A Method of Active System Safety

Brian Robinson Kirk

Thesis submitted for the degree of Doctor of Philosophy

Awarded by
London Metropolitan University
Department of Computing
London

January 2008

Abstract

The concept of Active Safety proposed originally by Prof Schagaev [3][4][5][6] can be applied to provide additional improvement in safety of a system over its operational lifecycle by continuous analysis and assessment of the state of the system in real time of its operation and reacting dynamically to improve its safety. This thesis develops the concept, theory and an implementation for a Method of Active System Safety (MASS) for application in the field of Aviation. The thesis has three parts:

Part 1 researches the Aviation domain and current safety practices. General and Civil Aviation flight statistics are analysed to gain and understanding of flight risks, their causes and opportunities to improve safety. Current approaches to safety management are reviewed then the Principle of Active Safety (PASS) is introduced.

Part 2 explores how PASS can be used as a basis for improving operational reliability, and so safety; the PASS algorithm is presented. A theoretical reliability model is then developed for the operational lifecycle of an aircraft and then conditional, preventive and PASS assisted maintenance strategies are evaluated. The beneficial effect of introducing PASS is then demonstrated at 2 levels: first *during the lifecycle* of use of an aircraft showing how apparent reliability can be improved and unnecessary maintenance reduced and second *during each flight*, using PASS to improve flight reliability. This uses an operational model (flight modes and limits) and a physical aircraft model (elements and fault detection) using dependency and recovery matrices. A means is proposed to provide timely and relevant safety advice based on continuous PASS analysis in real time of flight operations. A prototype implementation is described and a process proposed for characterisation of the system for a particular aircraft. The state of the art in Active Safety is reviewed and suggestions for further research are outlined.

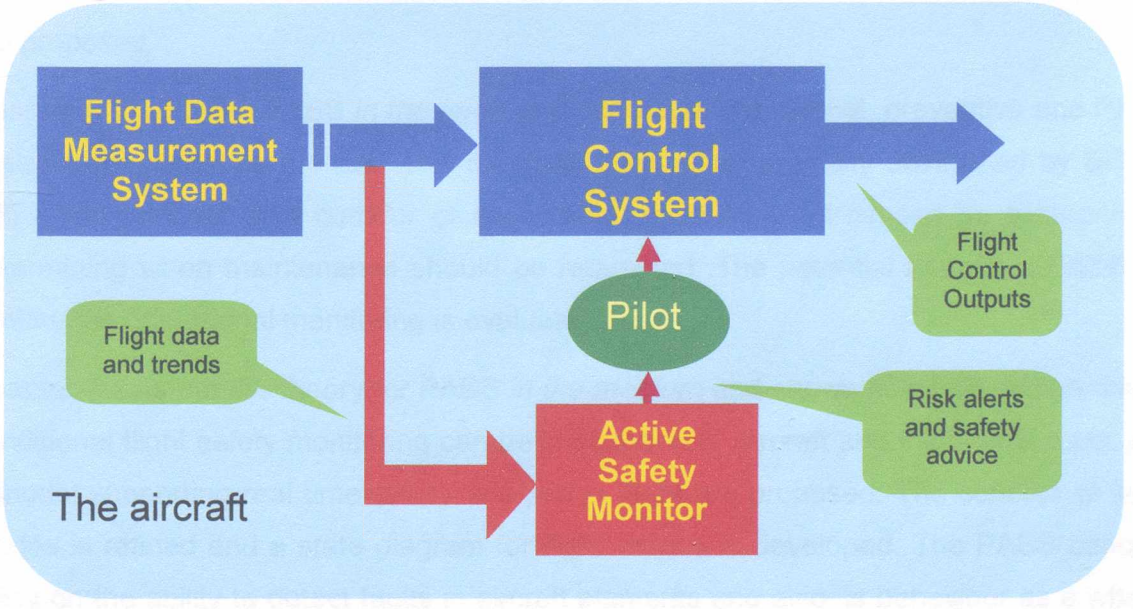
Part 3 contains supportive information in the Appendices.

The contribution made to the knowledge of Active Safety is a theoretical and practical development of the concept in terms of aircraft classification, flight risk analysis, operational reliability modelling, fault analysis, the application of PASS in aviation and a system design for an Active Safety Monitor which operates in real time of flight.

Summary

Safety is concerned with the avoidance of harm to people and property. At the operational level conventional approaches to safety in aviation have been based on the broad application of a set of regulations, procedures and control. At the equipment level it has been concentrated on the use of techniques such as static fault tree analysis and dynamic verification to achieve confidence in its design, and redundancy to achieve the required availability (system reliability) in operation. The impetus for improvement has often been the occurrence of serious accidents and flight data recording is mandated in Civil Aviation (CA) to provide data for a 'post mortem' analysis of their causes. These approaches have been very successful in improving the safety of flight in CA but the rate of improvement of safety has been low for three decades [25]. General Aviation (GA) continues to be much less safe; regulation is more lax and flight recorders are currently too expensive to fit and are not mandatory. Clearly new concepts and initiatives are needed to enable the continued improvement of safety.

The thesis of this dissertation is that the concept of Active Safety proposed originally by Prof Schagaev [3][4][5][6] can be applied to provide additional improvement in safety of a system over its operational lifecycle by analysing relevant data of the system in real time of its operation and reacting dynamically to improve its safety. Here 'active safety' is defined as the continuous analysis and assessment of the state of a system during its operation and the use of the results to sustain or improve the overall safety of the system.



Overview of the Thesis

The thesis covers the concept, theory and implementation of A Method of Active Safety using the context of aviation as the application domain.

Chapter 1 provides a brief introduction; it states the central proposition and aims of the thesis and reviews previous work in Active Safety.

Chapter 2 contains a survey of the aviation application domain and develops a classification based on mission, type of aircraft, technical characteristics. The purpose of this is to create a classification that will later support the characterisation of a configurable Active Safety Monitor to match as wide a range of particular aircraft types as possible. The aircraft market is then reviewed for military, civil and general aviation to gain a better understanding of where and how to target a practical Active Safety system.

Chapter 3 reviews safety in aviation in terms of the main causes, factors and impacts of risk. Safety management schemes are reviewed and weaknesses in current regimes are highlighted. It introduces the flight lifecycle and the risks associated with phases of flight such as taxiing, take-off, cruise and landing.

Chapter 4 introduces the Principle of Active System Safety (PASS) in the context of aviation over three scopes and timescales: the whole life of the aircraft, during a flight; and at the micro level within equipment implementation. These are referred to as PASS in the *large, medium and small*. Redundancy theory is introduced to support possible dynamic system reconfiguration as a means to conserve system safety. The PASS algorithm is described and a generalised theory of system safety presented.

Chapter 5 develops a reliability model for aircraft operation by considering a flight to be composed of flight phases each with its own risk profile. The operational reliability of flight, and of the aircraft in the long term, is cumulatively modelled on flight phases and transitions between them. Measures for operational point, mission and interval availability are proposed.

Chapter 6 introduces PASS *in the large* and compares conditional, preventive and PASS assisted maintenance models. The methods used were originally developed by Birolini [48] . The concept of a corridor of acceptable reliability is introduced as a means for determining when maintenance should be requested. The potential benefit of PASS for continuous operational monitoring is evaluated.

Chapter 7 sets out the theory for PASS *in the medium* and shows how information driven conditional flight safety monitoring can be implemented. Aircraft and Flight structures and a model supporting real time safety analysis in flight are proposed. The concept of flight modes is refined and a state diagram for flight modes is developed. The PASS concept relies on the ability to detect faults in aircraft elements and also its behaviour as a whole; techniques for achieving this are reviewed. The fault dependencies between elements are then used to determine the likely consequence of a faulty element and also the causal influences on that element. Algorithms are presented for evaluating the most likely impact of the fault in real time so that safety advice can be offered to mitigate its effect.

Chapter 8 describes the design of a system for a low cost implementation of an Active Safety Monitor. The software is written entirely in Oberon SA, a language designed by Prof N Wirth of ETH. The software has a clear modular structure and is supported by a set of development tools and test facilities. The fault tolerant aspects of the hardware design are outlined.

Chapter 9 describes the information used to characterise the Active Safety Monitor for a particular aircraft summarised in the diagram below. This includes a parameter correlation matrix for real time co-dependency checking, an element fault dependency matrix and the flight mode transition matrix; other matrices enable the definition of dependencies and variations of 'limits' relating to the flight context, as shown below:

	Parameter Values	**Elements**	**Flight Modes**
Parameter Values	**1** Parameter Correlation Matrix	**4** Parameters Used by Elements Matrix	**5** Parameter Limits per Flight Mode Matrix
Elements	**9**	**2** Element Fault Dependency Matrix	**6** Element Characterisation by Flight Mode Matrix
Flight Modes	**8**	**7** Flight Mode Characterised by Elements Matrix	**3** Flight Mode Transition Matrix

A process for eliciting the information needed to populate the matrices is proposed.

Chapter 10 reviews the state of the art in Active Safety. It proposes opportunities for further research and possibly further applications of Active Safety and PASS.

