

A breakdown of an airline's operating costs shows that on average, maintenance currently contributes around 8% of the total, as shown in figure 20.

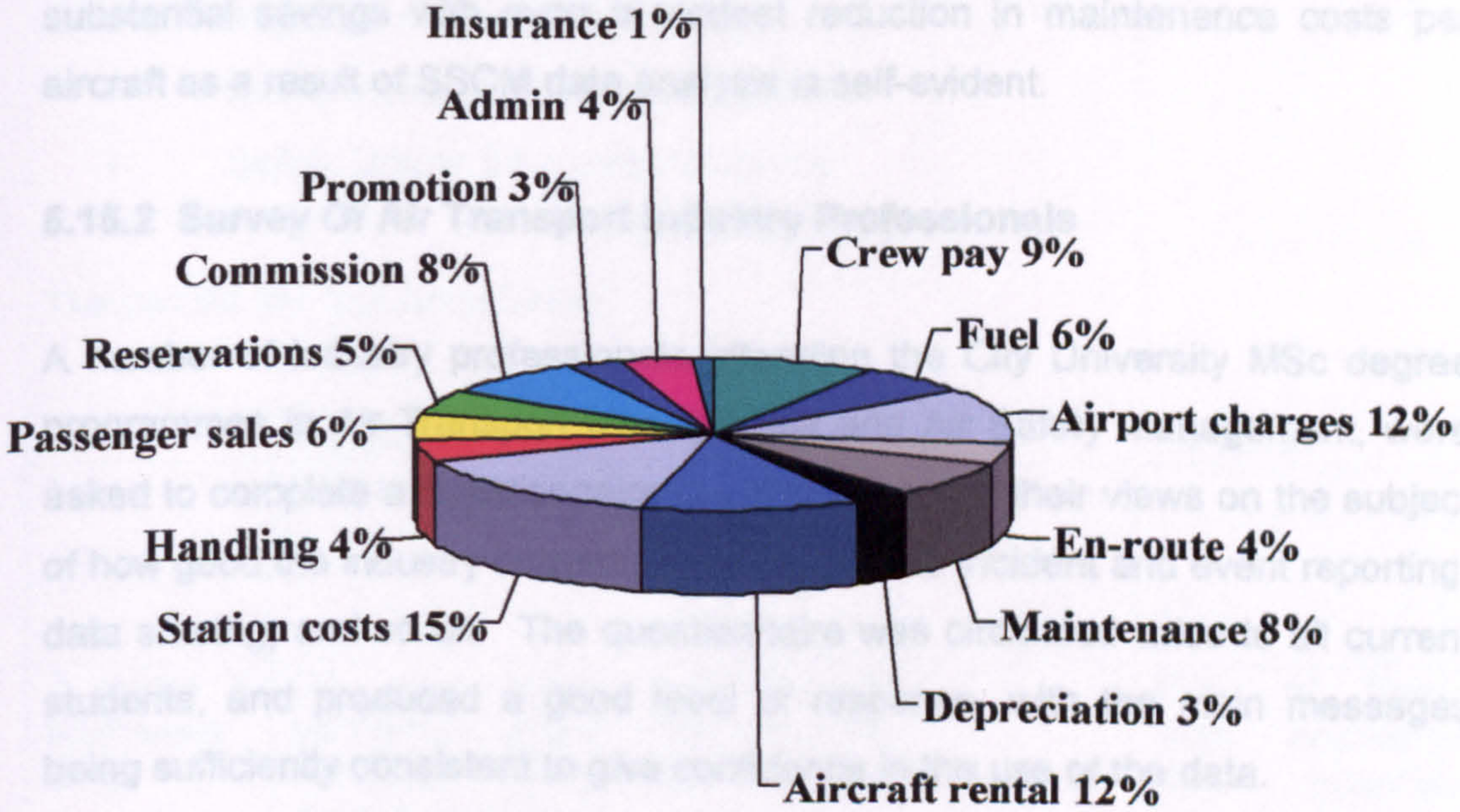


Figure 20 - Typical Airline Operating Costs *(ICAO)*

Driving down this cost is of course, a perpetual aim within any airline, especially when you consider that a single Airbus A320 flying a typical 2,650 hours a year, costs on average, getting on for $11 million to operate. This sum breaks down as follows:

- Leasing $2,650,000
- Insurance $400,000
- Fuel $1,854,676
- Flight crew $850,560
- Cabin crew $584,760
- Maintenance $1,501,128
- Navigation $161,172

- Landing $484,659
- Handling $816,710
- Sales & reservations $290,160
- Commission $1,322,259
- General & administration $631,184
- Total $10,696,708

Multiply this sum by the number of A320s in a fleet, and the potential for substantial savings with even a modest reduction in maintenance costs per aircraft as a result of SSCM data analysis is self-evident.

5.15.2 Survey Of Air Transport Industry Professionals

A number of industry professionals attending the City University MSc degree programmes in Air Transport Management and Air Safety Management, were asked to complete a questionnaire designed to solicit their views on the subject of how good the industry currently is with regard to incident and event reporting, data sharing, and so on. The questionnaire was circulated twice to all current students, and produced a good level of response, with the main messages being sufficiently consistent to give confidence in the use of the data.

39 students responded, including:

- AAIB safety investigator
- Air traffic controller working for NATS
- Air traffic controller in Malta
- Air traffic controllers (2) with the Royal Air Force
- Aviation consultant specializing in asset management
- Commercial pilots (11) working for national airlines, two of whom are also Quality / Safety Auditors, and another is a Flight Safety Officer
- Flight crew training officer with a national airline
- Commercial pilots with regional airlines (5), one of whom is also an international consultant in airline operations at higher management level
- Business aviation pilot

- Engineer working for an aircraft & systems manufacturer
- Engineers (3) working for national carriers
- Engineer working for a UK charter airline
- Engineer working for a VVIP flight
- Helicopter operator Commercial Manager (Engineering)
- Helicopter pilot and Safety Manager in the Middle East
- Operations manager with a national airline
- Royal Air Force fast jet pilots (2)
- Royal Air Force transport pilot
- Safety Managers (2) for UK airlines
- Safety Officer for a national airline

The results are tabulated below.

	Question	**Response**	**Remarks**
1	What is your role?	See above	
2 (pilots & engineers only)	Do you have any concerns about the reliability of your aircraft systems?	Yes x 15 No x 14	**52% of those who answered this question are concerned**
	If you answered yes, please give examples	See responses	
3 (pilots only)	How often, in percentage terms, do you have to refer to the MEL prior to dispatch. (Please indicate aircraft type(s))	60% (B747-200) >50% x 1 30% - 40% x 2 (both 747-400) 1% x 2 (B737-800, Falcon 20, King Air) "Hardly ever" (A330/A340, 737-800) 2% (757, 767) 5% x 4 (including very new Airbus fleet and 737-300 fleet) 10% x 4 (including very new Airbus/Boeing fleet and Bell helicopter fleet)	See responses

	Question	Response	Remarks
		15% x 1 (new A320 fleet) "Most flights" (C-130)	
	Have systems ever failed in an unexpected way?	Yes x 15 No x 8	**65% experience unexpected failure modes**
	If yes, have they ever done so in a way that you considered to be dangerous?	Yes x 11 No x 4	**73% experience dangerous unexpected failures**
4	Does your company have an incident / event reporting system (confidential or otherwise)?	Yes x 37 No x 1	**97% have reporting systems**
	If you said yes, does the system capture input from all areas of the business?	Yes x 20 No x 13	See responses
	Does the system allow you to enter all the information you would like to?	Yes x 25 No x 9	**26% cannot enter all the information they would like to**
	Is the system easy to use?	Yes x 29 No x 5	**86% say their existing system is easy to use**
5	If you said yes to question 4, is the system effective?	Yes x 21 No x 13	**38% say their systems are not effective.** See responses
	If you said no, why is it not effective?		See responses
6	When you enter something on the system, do you get effective feedback?	Always x 9 Usually x 14 Rarely x 10 Never x 2	**Only 25% always get feedback**
7	Do you have access to general reporting systems such as BASIS?	Yes x 20 No x 17	**46% have no access to general reporting systems**
	If you said yes, do you find it useful?	Yes x 17 No x 2	One respondent said "yes and no"
	If no, why not?		See responses
8	Do you know if other operators of the same aircraft types share your problems and issues?	Yes x 13 No x 14	See responses

	Question	Response	Remarks
	If no, why do you think that is?		See responses

Table 11 - Student Survey Results

Written responses, with added comments to show the links in to SSCM, are detailed below.

Question 2 – do you have any concerns about the reliability of your aircraft systems?

"Yes. Increasing (apparent?) incidence of Tornado engine problems – particularly vibration captions." (RAF pilot)

"Yes. IFE is unreliable and prone to fire." (Captain with national airline)

The use of the word "apparent" is a clear indication that in-service arising feedback to the operator is not as it should be. SSCM addresses this.

"Yes. No specific types." (AAIB safety investigator)

"Yes. Manufacturer's insistence upon bringing into service an FMS upgrade (A320 FMS2) which is known and documented by themselves to contain many serious 'bugs'." (UK airline Safety Manager)

"Yes.

1. I fly Airbus FBW aircraft. They are entirely dependant on software to function. In a period of terrorist activity how much security is placed on this software?
2. The Airbus product has defined limits of speed, G, etc., that the pilot cannot exceed. It may be necessary to exceed some limits one day to avoid an accident. Boeing allows this in the 777 flight control laws.
3. Finally, the Airbus control systems make their own control inputs on top of pilot's inputs to manual flight. This makes the aircraft unpredictable/unpleasant and perhaps unsafe in some conditions. This

is particularly so in gusty conditions near the ground." (Long-haul pilot with a national carrier)

This seems to indicate an unsatisfactory design feature which is not being feedback to the industry strongly enough to generate action. SSCM will facilitate this.

"Yes. We are getting a lot of Flight Management Computer (FMC) resets including a number of dual latches."

"Yes. Trent 700 and Trent 800 FADEC systems and engine compressors." (Engineer with a national carrier)

"Yes. Poor reliability of reversers on A330, poor corrosion resistance on the A320, fuel control on Boeing 757." (Engineer working for a UK charter airline)

"There are always systems that fail." (Long-haul pilot with a national carrier)

"Yes. Leading edge flap light on/off intermittently in flight." (B747-200 pilot)

"Yes. The aircraft onboard entertainment system electrical wiring is a big concern where many electrical sparking and other anomalies are taking place in many international airlines without proper action or follow up by either the authorities or the aircraft manufacturers. Another concern is the aircraft cabin fire extinguishing system, where statistically most cabin smoke or fires can be disastrous, for both human and technical reasons." (Long-haul pilot)

General comment on question 2: It is obvious, but not surprising, that there are still many concerns over system reliability within the user community. Increasing the awareness levels of such issues, hopefully leading to corrective action being taken, is one of the principal aims of SSCM.

Question 3 – how often, in percentage terms, do you have to refer to the MEL prior to dispatch? (Please indicate aircraft type(s))

"On all operational missions; for peacetime training, list of acceptable defects is more subjective, open to flexible interpretation depending upon scenario. Tornado F.3." (RAF pilot)

"Always when there is an entry of deferred defect in the logbook." (Long-haul pilot with a national carrier)

"The MEL can be difficult to interpret." (Captain with national airline)

The question of subjective interpretation of MEL requirements may at first glance appear specific to the military environment, but several MSc students have said off the record, that they come under considerable commercial pressure to accept aircraft faults that they would not normally do. This appears to be particularly true in the short-haul, low-cost world. SSCM would not allow such events (when reported) that result in safety alert levels being triggered, being ignored.

Question 4 – does the reporting system capture input from all areas of the business?

"Yes. Integral part of overall safety management system." (Helicopter company manager)

"Yes, as far as JAR requires it." (Regional airline pilot)

"No, pilots only." (Engineer with national airline)

"Yes, but some faults go unregistered." (Captain with national airline)

"No, people are afraid of reporting." (Long-haul pilot with a national carrier)

A very familiar story, providing evidence of an appalling safety culture in this case. Legislated confidential reporting will help, but the cultural change here is key.

"I believe it does." (Short-haul pilot with national carrier)

A communication breakdown here, he should know.

"The system in place only captures from the operational side of the airline." (Captain and Quality Auditor)

"No access to it except a written report that will be taken into account or not." (Regional airline pilot)

Is the system easy to use? "Yes, I tell the engineer what is wrong – he takes care of the paperwork." (RAF transport pilot)

"It's supposed to; however pilots seem to be the most likely to complete incident forms." (Helicopter pilot and Safety Manager)

"Yes, but not without chasing." (Engineer working for a UK charter airline)

Another cultural issue, where either the importance of event reporting has probably not been communicated well, or perhaps the system is not easy to use. SSCM addresses this latter point.

"I am only familiar with the ATC and aircrew reporting systems, but I am aware of the engineering ones that exist." (Air traffic controller with the Royal Air Force)

"No. The system only concentrates on the technical part of any incident or accident, neglecting other important aspects in the airline operations." (Long-haul pilot)"Yes. Engineering Operations, Flight Dispatch, Ground Operations, Training." (Engineer with a national carrier)

"No, flight ops and ground handling." (Pilot with a national airline)

"No. System concentrates on operational formal reporting, although it is being developed to encourage informal reporting from other areas of the business such as R&D". (NATS air traffic controller)

"No, only from the techs involved with the actual problem, which is then evaluated by the quality department." (Engineer working for aircraft & systems manufacturer)

A very narrow view in this company of the need for event reporting, which areas of the business should be doing so, and even more alarmingly, evaluation is performed by one department in isolation rather than in regular multi-skilled forums.

"Airport services, flight ops, engineering, cabin safety." (B747-200 pilot)

Does the system capture input from all areas of the business? "I can't really tell, but I suspect it does not." (Regional airline pilot)

Does the system allow you to enter all the information you would like to? "Don't know, it's the engineer's domain." (RAF transport pilot)

"No, human factors elements are not captured effectively yet." (RAF fast-jet pilot)

Question 5 – Is the system effective?