Chapter 11 provides a brief summary and draws conclusions based on the thesis.

Chapter 12 provides a numbered list of sources of information. References to them are denoted by square brackets in the text, like this [42].

Appendix 1 provides a summary of the abbreviations and mnemonics used in the text

Appendix 2 provides a glossary of terms

Appendix 3 provides details of flight data sets and future trends in this area

Appendix 4 includes the configuration data for flight mode detection (in XML)

Appendix 5 contains the detailed patent claims for the UK MASS Patent

Appendix 6 provides a review of the history of flight data recording technology

Appendix 7 includes a set of scenarios used for flight testing of the prototype system.

Theoretical, implementation and application contributions

The *theoretical novelty* is in the following individual contributions and their combination:

1. A proposed new Principle of Active Safety (PASS) based on the improvement of operational reliability of a system by real-time evaluation of operational data. The focus is on refining the context of analysis (the flight mode), detecting and determining the nature of any faults in the system and providing advice which can mitigate the effect of the fault and/or improve the safety of the system.

2. An analysis of the applicability of Active Safety for various classes of aircraft, particularly in GA and CA, leading to a new classification schema.

3. A method of analysing a system as a network of safety dependencies between elements and searching the resulting graph to determine the consequences of a fault in an element and the factors contributing to its occurrence.

4. A generalised Algorithm of Active Safety (APASS) which can be applied in aviation and other domains. Originally this was proposed by Prof Schagaev.

5. A means to refine the current context of safety analysis in real-time of flight.

6. An implementation based on a small, low cost fault tolerant computer, software and hardware development and runtime environment and a flexible XML based declarative specification for configuring the system and parameters for a particular type of aircraft.

7. A Patent which protects some key Intellectual Property of Active Safety.

The *implementation novelty* is embodied in the following:

1. The structure of the overall system, its architecture, design and implementation.

2. The organisation of the software in terms of its static modular structure and dynamic runtime framework.

3. The use of XML as a tool for configuration and characterisation of an individual implementation of Active Safety for a particular aircraft.

4. The identification of efficient data structures required for real-time implementation of APASS including the parameter co-dependency matrix, the flight mode transition matrix, the fault propagation dependency and recovery matrices.

5. The development of real time algorithms for flight mode detection (context refinement) and implementation of APASS in the context of aviation.

6. The determination and development of the tools necessary to prepare and use the system for trials in General Aviation.

The novelty in application is as follows:

1. Implementation of a practical scheme for applying Active Safety in GA.

2. Creation of a low cost equipment capable of operating as both a Flight Data Recorder and an Active Safety Monitor; based on solid state Flash memory.

3. Use of a WEB server in the equipment to ease integration with external Human Machine Interface devices.

Contents

Acknowledgements

I would first of all like to acknowledge my Supervisor Prof Igor Schagaev for introducing me to the new field of Active Safety and for his support, patience and encouragement during the research and preparation of the thesis. I would also like to thank Professor Bob Gilchrist for his support, reviews and advice, both before starting and during the research. Dr Hao Cai has been an excellent sounding board for ideas and has always been positive, enthusiastic and encouraging.

The research on Active Safety has been allied to and encouraged by the EU ONBASS Project, for details see www.onbass.org [75]. I would like to thank the following collaborators for their support. Prof Jurg Gutknecht, Prof Niklaus Wirth, Dr Felix Friedrich, Thomas Kaegi and Florian Negele of the Computer Systems Institute at ETH Zurich who provided the initial hardware prototype and software tools needed to create the application test environment used to prove the concepts. Angus Kintis of Spirit SA in Greece offered much advice based on his knowledge and practical experience of General and Commercial Aviation operational practice. Dr Thomas Wittig of Euro Telematik AG in Ulm Germany offered the benefit of his experience in avionics and current safety and avionics equipment regulations. Prof V Bukov of the Institute of Avionics in Moscow provided valuable insights and jointly authored 2 Papers [1], [2]. Dr Dan Alexandrescu of Irotech designed and produced the prototype hardware. Simon Monkman advised on the document layout and graphic design of the diagrams.

I would like to acknowledge the financial support of my employer Robinson Systems Engineering Ltd which has enabled me to engage in this research. I also offer warm thanks to my colleagues at Robinsons, including Stuart Doyle, Toby Harris, Tracey Williams and Dr Tom Priestley who have between them taken over my previous duties whilst the research has been in progress.

I would like to especially thank my two external examiners Prof V. Kutakov, Deputy General Director of the Russian Federation State Research Centre, and Prof J. Zalewski of Florida Gulf Coast University USA for their constructive criticism and supportive advice. The thesis has been revised and improved based on their feedback.

Finally I would like to thank my family. My wife Nina has put up with me being occasionally tired, distracted, and grumpy and *'always on that machine'* whilst providing an environment where I could be productive. My son Peter has kept me mentally refreshed with a miscellany of contributions that have provided light relief.

To anyone I have inadvertently omitted to mention, my apologies and thanks.

Author's Statement

I declare that this thesis is original work conducted by the author between January 2005 and September 2007 in the Active Safety Group of the Department of Computing, Communication and Mathematics of London Metropolitan University in London. Some parts of the thesis have already been published within private documents of the EU ONBASS (ON Board Active Safety System) Project [75] and in a filed UK Patent Application 0707057.6 [1] ; these are cited in the references.

My objectives for the research work have been to:

1. Discover the differences between research and development activities
2. Gain expertise and experience in research in a practical and effective way
3. Define the context and theoretical basis in the field of Active Safety in aviation and a Method of Active System Safety.
4. Contribute to Prof Schagaev's team effort to implement an ultra reliable active safety system for aviation, including a fault tolerant computer development [56].
5. Contribute to the ONBASS team effort to implement and verify an implementation of an Active Safety system for General Aviation.

I would like to acknowledge the source material that has been an essential foundation for the project. The key papers are from Prof I Schagaev [3] [4] [5] [6] [40] and Dr David Warren the founding father of Flight Data 'black boxes' [25] [31] [44] [48] [1].

I have received assistance in many aspects of the research as part of the Active Safety group at London Metropolitan University and from the team working in the ONBASS project from January 2005 to October 2007. In particular I received assistance from:

Prof I Schagaev of London Metropolitan University who acted as my Supervisor and gave direction to my contribution to the theoretical aspects of the research.

Dr Hao Cai of London Metropolitan University who assisted with the initial analysis of the forward and backward tracing algorithms.

Prof V Bukov of NIAAO in Moscow in collaboration with Prof Schagaev performed the analysis of the dependency graph for a specific aircraft.

Dr Eugene Zueff and Prof Schagaev developed the tools for creating and editing the Dependency Matrix.

Mr Angus Kintis of Spirit SA (Greece) contributed his experience of aviation and co-dependencies between flight parameters.

The system software team at ETH Zurich (Switzerland) who designed and produced the ONBASS development environment and the Minos real-time system, including: Prof Jurg Gutknecht: Oberon System Concept and Architecture

Prof Niklaus Wirth: Oberon SA Language Compiler for ARM processor

Dr Felix Friedrich (FF): WinAOS, Device Management and XML compiler

Mr Tom Kaegi-Trachsel: Minos Real-time System and Module loader

Mr Florian Negele, V Romanoff and Brian Kirk: Oberon SA Compiler Verification

Dr Wolfgang Richter (of ETG Germany): Minos WEB server and Flight Data Interface

Prof Michael Nikoliadis, Dr S Rossignol and Dr Dan Alexandrescu of Irotech (France) designed and produced the prototype ONBASS hardware and support tools.

My original contribution has been to identify, separate and refine the concepts and theory and to synthesize a clearly stated Method of Active Safety in Aviation. The main practical achievement has been producing a system design with Prof Schagaev as a basis for a working prototype and then working with the ONBASS team to implement it.

Dedication

This thesis is dedicated to the memory of my parents Doreen and Bill Kirk and their close friends Kath and Ron Harvison. Ron first sparked my interest in electronics and radio and was a kind and patient mentor for many years. He was a pioneer of computing and in 1949 designed the electronics for the 'Williams Tube', the first practical charge based random access memory technology [55],[98],[99] for computers.

A Method of Active System Safety

1 Introduction

Safety is concerned with avoiding harm to people, property and the environment. The Principle of Active System Safety (PASS) [2] seeks to improve safety by systematically lowering the risk of operation of a system by mitigating the consequences of detected faults. This thesis investigates and evaluates the potential for applying PASS methodically using aviation as an application domain. The central proposition of this thesis is:

" a Method of Active System Safety in the form of an Active Safety Monitor can be applied to provide an improvement in the safety of a system over its operational lifecycle by continuous analysis and assessment of its state in real time of operation, identifying faults, and consequent risk, and reacting dynamically to improve the operational reliability of the system and safety of its operation using fault tolerance techniques and risk mitigation."

This thesis develops the concept, theory and an implementation of a Method of Active System Safety (MASS) for application in the field of Aviation.