"Yes, but it took a lot of work to achieve employee/shop floor "buy-in" which is essential, prior to employee buy-in the system was very much reactive (i.e. not reacting to cited maintenance errors, MOR, Voyage Reports, etc), post buy-in the system is proactive, and has become a true Safety System." (Helicopter company manager)

A success story of change in a company culture. This is vital in understanding how safely they are performing.

"It is as effective as the user makes it (Flight Safety Department)." (Pilot with a national airline)

"No, not very effective because you rarely get feedback." (Pilot with a national airline)

"No. The system is via a paper form that goes through the military system and, whilst it is a report to primarily warn other controllers of areas, controllers are concerned that it could lead to disciplinary action." (Air traffic controller with the Royal Air Force)

"No, because there is no way to assess it and we crew members suspect it could be used as a personal penalty tool rather than a safety improvement one." (Regional airline pilot)

"Incredible but true, the 'no blame' culture although promised, does not truly exist. Hence controllers are reluctant to report occurrences in the first place. Secondly, there is a general feeling that when 'errors' are committed by pilots, investigations are rarely initiated or given due importance, unlike those when a controller is thought to be at fault. The latter might be more a cultural and/or political influence." (Air traffic controller)

"Yes, within boundaries." (Captain with national airline)

"In most cases, very little is done quickly. There are many issues that have needed changing for in excess of five years that affect flight safety." (RAF transport pilot)

"Probably because it is so easy to use, it lends itself to a lot of information being reported that is not of a safety nature. This adds a lot of work to sift through." (Engineer with national airline)

"No. My company has two systems, one incident/event reporting system that is compulsory to fill out, and one confidential reporting system directed to the head of the flight operations department for any deviations or other safety matters. Both systems, although good in their layout, are rarely followed with effective feedback or even action." (Long-haul pilot)

"No. I believe that in some cases it may be sanitised." (Long-haul pilot with a national carrier)

"No. More robust follow-up required." (B747-200 pilot)

"No, because it was implemented only to fulfill the legal obligations regarding safety, and people are not used to the system, it is not useful." (Long-haul pilot with a national carrier)

"No. It is not an open system and tends to be opinionated by a selected few. On occasions opinions/conclusions are made before the completion of an investigation." (Engineer working for a VVIP flight)

"No. Needs controlled and flagged to personnel when action required." (Engineer working for a UK charter airline)

"We have a new web based system that does not work – yet." (Captain with national airline)

"The safety system currently in use is still under development. The system is aimed at capturing the current incident reporting forms and therefore should allow all relevant data to be captured if it is on the forms. The company is currently looking at making a web based front end for pilot wake-vortex incident reporting to allow capture of both pilot and ATC concerns." (NATS air traffic controller)

General comments on question 5: It is clear that reporting system effectiveness is being seriously compromised by:

- Poor company cultures
- The desire to protect data
- A lack of recognition of the need for appropriate review, follow-up and feedback

SSCM addresses these last two points.

Question 6 – do you get effective feedback?

"It has to be chased up on the internet." (Captain with national airline)

"Feedback can be requested." (Pilot with regional airline).

Not a good example of an effective safety culture in this case.

"We have to follow it up to find out the analysis and result." (RAF transport pilot)

"Always – it is part of the system to give feedback to all reporters." (Helicopter company manager)

This comment again comes from a company that has made substantial advances in changing its safety culture.

Question 7 – are general reporting systems such as BASIS useful?

"System is designed for fixed wing airline operations and not helicopter North Sea operations." (Helicopter company manager)

As SSCM evolves, one of the key aims will be to ensure continuous improvement of the model through adapting to both new and changing requirements in response to the needs of customers in all areas of the aviation industry.

"It's got restricted use." (Captain with national airline)

"Although useful, it is used to report totally non-safety related things, causing the database to fill up. Sifting through these items to find the relevant ones is time consuming." (Engineer with national airline)

"BASIS can be useful but is very dependant on the way that a report is entered into the system. Some of the assigned categories are very subjective." (Pilot with a national airline)

"I don't know much about BASIS, or its contents." (NATS air traffic controller)

"I don't know what BASIS is." (Air traffic controller)

"I acknowledge the usefulness as such. However I experience WinBASIS (at least the version used by my airline) as very user unfriendly." (Engineer with national airline)

"No, because only the people in the Safety Department have access to the system." (Long-haul pilot with a national carrier)

"Limited to use by flight safety manager and flight safety officer." (Captain and Quality Auditor)

Yet again, an example of a poor safety culture. SSCM addresses this.

"In my company we have a bulletin published by the safety department and the information given is mostly articles taken from magazines or the internet. If one needs more information, it has to be by personal relations or favours." (Long-haul pilot)

"The organisation has not yet adopted such a system, but it is thinking about it." (Engineer working for a VVIP flight)

Question 8 – do you know if other operators of the same aircraft types share your problems and issues?

"No. No idea if they have problems." (Engineer working for a UK charter airline)

"No. Limited information available on these types of aircraft." (Business aircraft pilot).

"No. I am not privy within my job function to have access to that sort of data." (Flight Crew Training Officer with a national airline, and therefore a very worrying answer indeed).

"Companies are not very good at sharing negative information, especially if it could put them in a bad light." (Pilot with a national airline)

"I have no idea." (Pilot with a national airline)

"No. Only receive internal company reports." (B747-200 pilots)

"As the 'hands-on' operator, my visibility of manufacturers engineering information is very limited and I only find out what is deemed necessary by the design authority." (RAF transport pilot)

"No, no information exchange." (Captain and Quality Auditor)

"Part of the reason is a perceived concern that sharing information may cause a company to lose a competitive advantage. If we are talking about aircraft system malfunctions, that's one issue that it would seem that most operators are comfortable sharing....I think many companies are reticent to expose their 'dirty laundry' outside of their companies." (Helicopter pilot and Safety Manager)

SSCM addresses these points through data security and de-identification, and industry-wide adoption at all levels of the business.

"Yes, in some cases more so than us, could be due to shortages in manpower." (Engineer working for a national carrier)

The students were asked two further questions:

1. **Any other comments about the understanding of aircraft system behaviour and reliability that you would like to make**

Responses:

"Pilots are taught less now about system behaviour but more specifics about system operation. That's OK, but there is a danger that this will go too far and result in a deficiency in understanding of system behaviour."

This view clearly reinforces what has already been said in this area.

"Very little appears to be being investigated and reported." (Engineer working for a UK charter airline)

A poor safety culture again.

"AAIB experience is that, in general, aircraft system behaviour and reliability is relatively good compared with the operators' perception as to what they are doing and how they actually work." (AAIB safety investigator)

"The RAF aircrew operating the C-130K take great pride in keeping the aircraft going. That is our downfall as we define the lowest operating standard of the aircraft based upon our skill rather than putting our foot down and requiring a minimum equipment level that would enhance our skill." (RAF transport pilot)

"With the new technology and systems interactions modern aircraft have these days, it is vital that training departments in any airline concentrate more on the

technical systems behaviour especially during anomalies, rather than depending solely on electronic monitoring, ignoring the fact that such systems may fail themselves. No system is completely reliable." (Long-haul pilot)

"Technical training is inadequate. Many systems are misunderstood e.g. windshear, EGPWS/GPS. The aircraft technical log has problems. Failure indications are a potential problem." (Captain with national airline)

"The RAF has recently operated its Tornados for protracted periods on sortie profiles and under conditions which were never previously anticipated (cf hot and high desert ops at medium altitude, vice low level ops in Central Region). This will inevitably disrupt predicted failure modes and rates, and calls for a flexible and proactive approach to risk management and mitigation." (RAF pilot)

A clear need here for SSCM's environmental analysis capabilities to feedback into the original design model and reliability models to ensure safety levels are not being compromised.

"Airbus is getting much better at sharing system problems with operators. I have just started an initiative to improve pilot/engineer problem sharing within my company." (UK airline Safety Manager)

"Modern electronic flight control systems have brought with them many tremendous safety advantages. The down side is the manufacturer's apparent inability to explain how they work and what the limitations are. An example of this was a recent run of incidents where actual or imminent Mach overspeed events resulted in momentary loss of control because a 'normal law flight control mode' protection was activating with no indication to the pilot that it had done so. As a result the pilots ended up fighting the aeroplane for control and minimal risk overspeed events turned into major risk altitude deviations in RVSM airspace – including one TCAS event during the recovery." (UK airline Safety Manager)

"Computerisation of aircraft systems is advancing by leaps and bounds. However, this is creating a gap between the designers and the engineers who have to maintain the product/systems. There is not enough published information to understand the logic of the systems as compared to the previous analogue or hybrid systems." (Engineer with a national carrier)

"Systems that fail in flight often test satisfactorily on the ground, then fail again in flight, giving little confidence in ground tests." (B747-200 pilot)

Possibly examples of:

- Poor or ineffective built-in test
- Poor fault diagnosis
- Incomplete information in Fault Isolation Manuals
- Poor communication/feedback
- No reporting system feeding into a lessons learned system

SSCM addresses all these points.

2. The air transport industry is concentrating its flight safety efforts almost exclusively on addressing what are known as "human factors" accident causes, such as CFIT, approach and landing, loss of control, etc. Do you think system behaviours and failures should also be addressed?

Responses:

"Yes" x 29. (AAIB safety investigator, engineer working for aircraft & systems manufacturer, Air traffic controller with the Royal Air Force, three engineers with national carriers, flight crew training officer with a national airline, engineer working for a UK charter airline, NATS air traffic controller, Maltese air traffic controller, nine long-haul pilots with national carriers, three short-haul pilots (one also a quality auditor), two RAF pilots, three airline Safety Managers, engineer working for a VVIP flight

"For sure." (Captain with national airline)

"Yes, but given that varying statistics attribute up to 90% of all hull losses to human factors, it would seem prudent to concentrate upon that particular area." (Helicopter company manager)

"The man/machine interface is prone to breaking down under pressure, and may cause loss of spatial awareness. Inherent systems failures, and system behaviour in differing autoflight modes should be addressed." (Flight crew training officer with a national airline)

"It seems right that we should be focusing the bulk of our efforts to improve safety on the critical interfaces between man and machine." (Aviation consultant)

"Everything fails at some time but the human element is the easiest (and most difficult) to control." (RAF transport pilot)

"They are addressed. This is particularly done by the manufacturers, the regulators and the engineering maintenance companies. However, the communications between these organisations and airlines' Flight Ops departments are not as good as they should be (cuts both ways). It's a mistake to equate the 'air transport industry' with airline flight ops, which are only a part of the business." (AAIB safety investigator)

Almost every respondent agreed that system issues must be considered alongside the human factors events. The results clearly show that there are some serious concerns among end-users regarding the safety and predictability of aircraft systems, and that the use of event reporting systems, while improving, is still not as it should be. Of particular concern is the apparent low degree of access to existing database systems such as BASIS, and in particular, evidence of persisting poor safety cultures.

The objective of SSCM is to overcome many of these issues, not only by being legislated, but also through its data protection protocols and by the use of an independent organisation to host the system.

5.15.3 GAIN Survey Of Airline Flight Safety Personnel

In the summer of 2003, GAIN approached flight safety personnel from five major airlines who had indicated they were willing to share lessons learned and corrective action data, and questioned them about their requirements for such a system. The key results are listed below, and serve to reinforce the need for SSCM. In each case, the respondent was given the option of assigning a high, medium or low priority to the need, and in every case, each item was identified as having a high priority.

- Provide an automated system for sharing lessons learned and corrective actions among airlines
- The system must be simple, user-friendly, easy, readily available, and inexpensive to work with
- The system must provide information in a timely manner such that it is communicated to those who can use it before it loses its value
- Identify trends based on incidents in the data so they can be addressed before an accident happens
- Support identification of...issues with specific aircraft systems...
- Users must be able to query, sort and trend information
- The system should automatically disseminate periodic safety summaries to airlines
- The system must provide a user-friendly search engine with drill down capability
- The system should include a web-enabled database application
- The organisation operating and maintaining the system must have no direct interest in the outcome, other than sharing of safety information
- The system must store and provide access to safety lessons learned and corrective actions
- All names must be removed from the data
- Include pilot anecdotal information
- Data categorisations must include aircraft types, types of flight operations, carrier size, etc.

- Types of data and information to be stored or referenced include:specific aircraft system discrepancies..
- Information stored in the system should be well-documented recommendations by the airlines for incidents experienced and the associated corrective actions
- Establish policies for data quality, data security, dissemination and de-identification
- Include dictionaries describing information issue areas in the system
- Sources of information should include...hazard reports, incident and accident reports, airfield audits, ramp safety audits...

SSCM as proposed, addresses all these issues and concerns.

5.15.4 Further Industry Professional Statements

In 2003, the MSc Air Safety Management module on Safety Analysis and Statistics, included coursework which asked the students to comment on a number of aspects of the airline industry's current safety performance. One question posed was:

What action would you take to improve the number and quality of incident reports within your company? What are the main barriers to successful data sharing between operators of similar equipments?

Responses included the following;

"Error must be accepted as a normal component of any system where humans and technology closely interact. Because it cannot be eliminated, effective measures must be employed to minimise its effects on aviation safety. But as the saying goes, 'You don't know what you don't know.' For us in the airline business this means that we may believe that we are aware of everything concerning our operation. But how can we be certain?" (Commercial airline pilot)

"Today our airline's data scope is limited because the only data guaranteed to be collected is that related to accidents or major incidents. A more proactive approach is needed if we are to move forward. We must create basic solutions instead of short term fixes." (Commercial airline pilot)

"The problem of civil litigation (in data sharing) is probably the most significant. The only possible solution would be to de-identify the information before sharing it." (Commercial airline pilot)

"Currently one of the greatest barriers to increasing the amount of data that is collected is the fact that there is a misconception that Air Safety Reports are purely a job for the pilots. To correct this problem a similar system would have to be made available to all employees within the company. These schemes could be an extension of the Air Safety Reporting programme with simplified forms, used for such groups as cabin crew and ground staff." (Commercial airline pilot)

"Care must be taken when comparing data derived from operators subject to different operating patterns and constraints, which may lead to the drawing of invalid conclusions. For example, fleets of similar aircraft operated under different conditions – e.g. multiple sectors versus fewer, but longer routes flown daily – may yield potentially widely differing arising rates. Similarly, climatic and local terrain conditions must also be taken into account when comparing results." (Senior Royal Air Force officer and pilot)

Thus it comes as no surprise that many of the same issues and concerns discussed in this document are in the forefront of the minds of people working at the coalface. It is also apparent that the SSCM system addresses all the concerns and suggested functionality raised by these students.

5.15.5 Cost Benefit Case Study

In section 3.23 the power generation problem on the Airbus A330 and A340 fleets was discussed. As stated, the engineering investigation needed to

identify the causes of the declining reliability took well over a year. This timescale was due to a number of factors:

1. The complex nature of the failure mechanisms being experienced, which had several causal factors
2. Some failures were occurring which had not been predicted in the design analysis stage to have such severe consequences or fail as often as they actually did
3. A high percentage of the failing units were not being returned to the OEM for repair, as they had passed out of warranty and were being repaired elsewhere by other organisations who did not share their findings with the OEM
4. Incomplete event data available to the OEM, whose FRACAS system relied on paper-based reporting. This meant that there was an over-long audit trail with the documentation typically passing through four or five pairs of hands before reaching the reliability and safety analysis team
5. Data lag due to the documentation system described above, resulting in delays of anything between one week and three months before all the details of a failure event were available for analysis
6. Data lag due to the aircraft flying hours, necessary for reliability calculation, only being issued by the manufacturer on at best a monthly basis, with some operators reporting quarterly, and others not reporting at all

So how could a fully implemented SSCM have improved this situation? The company concerned used a standard engineer's overheaded time cost figure of approximately $50 per hour. The average number of engineers involved in the defect investigation and modification design / testing at any one time was approximately five. Assuming their full availability for work was 20 hours per week for 46 weeks, or 920 hours a year, this equates to a total actual investigation cost of:

5 engineers x 920 hours x $50 = $230,000

Setting aside the possibility that a more robust design process may well have avoided problems 1 and 2 anyway, and concentrating on items 3 to 6, it is estimated that the time saving from a complete and near-instantaneous SSCM analysis capability could have alerted the team to the scale of the problem approximately three months earlier than was the case. Furthermore, the more detailed nature of the information flow from SSCM into the parts reliability database and the original FMEA, may well have taken a month out of the investigation effort.

From this it can be conservatively projected that the two full-time investigation and data analysis engineers in the process may have been able to complete their work in one month less than they did, thus saving around 20 hours a week for four weeks each, which equals 160 hours. The investigation cost now looks like this:

Actual cost = $230,000
Less savings due to SSCM, 160 hours x$50 = $8,000
Projected investigation cost = $220,000

It must be emphasised that these costs are for the investigation, design and test efforts only, and take no account of the potential for further savings in such areas as staff travel costs, involvement of additional part-time team members for review meetings, etc., etc. Further work on the cost benefit of an SSCM system is presented later on in this chapter.

Therefore, not only could a substantial saving have been made on the investigation, but also the modified equipment would have been brought to market and the fleet retrofitted and returned to acceptable levels of reliability much earlier than was the case. Furthermore, the team would have had the confidence to know that the lessons from the investigation had been adequately recorded for future reference in order to hopefully avoid a similar problem re-occurring in future.

5.16 SYSTEM SUMMARY

Several potential initiatives to assist the industry in its drive towards improved safety have already been highlighted. Of these, SSCM takes existing standards in event, incident and accident data capture and analysis, and takes them to entirely new levels of data intensity, functionality, feedback and alerting. It achieves this through completely new areas of data capture, interlinking with both existing databases and manufacturers design analysis, plus independence in ownership and support from legislation.

A roadmap for introduction has been produced, and in addition to its potential for accident and incident reduction, there are clear cost and time benefits to be had in both time-to-market of new designs and reduced operating cost in service through minimised unscheduled maintenance requirements.

5.17 THE NEED FOR A BUSINESS CASE

"I would contend that a major aircraft accident would not only cost the carrier infinitely more than any hoped-for saving, it could have the same detrimental effect on the aviation industry as another terrorist attack, We must allocate our funds wisely. Safety is not a disposable commodity." [76]

If operators are required to introduce the SSCM system, then logic suggests that the result is likely to be a reduction in the rate of undesirable occurrences at least, and possible even catastrophic events. However, in order to present SSCM as a viable business tool, it is necessary to demonstrate to the industry that the cost of implementation and long-term operation of the system can be significantly outweighed by the potential cost-saving through incident and accident prevention.

5.18 AUSTRALIAN STUDIES

Although there appear to be no available figures for a similar cost-benefit analysis, which is hardly surprising given the innovative nature of the proposal, some comparisons can be drawn with analysis carried out by the Civil Aviation

Safety Authority (CASA) in Australia. This work [77] assessed the potential for accident rate reduction following the introduction of Safety Management Systems (SMS) by air operators. The study looked at accident rates in New Zealand over the periods 1994 to 1998 and 1998 to 2000, which showed an approximate decline of between 10% and 20% dependent on aircraft category. An assumption was made that some of the difference was due to implementation of SMS and that their progressive implementation may reduce risk by somewhere between 5% and 20% per year. It further assumed that it may take between five and six years for SMS to achieve its full effect in a carrier, and that it may therefore reduce risk overall by 25% to 75%. This wide range of effects was categorised as varying from minor to profound.

5.18.1 Economic Benefits Of Aircraft Accident Reduction

The Australian Bureau of Transport Economics estimated the cost of aviation accidents in that country to be AU$112 million (US$82 million) in 1996, and regarded this as the lower figure of an unknown range. There were 39 accidents in the country that year, and the Bureau broke the cost figures down further to estimate a cost per accident for high capacity category aircraft of AU$2.25 million, which in US dollars terms equates to $1.7 million.

The Bureau then looked at the 25% lower end potential for accident reduction and estimated a possible saving of AU$16 million per year (US$11.8 million).

5.18.2 Implementation Costs For SMS

Finally, the Bureau produced a breakdown of the estimated cost of implementing an SMS in an airline as summarised below.

Item	Notes	Major carrier cost AU$M (US$M)
Cost of employing a safety manager	Salary (includes 65% on costs for insurance, lighting, rental, furniture, etc.	150 (110)

Item	Notes	Major carrier cost AU$M (US$M)
Training costs	Approx $1,000 per day for 7-30 days	20 (15)
Facilities	Office, training aids, PCs etc	20 (15)
Management costs	Management time setting objectives and procedures	100 (75)
Ongoing costs	Stationery etc, staff costs	60 (45)
Upgrading or revising manuals	Will very greatly between operators	100
Cost of employing controllers	Salary of airworthiness officer	Already employed
TOTAL		**450 (329)**

Table 12 – Estimated SMS Implementation Costs

5.19 APPLYING BENEFIT FIGURES TO SSCM

Taking the Australian experience as being representative of a mature air transport system and applying the generally accepted belief that approximately 10% of global total-loss aircraft accidents have technical faults as a principal causal factor, it can be shown that at the lower, pessimistic end of the benefit scale (25%), there is already a potential saving of US$1.8 million in prevented accidents in that country in one year by SMS implementation. What now needs to be considered is the additional saving that SSCM can make.

Some help in this direction comes from the increasing use of FDM and FOQA programmes. One major operator already using a FOQA programme has gone on record as saying that they have calculated the programme has prevented one catastrophic engine failure and seven unnecessary engine changes every year, and one hull loss accident every 12 years.

In 2002, American Airlines took part in a proof-of-concept trial of an experimental safety data mining tool in order to assess its usefulness. As a result of this, the airline drew the following conclusions:

- Data mining can provide unexpected correlations of data from different sources that call for further investigation
- This type of tool is much quicker than other systems in identifying specific areas of interest. The airline considered this point alone to provide an increase in efficiency and productivity that was critical to their safety analysis work.

American went on to comment that such a system could show various apparently sporadic deviations from expected performance, highlighting areas requiring review. Trends identified validated the accuracy and usefulness of the tool, drawing the comment that the tool "produced indications and graphic products in seconds that had (previously) taken days of work."

In 2002, GAIN surveyed airline flight safety departments to identify the analytical methods they had in place in support of safety management. The results indicated that while most have some sort of data collection and analysis system, thus recognising the need, the tools used were a direct reflection of the type and amount of data gathered. Beyond the basic analysis of air safety reports, flight data and human factors reports, there were almost no other capabilities in place.

GAIN commented that the reporting and investigation of safety related events was "fundamental to the safety management process" and that the analysis of past events is vital to undertake proactive safety management activities. The airlines are increasingly recognising that effective safety management rests on the collection and analysis of relevant data obtained during the day-to-day conduct of flight operations. Required analytical improvements identified (both contained within SSCM) were:

- Better integration between existing tools to interface with airline data

- Customised tools to perform standard analytical procedures that commonly arise in airline flight safety management

The survey concluded that there was considerable need for better integration of safety information, "even among those airlines that already have fairly well-developed flight safety management programmes.

GAIN is repeating the survey, in expanded format, to a larger selection of operators (see Appendix B). The results will also be used to assist in the future development of SSCM trials models.

5.20 ILLUSTRATION OF POTENTIAL SAVINGS

A number of individual aircraft accidents, and series of accidents, that had technical failure issues as primary causal factors were analysed to demonstrate the potential for financial savings to the industry through SSCM implementation.

5.20.1 Hellas Jet Boeing 737 Accident

On 8 August 2005, a Boeing 737-300 operated by the Cypriot airline Hellas Jet, crashed on the Greek mainland with the loss of all those on board. It had apparently suffered total cabin pressurisation failure in the cruise, followed by incapacitation of the flight crew. The aircraft subsequently ran out of fuel. Initial investigations revealed that the cabin air conditioning system had required rectification five times in the preceding two months, and that questions had been raised by the airline's own engineers about the aircraft's fitness to fly. This inevitably leads to questions about how they may have voiced their concerns. Given the repetitiveness of related issues with this aircraft, it can be argued that had the company had SSCM in place, there would have been a much higher chance of the problem being brought to their attention than appears to have been the case. Furthermore, it is also contended that such frequent anomalies with the cabin conditioning system would have been likely to trigger an FHA non-compliance alert requiring corrective action to be taken, and thus potentially preventing the accident. Quite apart from all the human costs, the current market value of a Boeing 737 of this variant is around $7 million.

5.20.2 King Air Undercarriage Failures

Over a four-month period in the first half of 2004, there were no fewer than five non-fatal accidents to public transport category Beech King Air aircraft, involving either failure of the undercarriage to extend or its partial collapse on landing. The events demonstrate remarkable similarities and in at least one case, a component failure was identified as the primary cause. Had an SSCM system been in place, it is arguable that King Air operators could have been alerted to the prevalence of undercarriage issues and a technical investigation instigated. If, as a result, just one of these incidents could have been avoided, the potential saving to the operator through not suffering an undercarriage collapse and subsequent repair, is estimated to be in the region of $43,000. This is based on average overhaul figures for undercarriage and propellers and takes no account of any additional secondary damage [78].

5.20.3 Cessna Caravan Engine Failures

The single-engine Cessna Caravan utility aircraft suffered a total of six engine failures during 2004. It's Pratt and Whitney Canada PT-6A engine had previously built up a high reputation for reliability in several other applications. Examination of the 2004 incidents showed potentially significant issues with the aircraft operating environment, with five of the six occurring outside the United States and in parts of the world where extremes of climate and harsh operating conditions prevail. Discussion with one of the operators concerned revealed that they had lost confidence in the aircraft to such an extent that they had completely withdrawn the type from their operations. It was added that the aircraft manufacturer had been less than helpful in attempting to resolve the engine-related problems and were not sharing the experiences among operators. Here again, an SSCM system with feedback direct from the operators to the engine manufacturer may well have alerted them earlier to the problems being experienced and enabled a more rapid investigation and potential avoidance of one or more of the later events.

5.20.4 Dornier Do.328 Inadvertent Door Opening

In March 2002 a Dornier 328 aircraft was forced to abort its take-off when a "Doors" warning caption was illuminated on he flight deck. The probable cause was the cabin attendant grasping the inner door handle to restrain herself during the rapid acceleration, since it was discovered that the ergonomics of the cabin crew seat and door handle made such an involuntary action readily conceivable. The door became unlatched and opened rapidly, with the subsequent overtravel causing substantial damage to the door attachment arms. The remaining attachment strength of the door and airstairs was such that both would almost certainly have separated had the aircraft become airborne, with a potentially catastrophic outcome.

The investigation report commented that while the door design was technically compliant with the certification requirements, it lacked the necessary integrity to prevent a hazardous occurrence to the aircraft such as inadvertent opening. As a result, it was recommended that the door design should be reviewed. This event, while isolated as far as can be ascertained, illustrates the role of cabin crew in the SSCM system. It is postulated that the potential need to grab the door handle during acceleration must have been well known, and that more than one alert crew member would have recognised the potential problem and, given access to a suitable reporting system, brought it to the attention of the company.

5.21 SUMMARY OF COST SAVINGS

The cost of commercial aircraft hull losses averaged over all flight sectors, is estimated to be approximately US$75 per flight cycle [79]. This figure represents a very significant cost burden on the entire air transport industry, and it must be remembered that it takes no account of the cost of lesser events.

The case studies presented throughout this thesis have demonstrated the clear potential for SSCM to make produce significant financial benefits to operators, over and above those to be gained from the current drive towards global SMS implementation. In Chapter 1 it was shown that study of fatal accidents over a

20-year period contended that 3,303 lives were lost in accidents for which a design fault was the primary causal factor, while a further 2,465 people died in those where maintenance was the key factor. Based on the Australian experience discussed in this chapter, and making a conservative estimate that SSCM could reduce these losses by just 5%, with each death currently costing the industry US$3.2 million, there are annual savings of US$923 million to be made. Furthermore, there will be substantial additional financial benefits for the manufacturing industry through more accurate component reliability data, earlier warning of emerging problems and direct technical interface with the operators.

In the 1970s, a noticeable step-change improvement in the commercial aircraft accident and incident rate was seen. There were a number of reasons for this, including technological advances leading to improved reliability and aircraft and their systems. However, another significant factor was the introduction of the MSG system for maintenance task analysis, based on optimising scheduled maintenance by basing it on reliability and failure consequences, rather than the previous system of maintenance almost for its own sake. It is contended that the global introduction of SSCM is likely to result in a similarly significant reduction in accident and incident rates.