For over 150 years safety in many domains such as railways, ships boilers and aviation has been improved by investigating incidents, understanding the faults that caused them and using that knowledge to systematically improve their design and operation [1], [1]. The improvement process has naturally been slow: first a serious accident occurred, then an enquiry held, recommendations made, regulations formed and finally changes to the design and/or operational use of systems made. This process has been effective in the long term but future improvements require a faster and more adaptive response, particularly as the size and complexity of systems increases.

In the 1990's Prof I Schagaev introduced the concept of dynamic safety [3], [4], [5] and this has been refined into PASS [6], a trial implementation was presented in [1]. *The key difference in the PASS approach is that it deals with the behaviour of the whole system and in a timely way; it is a system wide and systematic approach and can be applied at different scopes of operation, for example over the lifespan of an aircraft, during a single operational flight or even over the lifecycle of a computer instruction.*

This thesis explores PASS and its application in the field of aviation in 3 main parts. Part 1 defines aviation in terms that make it possible to apply PASS effectively. This is achieved by using classification as a tool to reveal the essence, structure, similarities and relations. Classification is applied to aircraft and the aviation market. Then safety in aviation is explored based on an analysis of the evident risk factors and the features and

requirements for a new aviation safety system are analysed. This leads to the development of a systematic approach for improving operational safety. An estimate of the likely market for devices which could improve the operational safety of aviation, particularly General Aviation is included.

Part 2 is concerned with the analysis of risk related to an aircraft based on flight data measured in real time of flight. It provides a detailed description of PASS and the PASS algorithm and the results of modelling experiments involving aircraft operation. It concludes with an outline of future research opportunities.

Part 3 contains supporting material in the form of Appendices.

The aim of the thesis is to propose, analyse and develop a Method of Active System Safety (MASS) by refining the Principle for Active System Safety (PASS) for aviation. Rather than just recording data during an aircraft's flight, in order to allow post-crash analysis to be carried-out, the new approach proposes the analysis of available data in real time during the flight and reacting on an analysis of the data with the aim of accident prevention. The theoretical principles of active system safety are developed by separating the aspects of the flight safety (risk) model, information flow model and control system model. Subsequently, analysis of the dependencies within and between the models defines the features, functions and structures of the onboard active safety system and its software and hardware.

A review of the main organisations concerned with improving aviation safety and their initiatives is presented, including recent accident statistics and conclusions about their role in information and data processing for flight safety. The operational flight cycle is analysed in terms of safety and how the safety of flight might be improved by utilising this cycle (particularly the aircraft's flight mode model).

Existing solutions and technological perspectives for avionic systems and their potential roles for safety enhancement are reviewed in Appendix 6, as are possible roles of operational data recording systems and up-to-date requirements and trends in flight data recording in Civil Aviation (CA), Business Aviation (BA), General Aviation (GA), and Military Aviation (MA). Future aircraft trends, existing and required parameters, flight data volume and complexity, exiting safety supportive devices and specifications with respect to the flight safety system and flight data processing software, are also addressed. Constraints such as user/human-factors (the weakest link in the safety chain) are discussed, as well as technology limits, legal issues, feasibility limits, safety maintenance and management.

When acronyms are used in the text they are set in capitals e.g., GA; these abbreviations are defined in Appendix 1. A glossary of terms is defined in Appendix 2.

Part 1: The Aviation Market and Safety Management

To understand how PASS can be applied in Aviation it is important that there is a clear foundation for analysis. This is achieved by using classification [7] as a tool to reveal the intrinsic essence, structure, similarities and relations. Classification is first applied to aviation as a whole and then the aviation market. Then safety in aviation is explored based on an analysis of the evident risk factors making it possible to determine the functions and features for a new safety system for aviation. This leads to the development of a systematic approach for improving operational safety.

2 Survey of the Aviation Application Domain

2.1 Classification of Aviation

"*A defining (principal) attribute is that attribute of a substance which distinguishes it from any other type of substance, and thus without which that substance could not be conceived.*" Descartes, (Principles, part one, §53, I, 210-1)

There are at least three main reasons to classify aircraft for this research. The first reason is absence of proper definition for the term "general aviation" (GA) [68]. Classification here makes it possible to characterise the aviation domain, define limits and describe differences between various types of aircraft and so clarify terminology. Secondly, meaningful features and aspects of taxonomy provide a basis for the class of required features for system elements of active safety system. Thirdly, it provides a basis for unifying individual solutions for various types of aircraft. In practice it is desirable to separate the main and specific parts. The main part is common to all Active Safety systems whilst the specific part provides for adaption for particular aircraft types.

The classification of aircraft has generally been based on four aspects:

1. particular mission, based on its purpose (aviation sector)
2. type of aircraft (aircraft operation)
3. technical characteristics
4. state of development of aircraft

In the past a classification by type of propulsion has been used, however for our purposes this can be considered a 'consumer property' such as the type of a wing, the shape of a wing, the type of a landing gear and so forth. Another classification might be airworthiness, but this is just a measure of the quality, safety and readiness of the all aspects of the plane for flight; it is really a property.

Classification has also been used by international and regional aviation organisations to define various sets of standards and rules. In the following sections the standards are related to the classifications outlined above.

2.1.1 Classification of Aircraft by Mission

A classification of aircraft by mission is shown in Figure 2.1 below. According to the generally accepted standards (e.g. FAR, JAR) and the general approach of the main aviation authorities (ICAO, FAA, EUROCAE etc.), aircraft for a particular mission can be subdivided into two main groups: military and civil. In some cases a particular aircraft will be dual-purpose, used for both military and civil purposes.

The particular mission (use) of an aircraft affects safety, and, thus, requires general and specific safety maintenance procedures. Although little data is available from military sources we assume that safety standards for crews of military aircraft are similar to those established by internal standards of the countries in which they operate. The astronomical cost of modern military aircraft tends to ensure that their design and maintenance is made as safe as possible. Military aircraft are typically equipped with 'Systems of Objective Checking' (SOC) and various kinds of onboard devices for collecting and storing flight data. These are primarily intended to ease problem solving in crew combat training e.g. for analysis of performance and evaluation of each mission. When accidents or incidents occur then independent experts have access to the data stored during flight and investigate the cause(s).

For aviation involving passengers and freight classification is subdivided between CA and GA. A commercial aircraft is defined as "any aircraft carrying more than 30 passengers or a minimum actual load of 7500 pounds (or more), transporting passengers and/or freight for payment" [10]. Such aircraft are regulated by the ICAO and used to provide air transport services. Although the term "general-purpose aviation" is widely used it is in fact quite poorly defined and in order to focus the research the term GA needs to be more clearly defined. For example, the Federal Aviation Administration's (FAA) definition of the term embraces a very broad range of aircraft, including many which are not relevant for this research. The Association of GA Manufacturers (GAMA) [11] uses a similar catchall definition: "GA constitutes all aviation, except commercial and military". Though this definition is similar to the FAA's, GAMA does not even define the scope of CA. The Aircraft Owners and Pilots Association (AOPA) uses its own classification of aircraft, this includes short haul airlines. Nevertheless, this exclusion is too strict, as it would exclude air-taxis from the scope of our research. Often operators of air-taxis work without registration and also helicopters, not intended for hiring, can also be considered to be part of the GA market.

GA includes a wide variety of uses for private, corporate, state and local administrative bodies such as the Police and Fire Service services. Many kinds of aviation fall into more than one classification, for example some military aircraft are used to carry passengers, or as an air-taxis for politicians, prisoners and diplomats.

2.1.2 Classification by Type of Aircraft or Method of Operation

The type of an aircraft is defined by its construction and method of operation e.g. glider, or balloon. Classification by type is illustrated in Figure 2.2, it generally does not contradict with existing conventions however it has some distinctive features.

The type is based only on basic flight characteristics without specifics of construction features, for example, the propulsion unit. It has four levels of refinement:

1. Means of creating lift: generally this feature can be divided into two classes: lighter-than-air and heavier-than-air.
2. Presence of the wing: heavier-than-air aircraft can be subdivided into winged and wingless.
3. Wing mobility: this feature can be used to create two alternate categories - with fixed wing and with movable wing.
4. Wing construction: main constructional aspects are wing rigidity (soft, semi rigid, rigid) and kind of wing movement (spinning, alternating motion).

The lack of a systematic classification scheme in the FAA definitions is notable. Other approaches used to classify aircraft by type depend on the aims of the classification. For example the US Air Force uses simple codes for various aircraft types: G for Glider; H for Helicopter; V for Vertical takeoff plane; Z for Balloon or Zeppelin.