Due to the complexities of implementing such a system retrospectively, it is suggested that the first stage would be to introduce SSCM into a new aircraft project, such as the Airbus A350 or Boeing 787. In relative terms, implementation costs would be modest, and once proven, confidence would be gained in rolling out the model to earlier fleets.

CHAPTER SIX – SUMMARY AND CONCLUSIONS

6.0 INTRODUCTION

This chapter summarises the issues raised throughout the thesis, the range of proposals to improve the current system safety process and the advantages of the SSCM process. It also details planned future progress towards implementation.

6.1 WHERE SHOULD THE INDUSTRY GO?

Today's air transport industry is undoubtedly a very safe one. Major accidents as a percentage of total scheduled airliner departures are thankfully very small indeed, and this is the result of a great deal of hard work by all sections of the industry. Despite the recent global airline recession, which had a major impact in almost every sector (with the exception of the burgeoning low-cost carrier network), it is now clear that recovery is well underway, and gaining strength.

In recent months, Airbus, Boeing and Embraer all issued their own forecasts of how they saw the market developing over the next twenty years. Not surprisingly they all differ in some respects with regard to which particular categories of aircraft will do well in terms of future sales and which will not. Nevertheless, the overall message is clear and common to all three manufacturers; they all predict that the size of the world jet transport fleet will approximately double to somewhere around 35,000 aircraft.

As illustrated in chapter one, unless the current accident rate is significantly reduced, this doubling of the fleet size and the commensurate major increase in the number of scheduled aircraft departures, will inevitably lead to a much higher number of total hull loss accidents each year. If that is the case, then the possible deaths of several hundred people in air crashes each week, would have a disastrous effect on the airlines. Such an accident rate would possibly result in a major collapse in public confidence and the resultant drop in passenger numbers as people declined to fly, would hit the airlines finances very hard indeed. Many operators, especially those in the short-haul and

medium-haul sectors where alternative methods of transport are easier would not survive.

Even the low-cost carriers, who are today's success story, would not escape. Purely by virtue of the high percentage of total scheduled departures for which they now account, it is statistically inevitable that they will start to have accidents. This is already their greatest worry, as the underlying suspicion in many peoples' minds that low cost equals low safety, would instantly surface. Indeed at least one major European budget airline is already known to be investing very heavily in safety management processes and projecting themselves as always putting safety first, in a deliberate effort to distance themselves in the public's perception from their rivals, since one of them in particular is considered to be at significant risk of having the first budget airline catastrophic accident in Europe.

So, the underlying accident rate must come down still further from the historic low levels enjoyed for some years now, or the airline industry will not survive in anything like its current form. Much effort is being put into understanding and addressing the major human factors related causes of fatal accidents, including CFIT, approach and landing, loss of control and runway incursions. Relying again on statistics this is of course understandable, since such accident categories account for somewhere between 70% and 80% of all hull loss accidents. The problem is that we now take our eye off the ball with regard to the remaining 20%, which includes other human factors causes, weather related accidents and technical failures. Should we be ignoring the last category? This document has presented ample evidence that we should not.

So, what can be done to ensure a reduction in technical failures plays its part in the overall effort to bring the total accident rate down as the airline industry grows? Although the proposed SSCM is by no means the total answer to the problem of aircraft system safety, it clearly addresses most of the basic issues. Nevertheless, it has been shown that other changes need to be made across the industry, and made fast. As the upswing in airline fortunes gathers strength, there may be surprisingly little time to address these issues before the accident numbers start to increase. Indeed 2005, with its unfortunate increase in hull

losses, may have provided the first piece of hard evidence to support this; time is not on our side.

The introduction of an SSCM system is just one part of a package of six measures that need to be taken if significant advances in aircraft system safety performance are to be achieved. They are all of equal importance and the remaining five are summarised below.

6.2 A MANDATORY SAFETY ANALYSIS PROCESS

It has been shown that while a fundamentally sound process (ARP4761) already exists for much of the system safety analysis work, the one big problem with it is that the regulatory authorities still do not mandate its use. This despite the many years it has been around, and the clear benefits it has brought for those sections of the industry who have been conscientious enough to use it properly, especially with regard to accepting the need for independence in design safety assessment. A joint FAR / JAR / EASA safety analysis process regulation, incorporating ARP4761, issued and mandated by both the FAA and EASA is one possible answer.

In the meantime, aircraft and system manufacturers should be required to enter their system design analyses, (with suitable proprietary data and access safeguards to protect commercial confidentiality), directly into the SSCM system for instant assessment of FHA compliance, and compatibility with the parts catalogue data. Any parts reliability assessments used in safety assessments which are not based on the SSCM database will require the manufacturer to input an acceptable justification statement before system certification can be achieved.

6.3 RELIABILITY DATABASES

The continued use of MIL-HDBK-217F, NPRD 95, Bellcore and all the other non-aerospace specific component reliability databases must cease at the earliest possible opportunity, although of course first there must be something to replace them. The SSCM component reliability database will gradually build

into the standard repository of such information, since it will be aerospace specific, take full account of environmental and operational variances, and contain a much higher percentage of events for calculation purposes than has been the case previously.

Until such time as SSCM comes fully on line and can be implemented globally, the manufacturing industry will still have to rely on existing databases and / or their own empirical data, this is unavoidable. However, the regulatory authorities should change the existing certification requirements for failure rate justification statements in safety cases, by making them far more stringent. For example, it should no longer be acceptable to justify rates solely by quoting MIL-HDBK-217F as a source. Analysts should be required to make statements including, but not necessarily limited to:

- No other suitable source data is available
- Due regard has been given to the possible effects on the data of environmental and operational variations by means of sensitivity analysis
- Confidence levels in the data are at or above 90%
- Empirical data will be gathered to check data confidence, starting with system testing prior to certification and will continue following service entry

6.4 EVENT ANALYSIS AND LESSONS LEARNED SYSTEMS

Remember the words of the FAA's *Commercial Airplane Certification Process Study* discussed previously;

"Adequate processes do not exist within the FAA or in most segments of the commercial aviation industry to ensure that the lessons learned from specific experiences in aircraft design, manufacturing, maintenance, and flight operations are captured permanently and made readily available to the aviation industry. The failure to capture and disseminate lessons learned has allowed aircraft accidents to occur for causes similar to those of past accidents."

A major problem with existing databases, is that they can only be searched separately, there is no cohesion or attempt to make them interface with each other. There is also widespread concern about just how little is currently being learned from operational feedback, but:

- Who owns the database?
- Who pays for it?
- Who has access to it, both for input and for data analysis?
- How can the industry as a whole be persuaded to use it?

Although all these points are addressed in full by SSCM, there is still much good non-statistical information already out there, just waiting to be harvested. The commercial sensitivity argument that has prevented manufacturers of similar equipments sharing with each other the lessons they have learned, will always be a barrier. But, the independent ownership of SSCM can be exploited to provide an independent review forum with no regard to such matters.

Any such issues discovered during SSCM data review that should be shared between different manufacturers can result, at the very least, in the two companies being advised to talk to each other!

6.5 TRAINING SAFETY PRACTITIONERS

System safety analysis is a highly complex process and requires a much broader and deeper range of education options to compliment what we already have, including courses offering Certificate, Diploma and Degree level qualifications for safety professionals – of whom there are still pitifully few. What is required is an appreciation of the need to combine basic reliability data, physical elements, statistical and other analytical skills, and engineering judgment, while still producing results that are both understood and traceable.

The last statement on its own, makes clear the need for independence in safety assessment by trained analysts, since neither they nor the equipment designers can be expected to possess all these skills. They must work as a well-educated team.

6.6 EDUCATING THE INDUSTRY

Despite statements to the contrary, it is an inescapable fact that safety remains a trade-off in the aviation industry, especially in the current climate of extreme financial constraint. Market pressures including cost, time to market, competitiveness, the desire to protect the sales after-market of spares and repairs, will always be present. This situation can only get worse as times of economic downturn drive down manufacturers margins as they fight to remain competitive. Awareness of the need to fully appreciate the importance of system safety issues through a cultural change that really does give safety a priority, is the key to changing this view, but it will obviously take time.

There is no easy answer to how this can be achieved. However, new legislative initiatives such as EASA, are already forcing the industry into taking the understanding and management of risk much more seriously. The introduction of Safety Management Systems (SMS), is starting to gather pace in the operators, especially so since publication by the CAA of Civil Air Publication (CAP712), which is the best guidance document around for SMS in aviation. As a result, airlines, maintenance organisations and the armed forces are starting to seek education in SMS principles, but as yet the word has not got through to the manufacturers, certainly at system level. Perhaps the answer here is for the aircraft manufacturers to embed safety management and safety assessment requirements more clearly in the system and equipment contractual specifications they send out to their suppliers.

6.7 RECOMMENDATIONS FOR FUTURE WORK

The main stages in the development and introduction of SSCM are defined in the implementation roadmap shown in section 5.9. The next steps to take the proposal forward are:

- Detailed discussions with potential partners and database hosts.
- Software selection and error-proneness testing, leading to preliminary database design including interlink functionality with existing database

systems. This work to be carried out in consultation with experienced reliability database consultants.

- Detailed cost estimates at least up to and including the proposed field trial.
- Identification of trial participants through a series of field presentations to potentially interested groups.
- Continuing adaptation and refinement of the SSCM data elements to incorporate feedback from presentations and draft discussion papers. One of the principal aims must be to ensure all aspects of the industry are covered, such as the helicopter environment issue identified in the survey as being a shortcoming with existing data systems.

During the development of this proposal, preliminary discussions have been held with both Operational Monitoring and Human Factors, and senior Flight Safety specialists at Airbus, with excellent feedback resulting. These discussions will continue and expand as the SSCM proposal matures.

A draft paper based on this document has been sent for comment to the Human Factors Specialist in Maintenance Engineering Technical Services at the Boeing Company in Seattle. It is also intended that as SSCM development continues and matures, further work can be undertaken to introduce mathematical modeling as data subjectivity decreases.

6.8 END PIECE

It is now time for the whole aviation industry, including aircraft, system and component manufacturers, operators, maintenance organisations, steering bodies and not least the legislators, to take the system safety issue on-board and act. It can no longer be acceptable to assume that an aircraft system is safe because an accident that includes a failure of that system as a contributing factor has not yet happened. Similarly, the potential for undesirable interaction between different systems on the same aircraft must be better understood through better defined processes such as enhanced zonal analysis, assessment of external events and so on.

For some time now, the relatively stable failure rate of aircraft systems has been the excuse for the industry to concentrate its efforts solely on human factors causes, but recent accidents such as the Alaskan MD-80, the Lauda Air 767 and the Hellas Jet 737, must be seen as a clear warning to pay more attention to technical problems.

As has already been stated in the introduction, the two primary issues that need to be addressed are:

- The reliance by industry on obsolete, irrelevant or incomplete reliability date when building their safety cases for certification
- The unsatisfactory level of feedback from actual in-service equipment performance in order to validate the safety level assumptions made at the design stage

The use of out-of-date databases, which are still viewed as "industry standards", must cease. Too many design safety cases continue to be built on reliability assumptions using failure rate data from such sources. Although other commercial databases have since come along in an attempt to fill the gap left by the withdrawal of support for the earlier models, they tend not to be aerospace specific and in any event, are no true substitute for true empirical data from like equipments in service.

The industry as a whole has to recognise the desirability, not just from the safety standpoint, but also commercially, of adopting effective data capture, analysis and sharing systems. This is especially true once equipment goes out of manufacturers warranty. Up to that point, OEMs tend to see the vast majority of in-service events, for the obvious reason that operators know the OEMs will pay for the investigation and repair. It is later, when alternative repair arrangements may be made, that the data stream slows or even dries up altogether.

Currently, unless some drastic event occurs, safety cases tend to be left on the shelf once certification is granted. The operators and manufacturers have little visibility of actual safety levels and therefore, no opportunity to identify possible

safety non-compliances before they can potentially lead to an accident. Far better then, to have a system that will automatically highlight such non-compliances and force action to be taken.

SSCM takes the whole analytical process a long way forward from where it is today, in a manner that will bring genuine benefits to the industry in terms of improved safety and financial performance. This is true not just of the initial design analysis, but also of the in-service phase, which so far has been poorly addressed and is frankly, not well understood. It is time for the industry as a whole, including the regulatory agencies, to take advantage of the opportunity to tackle the technical safety issues in a more robust fashion.