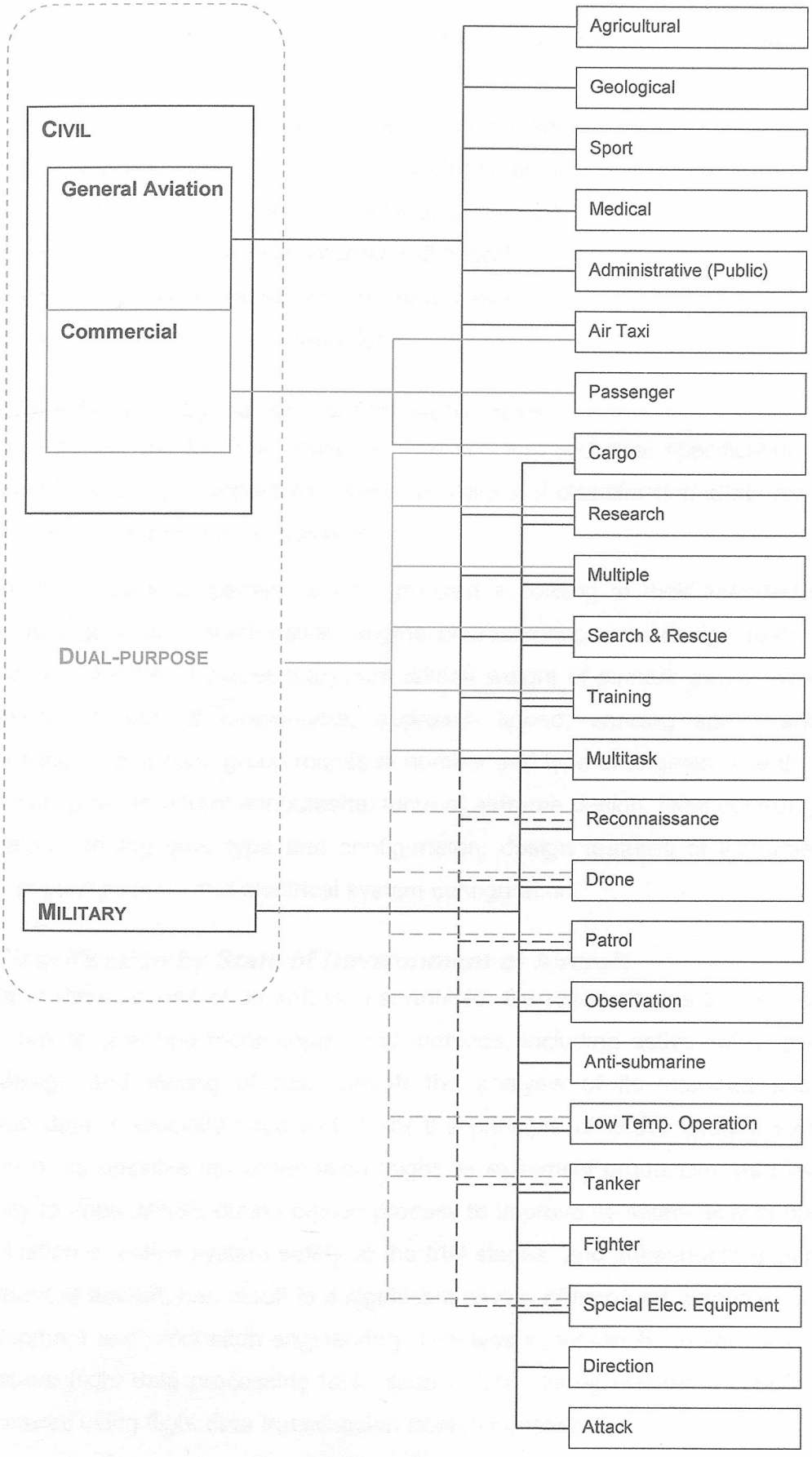


Figure 2.1: Classification of Aircraft by Primary Mission

It is generally assumed that aircraft with a rigid immobile wing are aircraft, but there are also other possibilities that our classification accommodates such as:

1. Means of creating lift: generally this feature can be divided into two classes: lighter-than-air and heavier-than-air.
2. Flexible wings(s) such as para planes or monoplanes
3. Semi rigid wings such as kites or delta winged planes
4. Rotor based planes (without motors e.g. Gyrodyne)
5. Flap winged planes, a helicopter/aircraft hybrid
6. Backpack wingless planes, e.g. rocket propelled
7. Other micro-lite based configurations

2.1.3 Classification by Technical Characteristics

Aircraft can be defined by their consumer features and technical specifications, this is illustrated in Figure 2.3. It separates alternative values of classification attributes and the elements of the indicated aircraft systems.

Selection of particular properties can be grouped according to their intended use, for example their general characteristics, engine characteristics and design features. The first group of properties includes maximum takeoff weight of aircraft; overall dimensions (wing span); number of passengers; approach speed; cruising speed and other characteristics. The second group relates to number and type of engines. The third group refers to distinctive structural attributes/features of airframe design, flight control type and configuration; landing gear type and configuration; design features of instrumentation; fuel system configuration and electrical system configuration.

2.1.4 Classification by State of Development of Aircraft

The state of development of aircraft is important for the research due to a possibility of using of new engineering technologies and methods, including active safety principles. During design and testing of new aircraft the analysis of its intended and actual operational data is crucially important. Here the principle of active system safety and evaluation of its possible implementation might be extremely productive, as there is an opportunity to apply MASS during design process to improve its safety later in operation. The application of active system safety at the trial stages, and subsequent experimental improvement of aircraft, can result in a significant saving of time and resources allocated for development and production engineering. This was successfully proven by Concorde project where flight data processing took place before, during and after flight in special ground centres using flight data transmission from the aircraft.

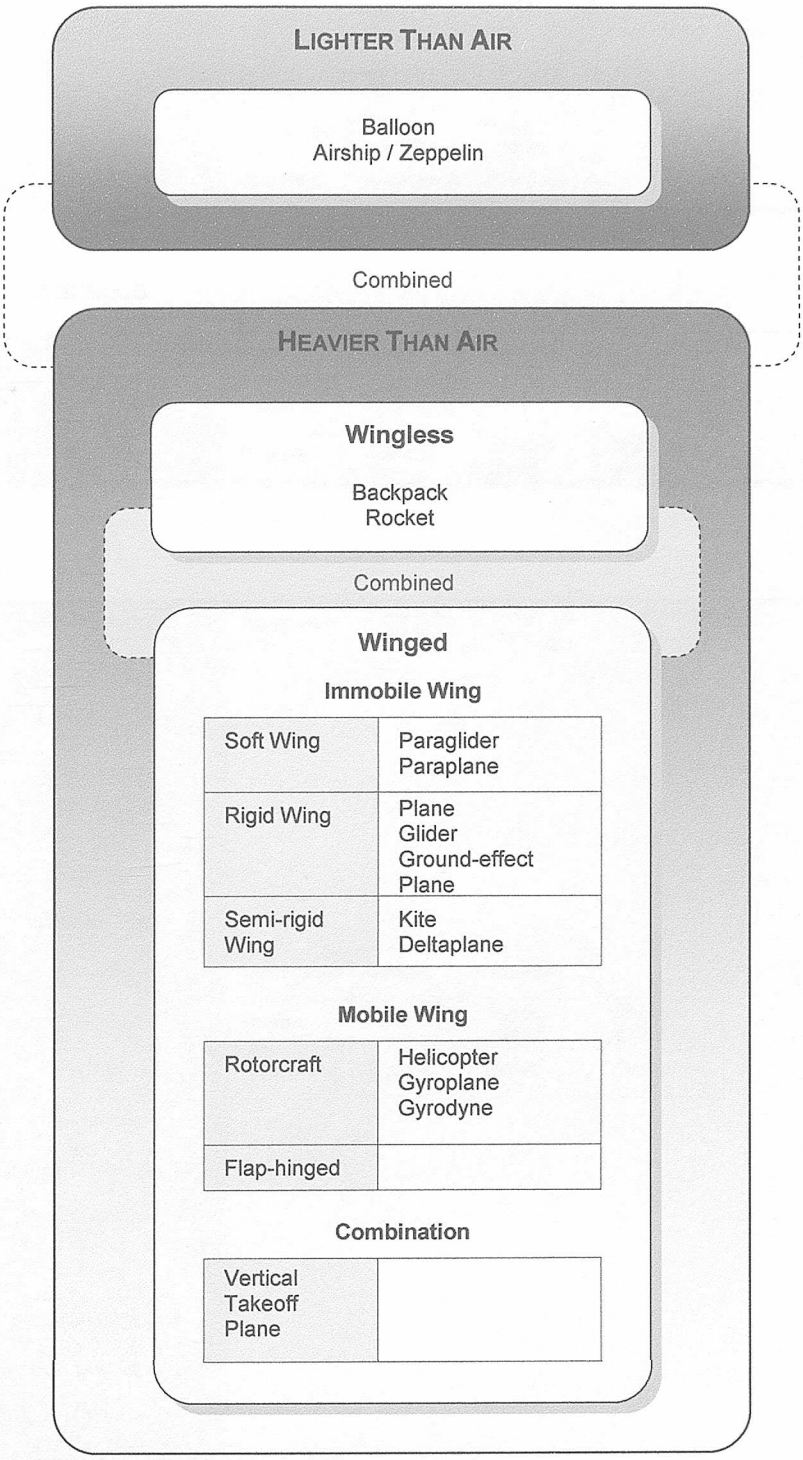


Figure 2.2: Aircraft Classification by Type

The safety of every flight of every Concorde [13] aircraft was monitored and managed by specially dedicated and trained personnel. The problem with this scheme for safety management is that it is so 'people intensive'. The cost of this real time safety management proved prohibitive and reliance on using expert people was its weakest link. If Concord had been commercially successful then the system would have become overloaded and unsustainable.

Common Characteristics

Flight Weight (Take-off)	Super-light	Light	Middle	Large		
Approach Speed (Knots)	< 91	B. 91 - 121	121 - 141	141 - 166	166+	
Aircraft Wingspan (Ft)	< 49 (15 m)	49 - 79 (15 - 24m)	79 – 118 (24 – 36m)	118 – 171 (36 - 52m)	171 – 214 (52 - 65m)	214+ (65+ m)
Number of Seats	Unmanned	Single-seated	Multi-seated			
Cruising (Air) Speed	Subsonic	Supersonic	Transonic			

Power Plant Characteristics

Number of Engines	None	Single	Double / Multiple	
Type of Engine	Piston	Turbo-prop	Rocket	
Type of Propellers	Coaxial	Reblade	Straight Blade	Multi (N) blade

Design Features

Landing Gear Type and Configuration	**Configuration**	No wheels	2-wheeled (Bicycle)	3-wheeled (Bicycle)	Multi-wheeled (Polycycle)
	Gear Type				
Flight Control Type and Configuration	**Rudder Type**				
	Aileron Type				
	Trim Type				
	Flap Type				
	Elevator Type				
Airframe Design	**Scheme**	Monocoque	Classic	Canard	
	Fuselage	Narrow	Wide	Single-aisled	Double-aisled
	Wings	Monoplane	Biplane	Strait	Delta
	Empennage				
CIS Design	**Cockpit Instruments**				
	Alternator				
	Antennas				
	Pilot Static System				
	Other Onboard Systems				
Fuel System Configuration					
Electrical System Configuration					

Figure 2.3: Aircraft Classification based on Technical Specifications

2.1.5 Conclusions on Classification of Aviation

The classifications presented here are not claimed in any way to be 'perfect', this would be impossible as classifications need to adapt to reflect what is important at the time. The intention has been to focus on a classification which is useful for the research. It highlights the key features of aircraft which are most likely to provide a basis for the

PASS analysis. This will now be further refined with the aim of identifying a basis for improving safety of aircraft operation

2.2 The Aircraft Market

In order to identify a Method of Active System Safety it is important identify where it might be applied most effectively. This section analyses the features and size of the segments of the existing aircraft market including military, commercial and general aviation. The possibility applying PASS in the short to medium term in the GA market segment is analysed in greater detail.

2.2.1 Military Aviation

During the last 20 years the volume of fighter aircraft purchased has declined and according to analysts, a drop in demand is expected from 2010 onwards despite of some stabilization in deliveries of military aircraft in 2002-2004, see Figure 2.4. The main reasons for this are probably strategic military, commercial and technological. The 1950-1990 Cold War is over and the style of modern warfare has changed. There are new forms of air operations based on satellite guided drones and Cruise Missiles (as used in Yugoslavia, Iraq and Afghanistan) and the trend of Air Forces adopting modern multi-purpose aircraft is based on economic necessity. So, for example, there is less need for intercept fighters. There are several commercial factors including the rapidly increasing cost of design and manufacture of new aircraft, increased aircraft service life to avoid replacement costs and increased use of short term leasing of aircraft. Obsolescence caused by rapid technological change in airframes, propulsion, avionics and weaponry also takes its toll.

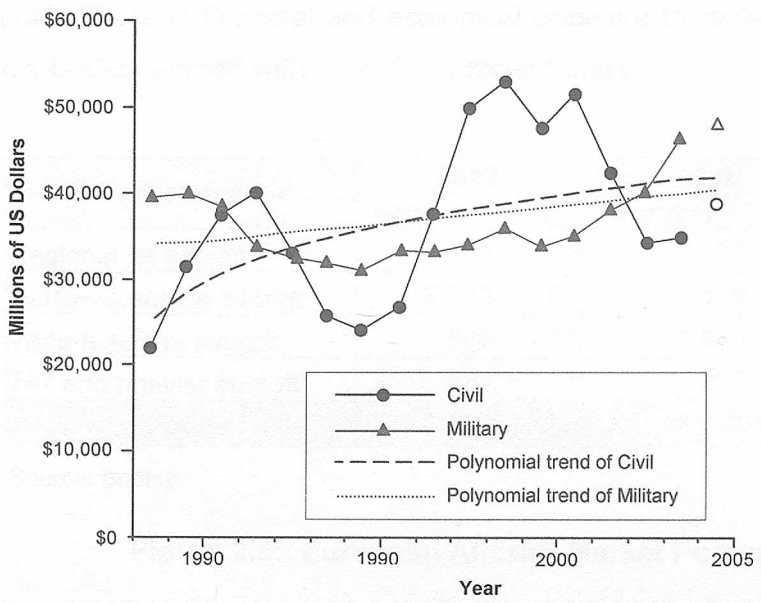


Figure 2.4: Sales of Civil and Military Aircraft

2.2.2 *Commercial Aviation*

Commercial Aviation (CA) is the largest sector of aviation with service and operation in over 200 countries. At the end of 2004 the CA network included 800+ airlines, 5,000 operators, 1,350 large and 10,000 small airports, 16,000 aircraft, 150,000 air pilots and 240,000 maintenance staff. According to long-term forecasts, the global CA capacity has a tendency for significant growth over the next 20 years however concerns about global warming may moderate actual growth after 2010.

It is characterised by long-distance and short distance aircraft, narrow and wide body aircraft mainly European or US designed and manufactured in Europe, US, Russia, and China. The current European fleet is about 3,900 aircraft. 67% of the fleet are narrow-fuselage aircraft and by 2025 the number of such aircraft will be almost doubled. European airlines will need almost 6,200 new jet aircraft at a total cost of $480 billion of which 75% will be narrow-fuselage and used regionally, many on 'low cost' airlines. The other 1,562 aircraft will be wide-fuselage ones with an estimated cost about $206 billion. Aircraft such as the Boeing 747 and Airbus A380 and heavier will support the market for long distance routes, about 200 aircraft of this class will be required. The majority of aviation companies in Europe will also require medium sized wide-fuselage aircraft. As competition in international markets intensifies smaller aircraft with lower operating costs will allow airlines to introduce new routes, create new markets with reduced commercial risk. Medium sized wide-fuselage aircraft are needed by European airlines to decrease their operating and maintenance costs and to create new international non-stop routes.

The forecast for CA development for European aviation manufacturers is positive, by 2022 Airbus expects a threefold growth of passenger traffic. Assuming a mean annual increment of passenger traffic of 5.3% in two decades it will require 16,600 new 100-seated aircraft. There is financial and ecological pressure to replace the existing fleet of 9,200 narrow-bodied aircraft with more fuel efficient ones.

European market	2002		2022	
	Number	%	Number	%
Regional jet aircraft	468	12	979	13
Narrow-fuselage aircraft	2,613	67	5,608	63
Wide-fuselage aircraft	585	15	1,869	21
747 and heavier aircraft	234	6	267	3
Total	**3,900**	**100**	**8,900**	**100**

Source: Boeing

Figure 2.5: European Aircraft Market Forecast

In support of the EU forecast Boeing forecasts that the largest part of deliveries will be narrow-fuselage aircraft, up to 13,650 units. The share of lighter regional jet aircraft will increase by 4,300 units. Regional airlines in the USA maintain lighter jet aircraft for new

non-stop trips. Airlines will use narrow-fuselage aircraft together with regional jet aircraft to increase the frequency of internal and short international trips gradually replacing turbo prop aircraft.

Class of aircraft	Number	% of total number	% total cost
Regional jet aircraft	4,374	18	5
Narrow-fuselage aircraft	13,608	56	39
Wide-fuselage aircraft	5,346	22	45
747 and heavier	972	4	11
Total	**24,300**	**100**	**100**

Figure 2.6: Market Demand for New Aircraft

Additionally airlines will increase their fleets of wide-fuselage aircraft (5,340 units), 45% of all such investments will go to medium wide-fuselage aircraft. They will be used in long-distance transportation markets, for example Atlantic and Pacific, and also on intense short-distance routes, for example, in Asia. Such aircraft as B747 and A380 will make up only 4% of all deliveries during 2003-2022, and their number will not exceed 900 units. An estimation of CA market expansion is $1.9 billion, and narrow and wide-fuselage aircraft make up about 85% of this figure.

Market expansion in the next 20 years will add approximately 3,000 aircraft to the freight aircraft fleet of which 75% will be converted from passenger aircraft. The cost of all newly delivered freight aircraft is evaluated at $132 billion at current rates. There is an opportunity here to use active system safety for this segment of CA as freight aircraft are not the best serviced and maintained. In the CA sector safety management schemes often conflict with operating companies profits, for example the minimisation of turn-around times used for freight and passenger flights.

Clearly there are global opportunities for introducing MASS based technology into the CA market to reach the global market for safety solutions, devices and systems.