REFERENCES & PUBLICATIONS

REFERENCES

Chapter 1

Page 18 [1] Uve Ltd, for City University Safety Analysis & Statistics MSc module 2003

Page 19 [2] *Aviation Safety Improvement using Cost Benefit Analysis* NLR-WP 1-D11 VO.1 ASICBA, National Aerospace Laboratory, April 2005

Page 20 [3] *Airplane Accident Summary,* Boeing Commercial Airplanes June 2002

Page 21 [4] *The Year In Review*, James Burin. Proceedings of the 57th International Air Safety Seminar, Moscow November 2004

Page 23 [5] R G W Cherry & Associates, Failure Theory, 2002

Page 23 [6] *Aviation Safety – An Analysis For Airline Manager*", Steve Monaghan. MSc Air Safety Management thesis, City University 2006

Page 25 [7] *Aircraft Maintenance Engineering: Developing an Aircraft Maintenance Programme using Reliability Centred Maintenance / MSG3 Analysis and taking into consideration ETOPs and Low Utilisation*, Mark Peirotti. PhD Air Transport Engineering thesis, City University 2005

Chapter 2

Page 31 [8] H Paul Barringer, Barringer & Associates, 2003

Page 32 [9] *System Reliability Analyses An Overview of Basic Concepts and Directory of Other Resources.* Weibull.com, ReliaSoft Corporation 2006

Page 32 [10] *NATO Requirements For Reliability And Maintainability.* ARMP-1 Edition 3, 2002

Page 32 [11] *Reliability Programme for Systems and Equipment, Development and Production.* US Military Standard 785B, 1988

Page 32 [12] *The New Reliability Paradigm.* Ian Knowles, Ministry of Defence 1996

Page 32 [13] *Reliability, Maintainability and Supportability: A Probabilistic Approach.* Dr Jezdimir Knezevic, University of Exeter 1993

Page 32 [14] *The New Reliability Paradigm.* Ian Knowles, Ministry of Defence. Paper presented at a Reliability Engineering course, Exeter University, 1996

Page 32 [15] *The Evolution of Reliability.* Paul Barringer, International Maintenance Conference, Florida 2003

Page 33 [16] *The Evolution of Reliability.* Paul Barringer, International Maintenance Conference, Florida 2003

Page 33 [17] *Patterns in Safety Thinking; A Literature Guide To Air Transportation Safety.* Geoffrey McIntyre, Ashgate Publishing 2000. Page 64

Page 33 [18] *The Efficiency Of Gaseous Diffusion Cascades.* Harold Urey, 1934

Page 33 [19] *Reminiscences of the Evolution of Reliability in Manufacturing.* Charles Latino, Reliability Center Inc., 2002

Page 34 [20] *Reminiscences of the Evolution of Reliability in Manufacturing.* Charles Latino, Reliability Center Inc., 2002

Page 34 [21] Conversation between the author and former UK Civil Aviation Authority regulator Ray Christie, March 2001

Page 34 [22] Conversation between the author and former UK Civil Aviation Authority regulator Ray Christie, March 2001, based in flight operations and trials data analysis conducted at the Royal Aircraft Establishment Bedford

Page 36 [23] Captain Brian S Richardson ALPA, Aeronautical Engineer & Former NTSB Investigator speaking in 2003

Page 41 [24] Letter to the author from John C Dalton, Technical Fellow, Airplane Safety, Boeing Commercial Airplanes, 2001

Page 42 [25] *Response to UK Department for the Environment, Transport and the Regions (DETR) Consultative Document on the Future of Aviation.* Royal Aeronautical Society 2004

Page 45 [26] Conversation between the author and former UK Civil Aviation Authority regulator Ray Christie, March 2001

Chapter 3

Page 51 [27] Boeing Commercial Airplanes annual twenty-year global market forecast, 2005

Page 53 [28] Accidents and Incidents Database. Federal Aviation Administration 2004

Page 54 [29] Kathy H Abbott PhD, Chief Scientific and Technical Advisor for Flight Deck Human Factors Federal Aviation Administration, speaking at the 56th International Air Safety Seminar, Shanghai, 2005

Page 55 [30] *System Safety Handbook for the Acquisition Manager.* United States S Air Force SDP 127-1, 1987

Page 57 [31] *The Evolution of Reliability.* H Paul Barringer, International Maintenance Conference, Florida, 2003. Page 7

Page 58 [32] *Aviation Safety Improvement using Cost Benefit Analysis* NLR-WP 1-D11 VO.1 ASICBA, National Aerospace Laboratory, April 2005. Page 49

Page 69 [33] *MIL-Hdbk-217 Use and Application Reliability Review.* Seymour Morris, Rome Laboratories, 1990. Volume 10 page 10

Page 69 [34] *The New Reliability Paradigm.* Ian Knowles, Ministry of Defence. Paper presented at a Reliability Engineering course, Exeter University, 1996

Page 71 [35] *System Safety Process.* Federal Aviation Administration 2001

Page 74 [36] *Logistics Support Analysis – Principles and Practice* Roger Siswick and Malcolm Shaw, BAE Systems Warton, 1991. Paragraph 1.3.7

Page 74 [37] *Logistics Support Analysis – Principles and Practice* Roger Siswick and Malcom Shaw, BAE Systems Warton, 1991. Paragraph 1.4.3

Page 76 [38] *Analytical Methods For The Logistics Professional* short course notes, Systems Exchange Seminars, Orlando 2000. Page 115

Page 76 [39] Ian Knowles, Principal R&M Engineer, Ministry of Defence Procurement Executive, presentation at University of Exeter 1993

Page 77 [40] *Reliability Engineering Course Notes* Dr Jezdimir Knezevic, University of Exeter 1993

Page 85 [41] *Commercial Airplane Certification Process Study.* Federal Aviation Administration, March 2002

Page 90 [42] Airbus Industrie statements on the future of long-range operations 2003

Page 93 [43] *Lauda Air B767 Accident Report.* Aircraft Accident Investigation Committee, Ministry of Transport and Communications, Thailand 1993

Page 95 [44] *Accident Report DCA94MA076.* National Transportation Safety Board 1999

Page 95 [45] *Safety Recommendation A-99-20 to A99-29.* National Transportation Safety Board 1999

Page 97 [46] *Climbing the Learning Curve.* Flight International 5-11 June 2001 pp 42 to 48

Page 99 [47] *Accident Report DCA97MA055.* National Transportation Safety Board, July 2000

Page 99 [48] *Normal Accidents: Living With High-Risk Technologies.* Charles Perrow 1984

Page 100 [49] *Accident Report AAR-02/01.* National Transportation Safety Board, December 2002

Page 106 [50] Global Aviation Information Network (GAIN) website

Page 110 [51] *Commercial Aviation Safety.* Alexander Wells, McGraw Hill, fourth edition, 2003. Page 92

Page 113 [52] *Proposal for a Regulation of the European Parliament and of the Council on establishing common rules in the field of civil aviation and creating a European Aviation Safety Agency.* European Commission Legislation Under Preparation 500PC0595 2002

Chapter 4

Page 115 [53] *BA Flight Data Analysis Programme 1969-1999.* Lecture by Captain M Holton, British Airways 2005

Page 115 [54] *Lessons Learned and Corrective Actions Systems for the Aviation Safety Community – Concept of Operations* GAIN September 2004

Page 116 [55] *Safety Analysis & Statistics* City University MSc module coursework, Squadron Leader Jeremy Attridge, Royal Air Force, August 2005

Page 130 [56] ICAO document No.9713 on Continuing Airworthiness, 1998

Page 136 [57] *Sentinel* Website, Mercator Company, Dubai, 2005

Page 137 [58] *Normal Accidents: Living With High-Risk Technologies.* Charles Perrow 1984

Page 138 [59] *Human Factors: The Big Picture.* Hazel Courteney, Head of Human Factors Group, UK Civil Aviation Authority, May 2001

Page 139 [60] *Preliminary – Notice of Proposed Amendment 25.310 Human Centred Design.* UK Civil Aviation Authority 2003

Page 142 [61] Draft European Commission regulation consultation document for a Commission Regulation laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations, JAA June 2003

Page 143 [62] *Proposal For A Directive Of The European Parliament And Of The Council On Occurrence Reporting In Civil Aviation.* European Commission document reference 2001/C 332 E/19, September 2001

Page 148 [63] *Continuing Airworthiness – The Basic Story.* John Saull and Bob Davies, International Federation of Airworthiness, May 2003

Page 152 [64] *GAIN Action Plan.* Global Aviation Information Network, September 2002

Page 156 [65] *Development of a Methodology for Operational Incident Reporting and Analysis Systems.* Direction Générale de l'Aviation Civile, 1996

Page 160 [66] *Safety Analysis & Statistics* City University MSc module coursework, Squadron Leader Jeremy Attridge, Royal Air Force, August 2005

Page 160 [67] UK CAA Paper 2002/02. Final report on HOMP Trial, 25 September 2002

Page 160 [68] *Patterns In Safety Thinking.* Geoffrey McIntyre, 2000. Page 90

Chapter 5

Page 167 [69] John Dalton, Boeing Commercial Airplanes, speaking at National Institute of Aerospace Safety Seminar, Langley Virginia, March 2006

Page 169 [70] Flight International 11-17 May 2004

Page 169 [71] Rolls-Royce website

Page 169 [72] Paper submitted for the 8th annual MRO Regulations, Quality & Safety Conference, Haro Ranter, October 17-18, 2001

Page 186 [73] Flight International 20-26 April 2004. Page 39

Page 189 [74] GAIN seminar on Lessons Learned and Corrective Actions, Denver, January 2005

Page 212 [75] *Handbook for Conducting Cost Benefit Analysis of Safety Measures in Air Transport.* A L C Roelen, R Piers, R J Molemaker and P Hayes, NLR 2001

Page 237 [76] Stuart Matthews, President of the Flight Safety Foundation, speaking in April 2004 about airlines cutting safety budgets

Page 238 [77] *Notice Of Proposed Rule Making Air Operator Certification – Air Transport – CASR Part 119.* Civil Aviation Safety Authority Australia Document NPRM 0201OS

Page 242 [78] *Operating Costs and Cost Comparison.* Corporate Airsearch International Inc., website 2006

Page 243 [79] Commercial Aviation Safety Team (CAST) presentation to NTSB Air Cargo Safety Forum 30 Mar 2004, page 13

PUBLICATIONS

Bachelder, Edward & Leveson Nancy, *Describing And Probing Complex System Behaviour: A Graphical Approach,* Massachusetts Institute of Technology 2001

Bond, Steve, *Improving System Reliability, Maintainability, Testability & Supportability Through a Totally Integrated ILS Programme Approach*, Journal Of The Institute Of Mechanical Engineers 1999

CAP712 Safety Management Systems For Commercial Air Transport Operations, UK Civil Aviation Authority 2001

Corker, Kevin & Gore, Brian, *Context, Coupling & Coping: Representing Human Performance In Safety Critical Systems,* San Jose State University 2000

Dekker, Sidney, *The Field Guide To Human Error Investigations,* Ashgate Publishing 2002

Fickeisen, Frank, *Improving The Effectiveness Of Aircraft Certification Analysis Processes,* International Federation of Airworthiness 2001

Knezevic, Jezdimir, *Reliability, Maintainability And Supportability – A Probabilistic Approach,* McGraw Hill 1993

McIntyre, Geoffrey, *Patterns In Safety Thinking*, Ashgate Publishing 2001

Reason, James, *Managing The Risks Of Organisational Accidents,* Ashgate Publishing 2000

Slotte, Stephen, *Part 25 Aircraft Life Certification Policy,* Federal Aviation Administration 1996

Wells, Alexander, *Commercial Aviation Safety,* McGraw Hill 2001

W.H. van, and G.W.F.M. van der Nat, *The use and needs for air safety data in the Netherlands : an exploratory study*, Amsterdam National Aerospace Laboratory NLR, 1998.

APPENDIX A – FAR / JAR 25 SYSTEM REQUIREMENTS

AIRCRAFT ELECTRICAL POWER SYSTEM

"The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.

(b) The aircraft systems and associated components, considered separately and in relation to other systems, must be designed so that–

(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the aircraft is extremely improbable, and

[(2) The occurrence of any other failure condition which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions is improbable.

(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimise crew errors, which could create additional hazards.

(d) Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider--

(1) Possible modes of failure, including malfunctions and damage from external sources.

(2) The probability of multiple failures and undetected failures.

(3) The resulting effects on the aircraft and occupants, considering the stage of flight and operating conditions, and

(4) The crew warning cues, corrective action required, and the capability of detecting faults.

(e) Each installation whose functioning is required by this subchapter, and that requires a power supply, is an "essential load" on the power supply. The power sources and the system must be able to supply the following power loads in probable operating combinations and for probable durations:

(1) Loads connected to the system with the system functioning normally.

(2) Essential loads, after failure of any one prime mover, power converter, or energy storage device.

[(3) Essential loads after failure of--

(i) Any one engine on two-engine aircraft; and

(ii) Any two engines on three-or-more engine aircraft.

(4) Essential loads for which an alternate source of power is required by this chapter, after any failure or malfunction in any one power supply system, distribution system, or other utilization system.

[(f) In determining compliance with paragraphs (e)(2) and (3) of this section, the power loads may be assumed to be reduced under a monitoring procedure consistent with safety in the kinds of operation authorized. Loads not required in controlled flight need not be considered for the two-engine-inoperative condition on aircrafts with three or more engines.

(g) In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft."

APPENDIX B- ACCIDENT MATRIX

Event type	Date	Aircraft	Registration	Circumstances	Findings	Category
Mechanical failure - airframe	25/05/2002	Boeing 747-209B	B-18255	While climbing through 1,600 feet the crew received clearance to climb to and maintain FL260. The Flight was then cleared to climb and maintain FL350. 13 minutes later, while approaching 35,000 feet, the aircraft disappeared off radar screens. Wreckage and bodies were found at sea. The flight probably disintegrated at high altitude since other debris was found about 45 kilometers from the crash site.	Break-up due to structural failure in aft lower lobe section of fuselage. In February 1980, the aircraft suffered a tail strike, was ferried back to Taiwan un-pressurized and temporary repair was conducted the day after. Permanent repair was conducted in May 1980, but was not accomplished in accordance with the Boeing SRM, in that the area of damaged skin in Section 46 was not removed (trimmed) and the repair doubler did not extend sufficiently beyond the entire damaged area to restore the structural strength. Evidence of fatigue damage was found. Maintenance inspection did not detect ineffective repair & fatigue cracks that were developing under the repair doubler. Safety recommendations addressed possible improper repairs to pressure vessel which may be hiding damage, allowing the development of multiple-site fatigue damage and fatigue fracturing that could lead to structural failure	Maintenance error; ineffective repair and poor oversight
	17/06/2002	Lockheed C-130A	N130HP	After dumping fire retardant, both wings separated in an upward motion. The right wing immediately separated from the fuselage at low altitude. The plane then lost control and rolled left. During this manoeuvre the left wing fell from the aircraft as well and the aircraft nose-dived into the ground. In April 1998 two one-inch cracks were found on the bottom of a wing (the service difficulty report does not state which wing), at Outer Wing Station 33, which is 33 inch (83cm) from the wing joint. These cracks were repaired.	In-flight failure of right wing due to fatigue cracking in centre wing lower skin and underlying structural members. Contributory factor inadequate maintenance procedures to detect fatigue cracking. NTSB determined that maintenance and inspection programmes applicable to firefighting aircraft did not adequately account for increased safety risks as a result of advanced aircraft age and severe stresses of firefighting. Recommended that Department of Agriculture and Department of Interior develop maintenance and inspection programmes for firefighting aircraft that include consideration of original design, age, and operational stresses, as well as engineering evaluations to predict and prevent fatigue cracking.	Maintenance error; inadequate procedures