Class of aircraft	2002		2022	
	Number	%	Number	%
Light (< 30 t)	578	33	1,330	38
Middle narrow-fuselage (30 – 50 t)	192	11	735	21
Middle wide-fuselage (40 – 65 t)	490	28	630	18
Heavy (> 65 t)	490	28	805	23
Total	**1,750**	**100**	**3,500**	**100**

Figure 2.7: Aircraft Cargo Fleet Analysis

2.2.3 General Aviation

General Aviation (or GA) is one of the most important parts of the global aviation market. In fact, in the U.S. alone, GA flight hours accounts for over 60% of all flight operations. The range of aircraft used goes from small propeller-driven aircraft to jet aircraft that perform non-scheduled commercial flights, corporate flights, and private aviation. European GA sometimes is considered as a part of CA except for air carrier operations. GA has a wide range of uses, for example:

1. Pilot training
2. Passenger Traffic including corporate, business and leisure travel
3. Law enforcement, , highway traffic management, search and rescue
4. Forest fire fighting
5. Air ambulance
6. Surveying, mapping, observation, photography and logging
7. Agriculture, fish and wildlife monitoring
8. Smuggling of people, drugs, munitions etc
9. Covert Operations (more recently)
10. Accident rates of GA operations are consistently higher for the following reasons:
11. Less regulation

GA pilots are involved in a wide range of operations and there is a wide variation in pilot qualifications and experience levels. Pilot certification ranges from student pilot to full Airline Pilot (ATP) with similar variability in flight hours, whereas all CA flights are crewed by at least one ATP. GA aircraft owners and pilots are individually responsible for the safety of flight whereas in CA and MA specially trained personnel to perform maintenance and safety duties.

Less Resources

GA aircraft have fewer cockpit resources and warning systems. Airports and landing fields for GA are of lower quality than for CA e.g. runways, approach lighting systems, and advanced services of airline centred airports. GA operations are predominantly single pilot whereas CA requires at least two pilots. There are far facilities, nearly 14,000 airports in the US alone, many of which are just landing strips.

Greater Risks

Many operations of GA, such as crop spraying, fire fighting, and banner towing, have special mission-related risks. There are more takeoffs and landings, the highest risk phases of any flight. The flights are shorter and as the number of flights increases the cumulative risk grows.

Effects of Weather

GA aircraft are more weather dependent, they usually fly through the weather instead of avoiding it, and may not have systems to detect, avoid or cope with adverse conditions. There is more discretion and flexibility in GA regarding decisions about exactly when to fly, for example recreational pilots often choose not to fly in poor weather conditions. Even though GA operations are different from scheduled air carrier operations, GA pilots who actively manage risk can significantly improve their safety.

2.2.3.1 Distribution of General Aviation

As mentioned above, the definition of GA varies in different countries. Those conducting GA surveys often experience difficulties in accumulating valid data. Some countries do not have an up-to-date register of their GA aircraft; others do not even have a designated authority for maintaining such records. As a result, the figures provided are inevitably approximations or estimates.

The available data [12] data confirms that the USA has the biggest GA market share, about 67% of the global GA fleet. The only other significant market shares are those corresponding to Canada, Germany, Australia, Brazil and the UK, see Figure 2.8 .

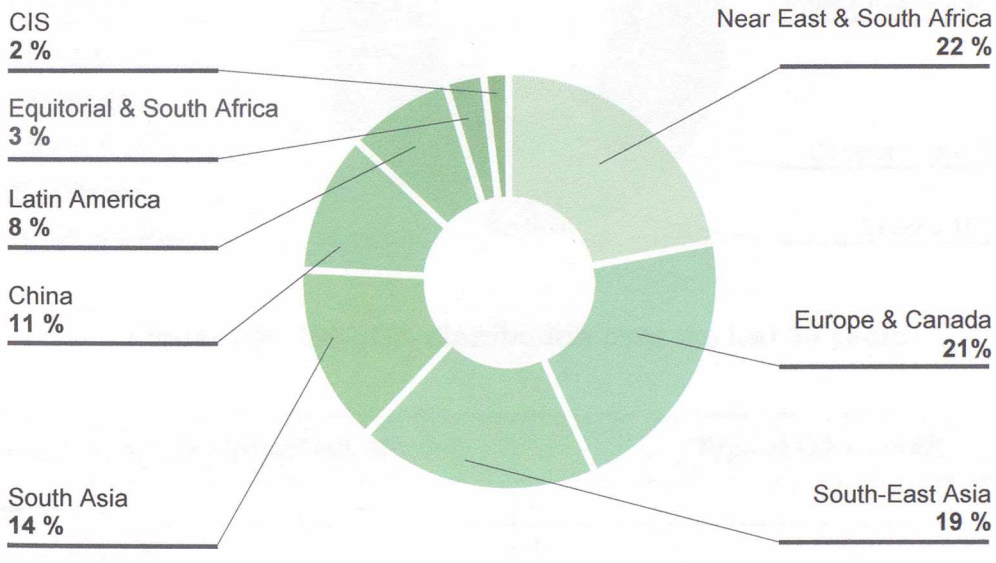


Figure 2.8: Global GA distribution (Source: FAA, 2004)

Research into GA figures has revealed that although extensive data is available for the U.S., limited data is available for Europe where GA regulation is still 'country' based. Recent FAA studies show steady growth of US GA in numbers as the result of new aircraft. Obsolescence and write-offs of aircraft provide a counter balance. Annual grow in GA is expected 1.2% over the 13-year forecast period, from 211,000 in 2002 to about 246,000 in 2015. This growth includes the addition of a new aircraft category – the light sport aircraft - from 2004 and they will account for 20,915 aircraft by 2015. This category is an ideal application for PASS, both during their design and operation.

2.2.3.2 Features of General Aviation Aircraft

General Aviation aircraft have the widest variety of applications (see Figure 2.3) due to low operational costs (better scalability with respect to Civil Aviation), shorter take-off and landing distances, flexibility in terms of operational altitude and regulations and easier access to GA airports, local airfields. A further important aspect with respect to GA is age of the aircraft. Although sales of new general aviation aircraft increased after the mid-90s, *most general aviation aircraft in use in 2000 in the US were more than 25 years old.* Amongst all GA aircraft categories, the single-engine piston aircraft category currently has the highest average age of all and accounts for the largest percentage of the GA fleet in the US. The oldest aircraft is single-engine piston aircraft with 8+ seats, this type of aircraft has the average age about 43 years. A report compiled by NASA in 1999 defined some further typical features of US GA aircraft. These features are summarised in Figures 2.11 and 2.12:

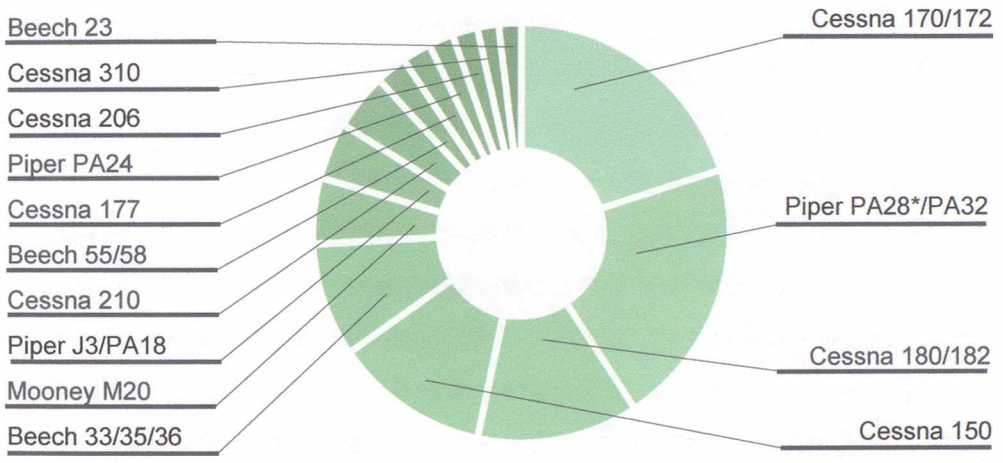


Figure 2.9: USA GA distribution over the last 30 years

Characteristics of Typical GA Aircraft	Typical GA Aircraft
Number of seats	4
Number of engines	1
Type of engine	Horizontally opposed, 4 or 6 cylinder piston
Landing Gear Type and Configuration	Fixed Tricycle
Airframe Construction	Aluminium frame, Aluminium skin, steel engine mount
Flight Control Type and Configuration	Mainly cable operated utilizing bell cranks and push-pull rods

Figure 2.10: Typical GA aircraft

Power Plant	CIS*	Aircraft Control	Airframe	Electrical System
Engine System	Cockpit Instruments	Flight Control	Empennage	Lighting System
Fuel System	Vacuum System	Rudder System	Fuselage	Source & Dist.
Propeller System	Pilot Static System	Aileron System	Tail	
Heating/Ventilation	Alternator	Elevator System	Wings	
	Antennas	Trim System		
		Flap System		
		Ground Control		
		Landing Gear		

Figure 2.11: Typical GA aircraft system breakdown

2.2.4 Helicopters

Another segment of GA that has recently experienced a period of stable growth is helicopters. Sales and volume of production has grown considerably, increasing from $4 billion dollars in 1996 up to $6.7 billion in 2001 and $9.8 billion in 2006. Forecasts in 2001-2010 are for 9,503 helicopters with a total value of this production exceeding $75 billion whereas in 1991-2000 7,963 helicopters were produced with value $52,7 billion. Different segments of the helicopter market are growing at different rates. The market volume for new deliveries of civil helicopters has reached $1.2 billion in 2007. It is expected that in the period between 2001 and 2010, 819 civil helicopters with a value of $12.43 billion will be produced. The proportion of annual deliveries of civil helicopters is between 1/3 and 1/7 of the respective military helicopter market and demand for civil helicopters is stable.

Fuel prices have been the main factor in slowing the market but even so sales of private, corporate and support helicopters are booming, with growth increasing by 400% from 1995 to 2000. Now they are no longer considered to be prohibitively expensive business executives are buying or hiring helicopters. Presently corporate helicopters represent only about 2% of civil helicopters, the market leader being the Bell / Agusta BA609 helicopter with tilting rotors.

Not surprisingly the manufacturers have made serious investments in the development of new models for this segment of the market. The Sikorsky S-76 has been modified to produce a new version (S-76C+) which is priced at about $7 million. The Eurocopter Consortium has expressed a strong interest in the business helicopter market and is offering the EC 155 an improved version of the Dauphin helicopter.

2.2.5 Conclusions on the Aviation Market

A short overview of the market shows clearly that the numbers for aircraft in service worldwide will grow further leading to increasing challenges for Air Traffic Control and

aviation safety. The trend to more intensive use of aircraft puts pressure on safety management schemes; most of them affect the main interest of the aviation companies: i.e., profit. For example narrow bodied aircraft will be used for longer flights without any possibility to check their condition and detect potential safety treats in between flights. A typical flight 'turnaround' time for a budget airline is down from about 60 minutes to only 20! As Boeing proudly declare:

"*our aircraft only make money when they are flying*"

Wide body aircraft will be used in two ways: for shorter flights in a similar way to narrow bodied planes with intensive use and frequent taking off and landing – the most risky phases of flight – and for long haul flights which relentlessly stress the engines and airframe.

For different reasons GA aircraft and helicopters are exposed to a wider variety of risks and so are a particular concern for safety management. The wider use of GA with less qualified pilots and insufficient maintenance is accumulating serious safety problems.

Taking all of this into account it is clear that the aviation market is suffering from pressure in two conflicting directions:

1. *an increase in the volume of flight operations* in CA and GA exposing an increasing number of passengers to operational risk and
2. *an increasing level of safety risk due to faster turnaround* of CA flights and poor maintenance facilities for GA aircraft

It is clear from this analysis that there is a need for PASS based systems which can automatically monitor and improve safety in the CA and GA markets. The case in the MA market is less clear, its value is higher but implementation more fragmented and difficult.

3 Aviation Safety and Risk of Flight

This chapter various flight risks and their statistics are reviewed and the types of risks that exist in flight operations are highlighted. A summary of current aviation safety is presented with special attention on GA safety. The objective is to get an appreciation of the aviation safety risk profile so that it becomes possible to propose how PASS might be used to reduce operational flight risk as effectively as possible.

3.1 Safety in Commercial Aviation

Safety in Commercial Aviation has been improving for the last 40 years. The number of accidents has been reduced to nearly 1 per 5 per million departures, see Figure 3.1 [25].

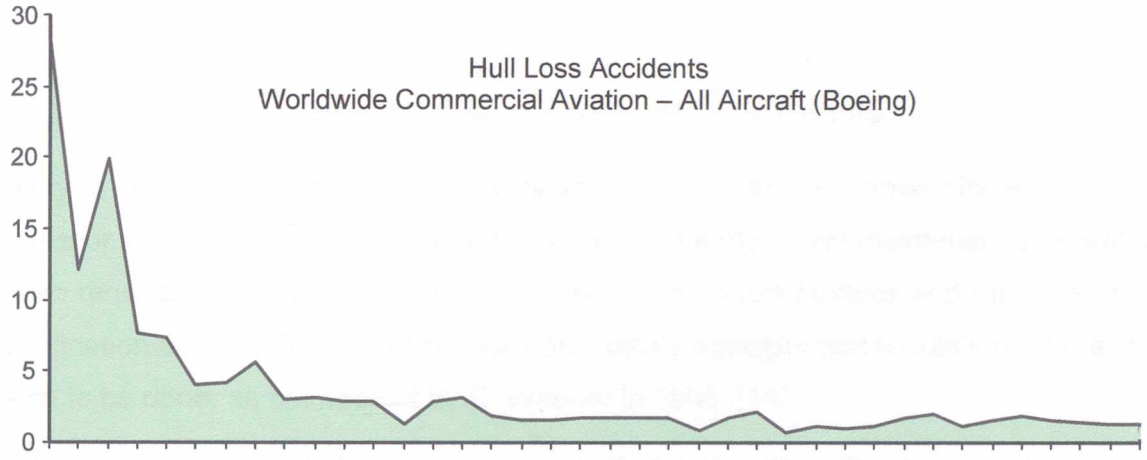


Figure 3.1: Global CA loss statistics per million departures, 1960 to 2000

It might be expected that new aircraft should be safer, and that as their share of the whole fleet grows the safety of aviation should naturally improve. However, this is not evident. The trends in aviation safety management are rather similar across all sectors and unfortunately not effective: in operation new aircraft are only as safe as the old ones. The factors that influence risk and its profile are almost identical for aviation at large and are highly influenced by personnel related factors (operator, flight crew, ATC, maintenance), equipment related factors (Airport, Aircraft) and environmental factors such as the weather, see Figure 3.2.

Various organisation and bodies share responsibility for safety in aviation. The aircraft manufacturers' responsibility is to design safer aircraft by developing and using safety-enhancing technologies and documentation. The aircraft operators' responsibility is for safe operational use and maintenance by providing professional quality piloting, flight management and maintenance support. Their common responsibility is safety related analysis and unconditional support of safety driven initiatives.

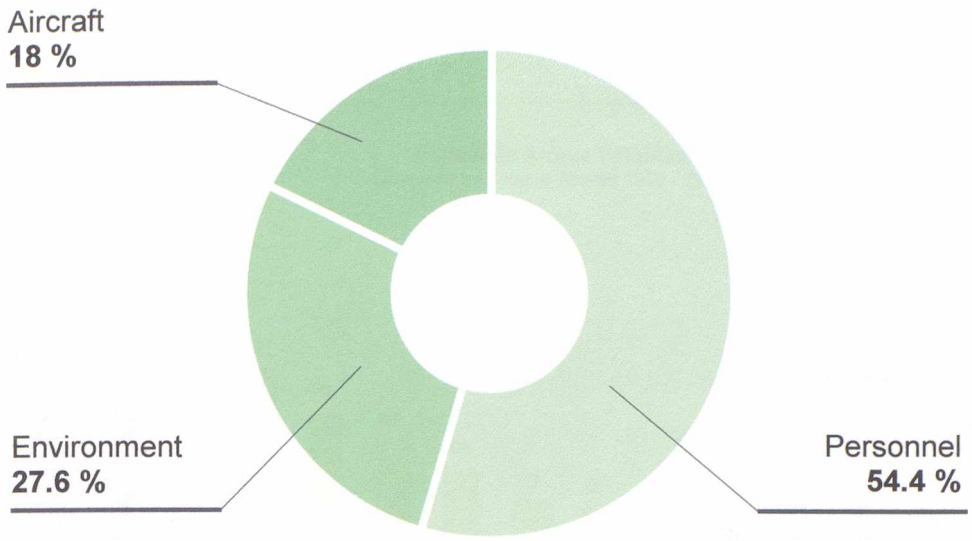


Figure 3.2: Main causes of CA accidents

Safety is only taken seriously if government bodies and ATC have efficient rules and regulations in place along with modern navigation facilities and maintenance operations. It also requires the inspection and modernisation of airport facilities and the international coordination of air traffic control services and safety management regulation. There is still much to be done, as pointed out by E. Weener in 1998 [14].

So far there is no generally accepted model of aircraft safety. By analysing the accident and incident data and applying judgment about future trends it becomes possible to determine which actions could be effective. It is also evident that the current practice of basing safety management schemes solely on sporadic after flight analysis is doomed to failure, due to current trends and commercial pressures already mentioned.

3.2 Main Risk Agents and Their Contribution

A review of the published statistics [15], [16], [17], [18], [19], [20] shows the main safety risks were Loss of Control in Flight (LCIF), Control Flight in Terrain (CFIT), Sabotage, Mechanical Malfunctions etc, see Figure 3.3. The available data is not exact, for example 618 fatalities had no clear cause. Many aviation accidents in the past have been attributable to the malfunction of aircraft hardware, e.g. sensors, pipes, engines, aircraft body, etc. In some cases this has been the result of unexpected faults. In most cases, though the root cause is attributable to human factors in about 52% of all accidents [14] and more specifically the absence of maintenance actions or the inappropriate maintenance.