	18/07/2002	Consolidated PB4Y-2	N7620C	Turned for firefighting drop in a smooth 15 to 20 degree bank turn. Left wing separated inboard of number 2 engine. Pitched nose down and plunged into ground vertically. Widespread fatigue was not evident over the entire wing but in some locations current crack detection techniques may have been unreliable	The in-flight failure of the left wing due to fatigue cracking in the left wing's forward spar and wing skin. A factor contributing to the accident was inadequate maintenance procedures to detect fatigue cracking	Maintenance error; inadequate procedures
	07/05/2004	Douglas DC-4	N44911	As crew started No.1 engine, there was an explosion in the wing area between Nos.1 and 2, and the outboard section of the wing broke away		
	06/03/2005	Airbus A310-308	C-GPAT	At cruising altitude of 35,000 feet, the rudder separated from the vertical stabiliser. Safe landing	On March 18 The French DGAC issued Emergency Airworthiness Directive DGAC AD UF-2005-048. The AD asked for an inspection of the of composite-fibre-reinforced plastic rudders on certain A.310 and A.300-600 aircraft. The FAA consequently issued AD 2005-07-07 on March 28. Airbus consider failure due to water ingress undetected through poor maintenance procedures.	Maintenance error; procedures not followed
	08/05/2005	Boeing 747-400	JA8072	Decompression inbound to Japan. Diverted		
	13/05/2005	McDonnell MD-88		Cabin depressurisation in the climb		
	01/08/2005	Canadair CL415	F-	Rear section separated from aircraft after dumping fire retardant load	No evidence of fatigue, corrosion or mechanical failure. No AD, SB or procedural change recommended. Pilot error suspected	
	14/08/2005	Boeing 737-300	5B-DBY	Apparent pressurisation failure in the cruise, followed by incapacitation of flight crew. Aircraft ran out of fuel and crashed	Air conditioning system had required rectification 5 times in previous 2 months. Questions raised by company engineers about the aircraft's fitness to fly	Possible maintenance error
Mechanical failure - undercarriage	01/01/2004	Douglas MD-81	JA8297	Left main gear collapsed towards the end of the landing roll		
	03/01/2004	Airbus A320	CS-TQE	Nose gear collapsed shortly after tug disconnect following pushback		
	15/01/2004	Boeing 747SP	EP-IAC	Hydraulic problem after take-off, landed with nose gear retracted	Retract actuator ram on right main undercarriage had fractured, resulting in a hydraulic leak and a total loss of pressure on one hydraulic system	Component failure
	20/01/2004	Beech King Air	C-FDOS	After take-off undercarriage "in transit" light stayed on, recycling had no effect. Undercarriage selected down but nose red light stayed on and collapsed on landing		

	31/01/2004	Fairchild Metro II	EC-HCU	Nose undercarriage collapsed during take-off roll	Aircraft had recently undergone some maintenance and was positioning for further work	Possible maintenance error
	04/02/2004	Ilyushin Il.18	EX-005	Nose undercarriage would not extend. Aircraft successfully landed on main gear assemblies		
	20/02/2004	Douglas MD-81	LV-WPY	Shortly after take-off, outer wheel on left main gear fell away. During landing, remaining tyre on that side failed		Possible maintenance error
	01/03/2004	Airbus A300B4	AP-BBA	Unusual vibration during take-off, followed by loud bang and aircraft settled to the left. Take-off aborted	Front two wheels on left main undercarriage had broken up and forward end of left bogie partly worn away	
	04/03/2004	Beech King Air	N30SE	Nose undercarriage indicator light not on, gear appeared to be down. During landing, when nose gear touched down, right main gear collapsed	Rod end of right main gear actuator separated	Component failure
	13/03/2004	Beech King Air	N11FL	Unsafe indication for left main gear when selected down. Collapsed during landing roll		
	01/04/2004	Beech King Air	N740GL	When undercarriage selected down left gear did not extend. Landed with left gear retracted		
	02/04/2004	de Havilland Twin Otter	YV-184CP	Unspecified technical problem en route, leading to diversion. Nose gear failed on landing		
	29/04/2004	Lockheed C-130H	96-1005	Undercarriage problem in flight, requiring manual extension. Right gear collapsed on landing		
	18/05/2004	Beech King Air	N500KA	Following electrical power failure, undercarriage lowered on emergency system. Main gear collapsed on touchdown		
	01/06/2004	Antonov An.32	9XR-SN	Loud bang on take-off and right gear bogie fell away. During landing, gear stub dug in and aircraft left the runway		
	16/07/2004	Commander 690A	YV-733P	Undercarriage would not extend, belly landing carried out		
	25/07/2004	Fokker 100	TC-IEC	Left main gear collapsed on landing		
	19/09/2004	Airbus A320	S7-ASD	Severe vibration during landing roll, ECAM messages "landing gear not downlocked" and "nose wheel steering". Aircraft could not be turned off runway	Tyre on RH gear had failed (possibly due to FOD), with debris damaging undercarriage downlock brace and actuator	FOD
	21/09/2004	Fairchild Metro III	C-FIPW	Left main undercarriage collapsed after touchdown. Aircraft ran		

				off the side of the runway		
	23/10/2004	Boeing 707-320C	PP-BSE	Loud crack heard at start of take-off roll and right wing dropped. Take-off aborted	Right main gear attachment fractured	Component failure
	07/11/2004	Boeing 747-200F	TF-ARR	Loud bang heard approaching V1, and ATC advised smoke coming from beneath the aircraft. Take-off aborted but aircraft overran	One or more tyres failed on RH side. Debris including part of the brake assembly found on the runway	Component failure
	06/04/2005	BN Islander	N29884	Landing gear failure caused aircraft to veer off runway		
	20/04/2005	DHC-8-300		Landing gear problems on approach. Landed with gear retracted		
	20/04/2005	Boeing 707-3J9C	EP-SHE	After touchdown, problems with the undercarriage (failure of a landing gear or tyre burst) caused aircraft to slide off the runway into a river		
	01/05/2005	DHC-8-103	LN-	Suffered right-hand main gear collapse on landing. Turned right of runway 05 and came to a stop 20 meters from jet fuel pumping station		
	09/05/2005	Rockwell Sabreliner 80	N972NR	During takeoff roll just after V1, flight crew and passengers heard a "loud bang" followed by swerving to the left. Aborted takeoff but overran, impacting a fence and trees, before crossing a road and coming to rest upright in a field. Fuel observed leaking from left wing		
	10/06/2005	Hawker-Siddeley HS.748	5Y-SFE	Gear failed on landing, causing aircraft to end up on its belly, blocking the runway		
	12/06/2005	Bombardier CRJ200	N960SW	Nose gear problems reported after take-off. Landed with nose gear up		
	13/06/2005	Beech 1900C	N575G	Left outboard wheel fell off on take-off. Crew unaware until after landing		Possible maintenance error
	28/06/2005	Bombardier CRJ200	N623BR	Nose gear collapsed as passengers were about to disembark		

Mechanical failure - flying controls	31/01/2000	Douglas MD-83	N963AS	At FL310 a problem arose with stabiliser trim. Crew radioed they were having control problems and descending through FL260. Troubleshooting jammed stabiliser. Problem maintaining altitude and diverted towards Los Angeles. During descent crew was also talking to Alaska Airlines maintenance personnel to troubleshoot stabiliser trim problem. Out-of-trim condition became worse, causing aircraft to pitch nose-down. When preparing for landing control was lost and aircraft seen 'tumbling, spinning, nose down, continuous roll, corkscrewing and inverted'. Crashed in 650 feet of water	Loss of pitch control resulting from in-flight failure of horizontal stabiliser trim system jackscrew assembly acme nut threads. Failure caused by excessive wear resulting from insufficient lubrication of jackscrew assembly. Contributing to the accident were extended lubrication interval increasing likelihood that missed or inadequate lubrication would result in excessive wear, and extended end play check interval which allowed excessive wear of acme nut threads to progress to failure with no opportunity for detection. Also contributing was absence on MD-80 of fail-safe mechanism to prevent catastrophic effects of total acme nut thread loss = single point failure	Maintenance error; missed procedures. Non-fail safe design
	16/02/2000	Douglas DC-8-71F	N8079U	Just departed when crew reported balance problems. Crashed left wing low, nose low attitude.	Loss of pitch control resulting from disconnection of right elevator control tab. Disconnection caused by failure to properly secure and inspect attachment bolt	Maintenance error
	20/05/2002	Cessna Citation II	N13VP	During takeoff roll when pulling aft on control yoke, pilot noticed nose landing gear was not coming off of runway at 120 knots with full aft control input. Aborted takeoff, but aircraft left the runway	Elevator trim system 12 degrees out of trim in nose down direction. Pilot failed to note improper setting prior to takeoff	Maintenance error
	28/07/2002	Ilyushin Il.86	RA-86060	Lost control after takeoff, crashed into forest just outside airport and burst into flames.	Stabiliser spontaneously shifted to full down (-12 degrees) position two seconds after takeoff. Six seconds after the shift, captain tried to compensate by thrusting control stick forward as far as possible, but was unable to regain control	

	08/01/2003	Beech 1900D	N233YV	After takeoff the nose pitched up from 7 degrees to 52 degrees by the time it reached 1,200 feet. Aircraft rolled and struck corner of a hangar	Two days prior to accident, maintenance had been performed on elevator tab. Loss of pitch control resulted from incorrect rigging of elevator control system compounded by aft centre of gravity, substantially aft of certified limit. Contributing was: (1) operator's lack of oversight of work; (2) maintenance procedures and documentation; (3) weight and balance programme; (4) quality assurance inspector's failure to detect incorrect rigging; (5) FAA's average weight assumptions in its weight and balance programme guidance; (6) FAA's lack of oversight of maintenance programme and weight and balance programme	Maintenance error
	23/04/2003	Beech 99A	C-FDYF	At 4,000 feet crew selected flaps for approach, bang heard from rear of fuselage. Aircraft commenced uncommanded pitch-up to near-vertical attitude, stalled, nosed over, and began spin to the left. Crew countered the spin but aircraft continued to descend in near-vertical dive. Through application of full-up elevator and manipulation of power settings, pilots able to bring aircraft to near-horizontal attitude. Forced landing carried out	During flight, horizontal stabiliser trim actuator worked free of mounting structure, and flight crew lost pitch control. During replacement of horizontal stabiliser trim actuator, upper attachment bolts were inserted through airframe structure but did not pass through upper mounting lugs of trim actuator. Improperly installed bolts trapped actuator mounting lug assemblies, suspending weight of actuator and giving false impression that bolts had been correctly installed. Dual inspections, ground testing, and flight testing did not reveal faulty attachment	Maintenance error

	24/06/2003	Tupolev Tu.134	RA-65929	In May and June 2003 maintenance work was performed and rudder actuators replaced. Immediately after installation deflection speed for right rudder input decreased from 38.2 degrees per second to 18.3 degrees on day of accident. More pressure necessary for full rudder deflection. Although captain noticed this prior to departure, he decided to continue anyway. During takeoff aircraft began to deviate to left of centreline. This movement could not be countered by applying rudder, so captain decided to use nosewheel steering. One of the nosegear tyres failed. At 250 km/h takeoff was abandoned. Neither spoilers nor emergency brakes were used, aircraft could not be brought to a halt on 2,530m long runway and overran 577 metres. Nosegear collapsed and aircraft sustained substantial damage	Poor quality of work during replacement & adjustment of hydraulic amplifier; unsatisfactory flying & technical operation after completion of replacement of hydraulic amplifier, during which incorrectly installed rudder actuator was not discovered; decision to continue takeoff despite significant efforts needed for deflection of right rudder pedal already noted during pre-flight checks; late rejection of takeoff	Maintenance error
	12/03/2004	Cessna CitationJet 1	D-IMMM	When pilot attempted to rotate the aircraft did not respond. Take-off aborted and aircraft overran		
	16/04/2004	Beech King Air	F-OHJL	Immediately after lift-off the aircraft yawed to the left and ditched	Post maintenance test flight	Possible maintenance error
	12/05/2005	Boeing 717	N910ME	Control system warnings in the climb. Aircraft went into uncommanded pitching descent from 23,000 ft to 13,000 ft, where control was regained. Diverted and landed safely	Lightning strike thought to have played a part	External event
Mechanical failure - instruments	03/02/2004	Beech King Air	LX-KTY	Being ferried for maintenance and made overnight technical stop. During preparation for departure, co-pilot smelt fumes and saw smoke coming from under the instrument panel. Fire gutted cockpit and cabin before it could be put out. Aircraft was connected to GPU with electrical power on		

Mechanical failure - systems	09/11/2000	Swearingen Metro II	N731AC	Struck trees, crashed and caught fire after takeoff in IMC conditions	Indicated failure of right hand AC bus during takeoff with low ceiling. The factors were the low ceiling, night, and the excessive workload the pilot experienced on takeoff with an electrical failure without a second in command	Component failure
	16/04/2002	Hawker-Siddeley HS.748	ZS-OLE	Developed a hydraulic problem, resulting in a complete hydraulic failure. A safe landing was carried out, but veered off and entered a ditch	Leak from L/H engine hydraulic pump, which was not dealt with properly. Contributing to this was an incomplete emergency checklist	Maintenance error
	26/03/2003	Boeing 717-2BD	N957AT	On final approach, the aircraft suffered multiple electrical problems. The pilot lost some electrical systems and computer screens in the cockpit malfunctioned. The plane was about three miles from the airport at the time. The pilot landed the plane safely	Failure of the left power control distribution unit (PCDU)	Component failure
	21/11/2003	HS.125	D2-EXR	An in-flight hydraulic failure forced the crew to return to Luanda for an emergency landing. Intentionally belly landed between runways 25 & 23		
	23/07/2004	Basler DC-3 Turbo	FAS117	Hydraulic problem en route. Overran on landing		
	08/02/2005	Airbus A340-600	G-VATL	No.1 engine lost power, shortly followed by No.4. Fuel cross fed manually and aircraft diverted	Fuel control computer system had design logic fault causing it not to transfer fuel automatically between tanks	Design fault
	03/02/2005	Ilyushin Il.76TD	ST-EWB	Pilot stated aircraft had developed problems with the fuel system. Crashed during attempted emergency landing		
	10/05/2005	Douglas DC-9-51	N763NC	Loss of right hydraulic system fluid quantity during a climb to cruise. The flight and landing was made without incident but aircraft then run away into A319 seriously damaging both	Right hydraulic reservoir empty, but cockpit gauge did not show it	Component failure, or possible maintenance error
	10/06/2005	BAE Avro RJ85	N530XJ	Hydraulic fluid spraying into cabin during taxy in. Emergency evacuation		
Mechanical failure - engines	15/03/2001	Douglas C-47	N842MB	During cruise at 5,000 feet, pilot heard a loud "bang". RH engine on fire and shut down. Propeller would not feather. On pulling extinguisher handle the engine separated from the aircraft. Aircraft lost hydraulic pressure. Emergency landing without further incident	Failure and separation of No.12 cylinder from the engine case that resulted in an in-flight oil fed fire; and the subsequent separation of the right engine from airframe	Component failure

	05/06/2002	Fokker F.27	G-CEXF	17 seconds after lift off, first officer requested 'climb power' and commander proceeded to reduce fuel trimmers towards climb power setting. Crew heard a loud 'bang' and LH engine Fire Warning activated. Commander shut down the engine, feathered the propeller and activated the fire extinguishers. Landed safely	Minimal fatigue strength margin of HPT disc, susceptible to rapid cracking if subjected to vibratory excitation, such as resonance. Abutment between HPT and IPT discs resulted in small gap being present between seal arms while engine operating. Allowed sufficient reduction in natural frequency of turbine disc vibratory mode for it to be excited while operating within normal speed range of engine. Protracted time taken following an earlier event, due to nature of tests required, to understand cause of failure, precluded timely introduction of suitable preventative action aimed at avoiding recurrence prior to the HPT disc failure on this aircraft. Fuel leakage from severed low pressure pipe, part of engine bay fuel system, led to major fire, external to nacelle	Unpredicted failure mode
	25/06/2001	Embraer Bandeirante	VH-OZG	In cruise at 10,000 feet RH generator warning illuminated. Reset and monitored output. 5 to 10 minutes later warning again illuminated. Simultaneously, RH engine fire warning activated. Several circuit breakers tripped. Unable to select engine fuel cut off with condition lever and could not feather propeller. MAYDAY due to smoke in cabin. Diverted, selected gear down but did not get any indication. Touched down on extended right main gear and skidded along runway. Came to rest with fire in right engine nacelle still burning	Vibration from worn armature shaft of right starter generator resulted in fractured fuel return line. Armature shaft failed in-flight. Sparks or frictional heat generated by failed starter generator ignited fuel/air mixture in RH engine accessory compartment	Component failure
	30/08/2002	Fokker 100	PT-MQH	At cruising altitude, crew noted "fuel filter" and "fuel low press" warnings for No. 2 engine. Fuel imbalance developed & aircraft losing fuel quickly. Diverted, but both engines stopped due to fuel exhaustion when still 16 miles from airport. Emergency landing in a field	Fuel line to No. 2 engine fuel pump snapped, causing fuel leak	Component failure

	11/11/2002	Fokker F.27	RP-C6888	Shortly after takeoff engine trouble developed in one engine. Pilot declared emergency and tried to land in a reclamation area, but decided at the last minute to ditch in the sea. Aircraft broke up and sank		
	08/12/2002	Boeing 767-219ER	ZK-NBC	Climbing through FL110, crew heard loud 'bang' and felt aircraft move right, followed by progressive yaw left. No.1 engine failure, shut down. Emergency declared, aircraft landed safely. Large rupture of outboard core cowl and severe gouging and scoring of outboard side of engine strut. LE flap panel extensively damaged, No. 2 canoe fairing behind engine sustained debris impact and puncture damage. First-stage HPT disk failure, releasing large segment of disk rim and outer web. Engine casing around disk completely severed & central shaft fractured between stage-one and stage-two high-pressure turbine disks	Initiation & growth of fatigue cracking from rear bottom corner of turbine blade fir tree slot. All cracked fir tree slots & several other uncracked slots showed surface microstructural flow & damage attributable to shot peening operation in a 1998 repair. Changes to manufacturing & repair shot peening processes. Revised inspection requirements to include more thorough examination	Maintenance error; inappropriate repair and inspection process
	05/01/2004	Fokker 70	OE-LFO	Severe engine vibration, loss of power, landed in undershoot	LP compressor case ice impact panels on both engines had come away in flight and become caught in front of the fan outlet guide vanes, resulting in by-pass duct blockage and significant loss of thrust	Component failure
	21/01/2004	Dassault Falcon 20	N200JE	Following touchdown, directional control was lost immediately after thrust reversers were deployed. Aircraft ran off side of runway	Left thrust reverser deployed, but right remained stowed	
	10/02/2004	Fokker 50	EP-LCA	Lost control and crashed on final approach. Both props went into reverse 2.5 miles from runway		
	08/02/2004	Cessna Caravan	VH-CYC	During training flight, engine power reduced to idle and propeller feathered to simulate engine failure. Engine then flamed out and aircraft ditched		
	07/03/2004	Cessna Caravan	XA-TBJ	Forced landing following loss of engine power		
	17/03/2004	Cessna Caravan	5H-MUA	Shortly after take-off a loud "buff" sound from the engine and a heavy splash of oil hit the windscreen. The engine then failed, and the aircraft forced		

				landed on a road		
	20/03/2004	Cessna Caravan	V3-HGB	Five minutes after take-off the engine lost power. Aircraft ditched		
	27/03/2004	Mitsubishi Mu-2B	N81MF	During descent, RH engine torque meter was reading zero. Pilot later stated this had happened before and that the torque would come back if he manipulated the throttle. However, he apparently took no action, the aircraft touched down hard and bounced leading to undercarriage failure		
	04/04/2004	Antonov An.26	UN-26582	Right propeller detached in the cruise and impacted the fuselage. Emergency descent and safe landing		
	27/04/2004	Cessna Caravan	N738FX	Engine failed en route. Forced landing on road		
	12/05/2004	Cessna Caravan	HK-2708	Crashed en route following an engine problem. Aircraft reportedly overloaded		
	08/06/2004	Hawker-Siddeley HS.748	TR-LFW	On climb out, crew noticed loss of oil pressure to No.2, which was shut down and feathered. Hydraulic pressure was then lost and gear failed to extend. Aircraft crashed into trees during attempted ditching		
	20/06/2004	Douglas DC-3	HK-1212	Immediately after take-off No.2 engine began to backfire and lost power. Aircraft lost height and hit trees		
	26/06/2004	Lisunov Li.2	RA-1300K	Lost power on one engine shortly after take-off. Lost height and hit a house	Investigation found lack of fuel in left tank	Possible maintenance error
	30/06/2004	Beech King Air	N432FA	Loss of engine power in the initial climb. Undercarriage collapsed on landing		
	12/07/2004	Convair 440	N4826C	En route No.2 engine high cylinder head and oil temperatures. Engine developed vibration and caught fire, which the fire bottles failed to extinguish and aircraft ditched		
	16/07/2004	Boeing 767-300ER	EI-CXO	Fire warning in No.2 engine just after V1. Take-off continued, engine shutdown and fire bottle discharged. Fire not extinguished and emergency landing carried out	Flexible fuel hose connected to Turbine Cooling Control had failed close to a connector, allowing fuel to spray out under pressure	Component failure

	21/07/2004	Fairchild Merlin IIIB	N84GA	On line-up, left engine hesitated at 75% torque, then increased to 90%. During take-off roll at 70kt, CAWI system on LH engine failed and it lost power. Aircraft veered left and take-off aborted, right engine surged during deceleration	Sensor wire to CAWI system on LH engine was broken and RH engine was misrigged resulting in delay when reverse thrust was selected	Component failure and maintenance error
	27/07/2004	Boeing 767-300ER	5Y-QQQ	No.1 fire warning shortly after take-off. Shutdown and extinguishers fired. Landed safely	Failure of No.3 bearing between LP and HP turbines, allowing hot oil/air mixture to escape under pressure. Spray entered area between engine and cowls and ignited. Bearing had been subjected to high temperatures for some time	Component failure
	09/08/2004	Avro RJ100	HB-IXU	En route, excessive vibration from No.2 engine, quickly followed by uncontained failure. Debris ingested by No.1, resulting in fire warning. Both engines shut down		
	16/08/2004	Cessna Caravan	HP-1397APP	Engine failure immediately after take-off. Forced landing on road		
	09/09/2004	Cessna 210N	ZS-KOX	Loss of power 11 minutes after take-off. Crashed during attempted forced landing	Propeller assembly found 5 nm from crash site	
	14/09/2004	Ilyushin Il.76T	4K-AZ1	No.3 fire warning climbing through FL110, almost immediately followed by No.4 fire warning. Safe overweight landing	No.3 engine suffered uncontained failure of LPT section, with debris impacting No.4, cutting fuel lines and leading to a fierce fire. Debris also impacted wing and fuselage	Component failure
	05/10/2004	Antonov An.12	ST-SAF	Engine failure in the cruise. Crashed during diversion	Evidence that none of the engines were developing power at the time of impact	
	17/10/2004	Boeing 777-200ER	F-OPAR	During taxy, overtemp warning on No.2 engine. AFS extinguished fire in upper RH area of cowling	Hydraulic leak from flexible hose igniting, possibly, when reverse thrust was engaged during landing	Component failure
	20/10/2004	Boeing 747-100F	N709CK	After take-off, No.1 engine and pylon broke away. Safe landing		
	22/10/2004	Beech 1900C	N79YV	One engine lost power during descent, quickly followed by second engine. Aircraft ditched		
	01/12/2004	Boeing 777-300	B-HNI	Shortly after take-off, the D duct, part of the thrust reverser on No.1 engine, detached and fell away	Heat from the engine caused delamination of the duct, leading to its failure	Induced component failure
	01/12/2004	GA Gulfstream IV	G-GMAC	Failed to slow on landing and ran off the side of the runway	Crew could not activate thrust reversers or ground spoilers	

	08/01/2005	Antonov An.12	9Q-CIH	Engine failure after take-off, failed to maintain height and crashed	No AOC, not insured, no crew qualification or training records, no maintenance records, aircraft 6.5 tonnes over MTOW	
	19/02/2005	Boeing 747-436	G-BNLG	No.2 surged & suffered internal damage after take-off. Aircraft continued across the Atlantic on 3 engines but had to divert due to high fuel burn	Second engine shut down in the cruise on same aircraft 6 days later	
	22/02/2005	CASA Aviocar	P-2032	Crashed into the sea 100 metres offshore, approx. 400 metres from the runway. Engine trouble reportedly preceded the accident		
	22/02/2005	Convair CV.580	FAB-73	Crashed shortly after take-off following engine problems		
	08/04/2005	McDonnell MD-88	N	Take-off aborted due to contained engine failure		Component failure
	19/04/2005	Embraer ERJ145	N814HK	Uncontained failure of LH engine. Landed safely		Component failure
	02/06/2005	Antonov An.24B	ST-WAL	Crashed on takeoff. A fire erupted in the nr.1 engine, causing severe damage to the engine and the left-hand side of the fuselage.		
	06/06/2005	Douglas DC-3	HK-3462	The aircraft crash-landed while attempting to return to the airport following engine problems. The aircraft caught fire after it had been evacuated.		
	13/06/2005	Douglas R4D-8	N3906J	Just after take-off at about 300 feet, the No.1 engine caught fire. Aircraft crashed in a residential area	Propeller pitch control mechanism failure, crew could not feather it	Component failure
	06/08/2005	EADS ATR-72-202	TS-LBB	One engine failed in the cruise, quickly followed by the second. Aircraft ditched	Aircraft had been fitted with wrong fuel gauge (intended for ATR42) which over read fuel contents by 1,800kg	Maintenance error
Mechanical failure - miscellaneous	11/05/2004	Airbus A320	EC-HTD	After take-off, fan cowls on both engines came open and were torn off by slipstream, striking the aircraft, which landed safely	First take-off after overnight ramp maintenance	Maintenance error
	13/07/2004	Airbus A320	N951LF	During take-off, No.1 engine cowling outboard section opened and separated. Later No.1 engine oil quantity amber light on. Landed safely		Possible maintenance error
	04/12/2004	Convair 580	N161FL	Post-maintenance test flight after work on left propeller. Crew shut down and feathered left engine, but after re-start the propeller was not operating correctly. During approach, the flaps failed to travel, alternator light was on and hydraulic gauge indicated zero. No nosewheel steering or		Possible maintenance error

				brakes, aircraft ran off the runway		
	24/05/2005	McDonnell MD-90	N910DN	Slide deployed just after take-off. Emergency landing		
Mechanical failure - unspecified	24/02/2005	Rockwell Jet Commander	XC-COL	18 minutes after takeoff, the pilot radioed that he had some problems and that they were diverting. Disappeared from radar and was later found to have crashed in a mountainous area.		
	26/03/2005	Let 410	HK-4146	Failed to climb and hit hills close to runway	Initial reports suggest technical fault	
	02/05/2005	Swearingen Metro III	ZK-POA	Crashed in rural farmland Following midair break-up. Fire believed to have erupted prior to the accident. Landing gear extended as it crashed, which could indicate a fire in the area of a main gear wheel well		
	02/06/2005	Let 410UVP-E3	TG-TAG	Crashed while returning to the airport after developing technical problems after takeoff.		
Design error	06/03/2002	Dornier Do.328	G-BWIR	During take-off roll at 100 kts, red 'Doors' warning caption illuminate. Rejected the takeoff, bringing the aircraft to a complete halt on the runway. Probable cause was senior cabin attendant grasping inner door handle to restrain herself during rapid acceleration. The ergonomics of the cabin crew seat and door handle made such an involuntary action readily conceivable. Such action led to the door unlatching and opening rapidly. Failure of the damper attachments and disruption of the banister mechanism then allowed forcible over-travel, leading to failure of the airstair attachment arms. The remaining attachment strength of the door and airstairs was such that both would almost certainly have separated had the aircraft become	The door and airstair design, though technically complying with the certification requirements, lacked the necessary integrity to prevent a hazardous occurrence to the aircraft. Follow-up / safety actions: Safety Recommendation 2003-109: It is recommended that the European Aviation Safety Agency review the design characteristics of the door operating, attachment and restraint mechanisms of the Dornier 328 aircraft type, in order to minimise the possibility of inadvertent door operation and to ensure that there is sufficient residual strength in the door/airstair attachments to prevent separation of the door in the event of a door coming open during takeoff or initial climb	Design fault

				airborne. Had separation occurred, the port propeller and other critical parts of the aircraft would probably have been struck. A catastrophic outcome could not be ruled out.		
	20/12/2004	Lockheed-Martin F/A-22		Control lost shortly after take-off. Pilot ejected safely	The aircraft was lost due to the failure of all three rate sensor assemblies, which provide feedback on yaw, roll and pitch status to the Flight Control System (FCS). The pilot had inadvertently triggered the failures during his pre-flight preparations when he shutdown the engines for a maintenance check, believing the FCS was continuously powered by the APU	FCS momentarily lost power, known system anomaly, programmed to interpret momentary power loss as instruction to enter test mode, which or latches the unit. FCS unable to warn pilot. 20 control units returned to BAE by this time for investigation of suspected latching events, resulting in a design change and fleetwide embodiment of a new standard unit

APPENDIX C – SSCM EVENT CODES TABLE

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
Crew report	C	Fault indication	1	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Failure	2	None	A	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
Crew report (continued)	C	Parameter exceedance	3	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
					X	Human factor event	H
Flight data	F	Fault indication	1	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Failure	2	None	A	Confirmed Fault	F

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
Flight data (continued)	F	Failure (continued)	2	None (continued)	A	Induced fault	I
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Parameter exceedance	3	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
On-board diagnostics	D	Fault indication	1	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
On-board diagnostics (continued)	D	Fault indication (continued)	1	None (continued)	A	No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other		Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Failure	2	None	A	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Parameter exceedance	3	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
On-board diagnostics (continued)	D	Parameter exceedance (continued)	3	Reset	B	Confirmed Fault	F
						Human factor event	H
						Induced fault	I
						Monitor	M
						No fault found	N
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
1st line engineer	E	Fault indication	1	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Replace	D	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
1st line engineer (continued)	E	Failure	2	None	A	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Repair	E	Confirmed Fault	F
						Induced fault	I
						Human factor event	H
				Replace	D	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Parameter exceedance	3	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Repair	E	Confirmed Fault	F
						Induced fault	I
						Human factor event	H
				Replace	D	Confirmed Fault	F
						Induced fault	I
						No fault found	N

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
1st line engineer (continued)	E	Parameter exceedance (continued)	3			Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Scheduled maintenance	4	On-aircraft maintenance	F	Condition / status report	S
				Replace	D	Condition / status report	S
2nd line engineer	F	Unscheduled maintenance	5	Repair	E	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Replace	D	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Scheduled maintenance	4	Overhaul	G	Condition / status report	S
				Replace	D	Condition / status report	S
Depot / MRO repair	G	Unscheduled maintenance	5	Repair	E	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Replace	D	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
Depot / MRO repair (continued)	G	Scheduled maintenance	4	Overhaul	G	Condition / status report	S
				Replace	D	Condition / status report	S
Investigation	H	Fault indication	1	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
					A	No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
		Failure	2	None	A	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N

DATA SOURCE	CODE	EVENT CATEGORY	CODE	ACTION TAKEN	CODE	FINDINGS	CODE
Investigation (continued)	H	Failure (continued)	2	Other (continued)	X	Human factor event	H
		Parameter exceedance	3	None	A	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Reset	B	Confirmed Fault	F
						Induced fault	I
						Monitor	M
						No fault found	N
						Human factor event	H
				Other	X	Confirmed Fault	F
						Induced fault	I
						No fault found	N
						Human factor event	H

APPENDIX D – GAIN AIRLINE FLIGHT SAFETY MANAGEMENT SURVEY

AIRLINE FLIGHT SAFETY MANAGEMENT SURVEY

As part of the current GAIN Action Plan, Working Group B *Analytical Methods and Tools* is undertaking this survey of airline flight safety management processes and requirements to guide GAIN in its future activities to address airline needs for analytical methods and tools.

The intent of this survey is to understand and document how airline flight safety management processes and procedures are currently practiced, and the resources available to support the analysis of flight safety data. The survey will collect data on staffing levels, training and experience, and how flight safety duties are generally performed. It also asks about what data sources and analytical techniques are being utilised by flight safety offices. Opinions about enhancements to analytical methods and tools and additional training opportunities which would help improve safety management within an organisation are also requested.

Survey responses will be confidential and the information will be de-identified in presenting the survey findings. Participating airlines will not be identified, except in terms of their general size and scope of operations (e.g. a large European carrier with worldwide services).

Q.1 Current aircraft fleet

Enter number of aircraft in each category

_____ Wide-body jet aircraft

_____ Narrow-body jet aircraft

_____ Regional jet aircraft

_____ Turboprop aircraft

Q.2 Flight safety staffing levels

(a) Flight safety department

*Enter number of **flight safety department** staff in each category*

_____ Full-time personnel

_____ Part-time personnel with flying duties (*average hours per month:* __)

_____ Other part-time personnel (*average hours per month:* _____)

*Enter number of staff positions (full-time equivalent) with the following **flight safety** duties in the **flight safety department***

_____ Flight safety programme management

_____ Incident and safety report investigation

_____ Internal and external audits

_____ Flight data management / flight operational quality assurance

_____ Other *(describe)* _____

b) Other departments

*Enter number of staff with designated **flight safety** responsibilities in **other departments** (e.g. flight operations) in each category*

_____ Full-time personnel

_____ Part-time personnel with flying duties (*average hours per month:* ___)

_____ Other part-time personnel (*average hours per month:* _____)

*Enter number of staff positions (full-time equivalent) with the following **flight safety** duties in **other departments***

_____ Flight safety programme management

_____ Incident and safety report investigation

_____ Internal and external audits

_____ Flight data management / flight operational quality assurance

_____ Other *(describe)* _____

Q.3 Flight safety department staff background, experience and training

*Enter the number of **flight safety department** staff with the following background, experience and training.*

(a) Background/experience

_____ Line pilot

_____ Flight instructor / check pilot

_____ Maintenance inspector

_____ Flight attendant

_____ Other *(describe)* _____

(b) Flight safety training/qualifications

Count each individual once on the basis of their most extensive formal training.

_____ Degree/certificate in safety management [MOST EXTENSIVE]

_____ Military safety officer school

_____ Safety auditor credentials

_____ 1-2 week short courses

_____ 2-4 day short courses

_____ Attend workshops, seminars, etc. [LEAST EXTENSIVE]

Q.4 Flight safety department staff training

(a) How many different courses have **flight safety department** staff taken in the past **three years**? _____

List each course, the organisation that offered it, and how many staff have taken the course during that time:

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

(b) How many **other** courses have **flight safety department** staff taken **more than three years ago**? _____

List each course, the organisation that offered it, and how many staff have taken the course:

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

Course: _____

Organisation: _____
Staff: _____

Q.5 What guidance do flight safety department staff get on how to manage safety?
Tick all that apply and provide associated information

_____ Company safety manual with detailed procedures to be followed

_____ Recommendations from company Safety Committee

_____ Interaction with senior management on a regular basis (*How often?* ___)

_____ Interaction with flight safety staff at parent company or code-share partners

_____ Information from industry associations, civil aviation authority, etc.

_____ Training on the use of in-house analytical tools

_____ Other *(describe)* _____

Q.6 How would you describe your company's flight safety management strategy?
Tick all that apply and provide associated information

_____ Monitor safety reports, identify risks, and implement corrective actions

_____ Analyse flight data from quick access recorders, identify exceedences from nominal performance, and implement follow-up actions

_____ Preserve confidentiality and foster a non-punitive safety culture

_____ Conduct regular safety meetings with flight crews (*How often?* _____)

_____ Other *(describe)* _____

Q.7 **What safety data or information does the flight safety department collect and analyze on a routine basis?**

Tick all that apply and provide additional information where indicated

_____ Air safety reports *(U.S. carriers: tick if included in ASAP programme)*

_____ Confidential human factors reports

_____ Cabin safety reports

_____ Ground damage reports

_____ Hazard identification reports

_____ Safety hot line

_____ Aircraft flight data (FDM/FOQA)

_____ Aircraft technical log

_____ Other *(describe)* _____

Q.8 **What other sources of information does the flight safety department make use of?**

Tick all that apply and provide associated information

_____ Line Operations Safety Audits *(date last performed:* _____*)*

_____ Internal evaluation assessments *(how often performed:* _____*)*

_____ Consolidated safety information from other airlines (e.g. STEADES)

_____ Informal reports from flight crew or other personnel

_____ Feedback from flight crew during training or safety briefings

_____ Information from civil aviation authority

_____ Information from manufacturers or industry associations

_____ Safety bulletins and magazines

_____ Internet, e-news

_____ Conferences, seminars, workshops *(approx. number in past year)* _____

_____ Other *(describe)* _____

Q.9 Which analytical tools does the flight safety department use?

Tick all that apply and provide associated information. If used in the past but no longer used, enter "P".

_____ Microsoft Excel or similar spreadsheet program

_____ Microsoft Access or similar database management software

_____ AQD

_____ AvSIS

_____ BASIS/ASR

_____ Other BASIS modules *(list)* _____

_____ Other commercial air safety reporting system *(which?)* _____

_____ Internal company air safety reporting system

_____ FDM/FOQA analysis tools *(which?)* _____

_____ Aircrew Incident Reporting System (AIRS)

_____ Procedural Event Analysis Tool (PEAT)

_____ Risk analysis tool *(which?)* _____

_____ Other *(which?)* _____

Q.10 Which aspects of the work in your flight safety department could benefit from increased automation or better integration between existing systems and tools?

Tick all that apply and provide additional information where indicated

_____ Getting information from flight crew and others

_____ Data entry

_____ Correcting reports in database

_____ Preparing routine reports

_____ Transferring data between different analysis programmes or reformatting data to match the requirements of specific analysis software

_____ Other *(which?)* _____

Q.11 What are the outputs of the flight safety department

Tick all that apply and provide associated information

_____ Regular briefings to senior management *(about how many per year?)* ___

_____ Briefings to the Board Safety Committee *(about how many per year?)* _

_____ Periodic safety report or incident digest *(about how many per year?)* _

_____ Periodic safety summary *(about how many per year?)* _____

_____ Flight crew briefings *(about how many per year?)* _____

_____ Presentations at training courses *(about how many per year?)* _____

_____ Articles in company safety magazine

_____ Pilot and department bulletins*(about how many per year?)* _____

_____ Exchange of information with other airlines

_____ Other *(which?)* _____

Q.12 Do you attempt to measure the overall safety level in your airline? Yes / No *(circle one)*

If so, how? _____

Q.13 Do you share flight safety information with other airlines? Yes / No *(circle one)* If so:

(a) What type of information? _____

(b) How is the information shared? _____

What types of information would it be helpful to obtain from other airlines, if it could be made available? _____

THE FOLLOWING QUESTIONS ARE DESIGNED TO PROVIDE INFORMATION ON FLIGHT SAFETY TRAINING NEEDS AND CONSTRAINTS

Q.14 In which areas would you like the flight safety staff to be able to obtain additional training or education?

Tick all that apply and provide additional information where indicated

_____ Incident investigation

_____ Human factors analysis

_____ Statistical analysis

_____ Risk assessment

_____ Root cause analysis

_____ Use of specific analysis tools *(which?)* _____

_____ Other *(describe)* _____

Q.15 What impediments (if any) limit the ability of the flight safety staff to get needed training or education?

Tick all that apply and provide additional information where indicated

_____ Lack of appropriate courses

_____ Cost of attending courses

_____ Too much workload to permit time away from the office
_____ Other *(describe)* _____

APPENDIX E – STUDENT QUESTIONNAIRE

MSc AIR TRANSPORT MANAGEMENT / AIR SAFETY MANAGEMENT

AIRCRAFT SYSTEM SAFETY QUESTIONNAIRE

As part of our research programme into aircraft system safety, we would like your views on a number of related issues.

Whatever your role in the industry, your feedback would be greatly appreciated. Please spend a few minutes answering the questions below, and return this paper to Steve Bond at s.j.bond@city.ac.uk

Many thanks!

Question 1

What is your role? Pilot / engineer / ground handler / operations / ATC /

Other (please specify).....

Question 2 (for pilots and engineers only)

Do you have any concerns about the reliability of your aircraft systems?

Yes / No

If "yes", please give an example(s)

.....

.....

.....

Question 3 (for pilots only)

How often, in percentage terms, do you have to refer to the MEL prior to dispatch? (Please indicate aircraft type(s)

.....

Have systems ever failed in an unexpected way? Yes / No

If "yes" have they ever done so in a way that you considered to be dangerous? Yes / No

Question 4

Does your company have an incident / event reporting system (confidential or otherwise)?
Yes / No

If you said "yes", does the system capture input from all areas of the business?

.....

.....

Does the system allow you to enter all the information you would like to?

Yes / No

Is the system easy to use? Yes / No

Question 5

If you said "yes" to Q4, is the system effective? Yes / No

If you said "no" , why is it not effective?

.....

.....

Question 6

When you enter something on the system, do you get effective feedback?

Always / Usually / Rarely / Never

Question 7

Do you have access to general reporting systems such as BASIS? Yes / No

If you said "yes" , do you find it useful? Yes / No

If "no", why not?

.....

.....

.....

Question 8

Do you know if other operators of the same aircraft types share your problems and issues?
Yes / No

If "no", why do you think that is?

.....

.....

Question 9

Any other comments about the understanding of aircraft system behaviour and reliability that you would like to make

.....

.....

.....

.....

.....

Question 10

The air transport industry is concentrating its flight safety efforts almost exclusively on addressing what are known as "human factors" accident causes, such as CFIT, approach and landing, loss of control, etc. Do you think system behaviours and failures should also be addressed?
Yes / No

Thanks for your time