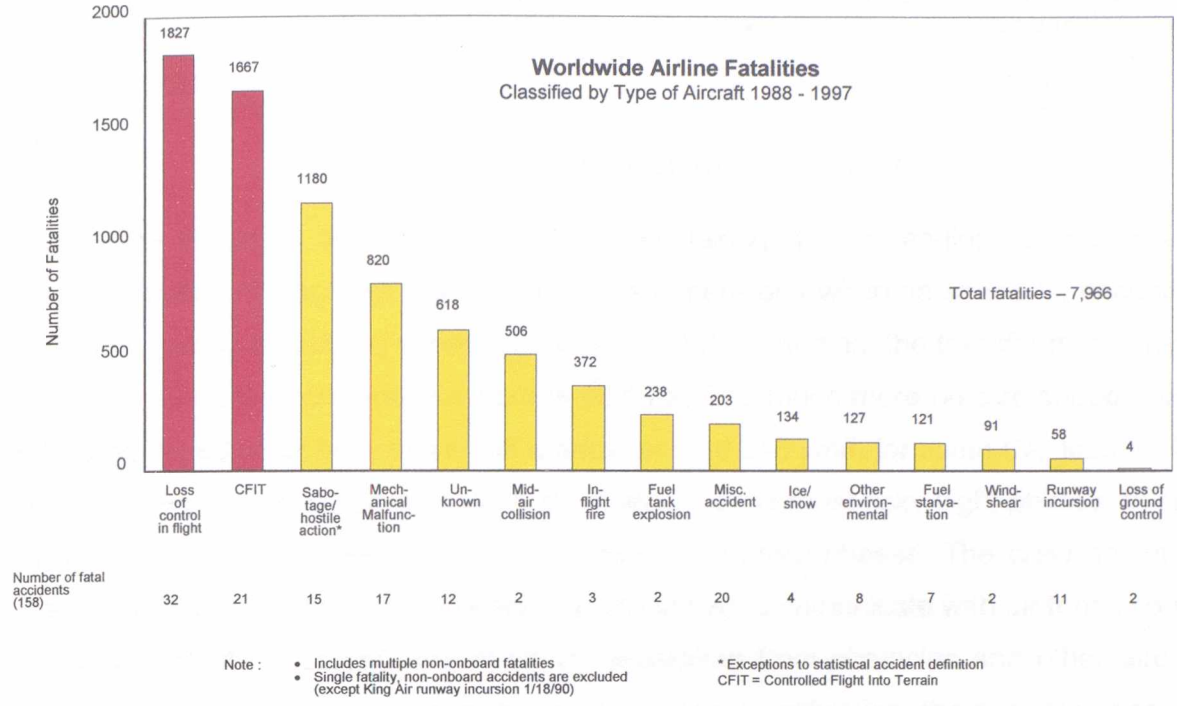


Figure 3.3: Boeing statistics of world accident fatalities

A simplistic model a flight could be split into five phases: taxi-out, takeoff cruising, descent and taxi-in as illustrated in Figure 3.4 below:

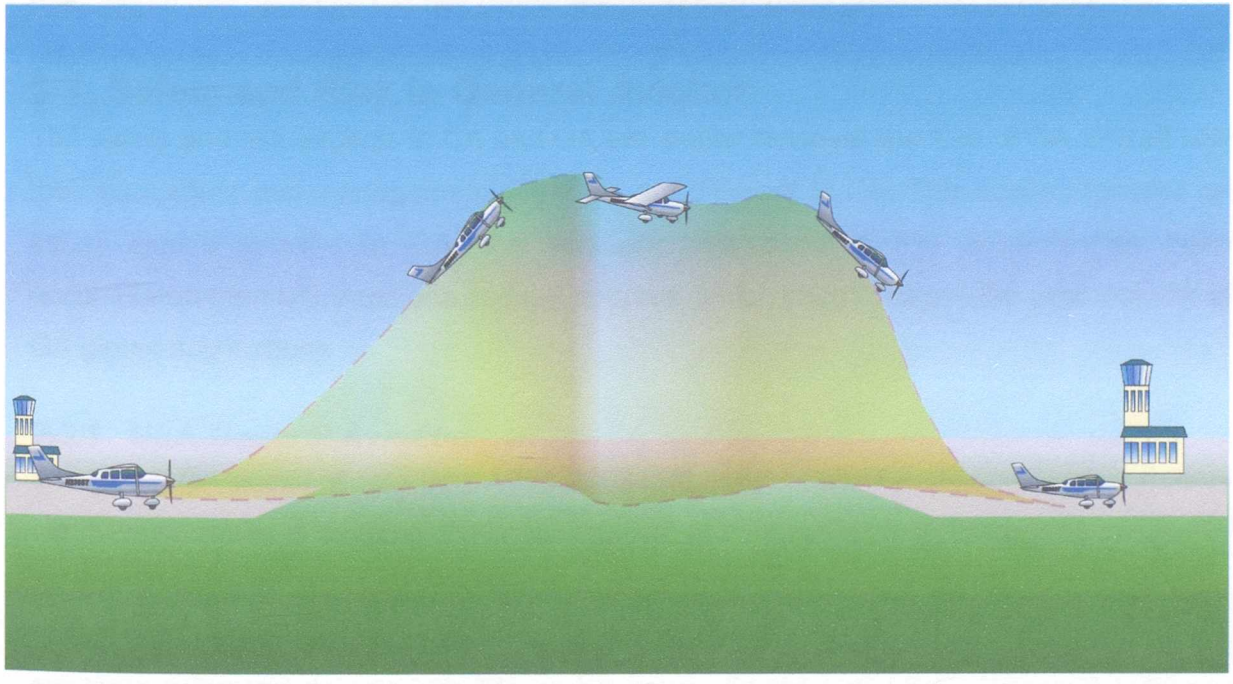


Figure 3.4: Simplistic Model of Operational Flight Phases

The risk of each phase of flight is illustrated by statistics below in Figures 3.6 and 3.9.

Taxi	Takeoff	Climb	Cruise	Descent	Manoeuvre or Hover	Approach	Go Around	Landing
4.1%	19.6%	3.6%	14.9%	2.7%	14.8%	11.0%	2.0%	27.3%

Figure 3.5: Risk of each phase of flight

In practice the most risky phases of flight are taking-off and landing. During take-off aircraft movement transfers from two to three dimensions when its speed V_a exceeds a threshold (taking off speed) speed V_{to} : $V_a > V_{to}$. When landing, the transfer from three to two dimensions is even more dangerous as it requires much more precise speed control – landing speed must be within small window around 240 km/h for some CA, less for GA: $V_{lmin} < V_a < V_{lmax}$. The statistics confirm that these are the most risky flight phases, in spite of their relatively short duration in comparison with other phases. The crew are under maximum stress having to change altitude and speed, communicate with air traffic control (ATC) and/or other aircraft, and maintain separation from obstacles and other aircraft. Aircraft systems are also stressed due to higher engine utilisation, the possible operation of retractable landing gear, rubber and ailerons etc. Wind and weather conditions are also much more unpredictable and dangerous at the low altitude.

The phases related to landing have the largest percentage of total accidents i.e., landing (27.3%), manoeuvring (14.8%), approach (11%), and descent. The figures vary by aircraft type due to different durations in each phase, aircraft-specific hazards and the type of operational use. Even so the risk profile will be similar to the presented in Figure 3.5.

3.3 Safety and Risk in General Aviation

The safety and risk aspects in CA and GA are similar however the size of GA aircraft and their equipment and management schemes are different to CA. This section focuses on safety issues specific to GA, the accident data used in this analysis has been accumulated from US, Australia and UK sources, which encompasses the vast majority of GA global applications.

3.3.1 USA General Aviation

The NTSB GA accident data from 1996-2003 [15], [16] shows that GA with 1.36 accidents per 100,000 hours is certainly the "poor relative" in comparison with CA where number of accidents is 0.029 per 100,000 hours. It also shows that accidents caused by human factors dominate the statistics and no that substantial improvement in safety has been achieved in the last decade, see Figure 3.6 below. Of the 1,468 such accidents the most frequently cited causes were aircraft handling and control (65.6%), followed by planning and decision-making (41.1%) and use of aircraft equipment (12.2%). Issues related to

personnel qualification were cited in almost half of the 209 accidents. Examples of causal factors include lack of total experience, lack of experience, and inadequate training.

Year	Total Accidents	Fatal Accidents	Fatalities	Hours Flown	Accident Rate (per 100,000 flight hours)	Fatal Accident Rate (per 100,000 flight hours)
2003	1,732	351	626	25,800,000	6.71	1.36
2002	1,713	345	581	25,545,000	6.71	1.35
2001	1,726	325	562	25,431,000	6.79	1.28
2000	1,837	345	596	27,838,000	6.60	1.24
1999	1,905	340	619	29,246,000	6.51	1.16
1998	1,904	364	624	25,518,000	7.46	1.43
1997	1,845	350	631	25,591,000	7.21	1.37
1996	1,908	361	636	24,881,000	7.67	1.45

Figure 3.6: USA General Aviation Accident Statistics

The annual reviews of US GA accident data highlight that the fatal accident rate in the US for personal flying remained the highest of all GA categories with 1.61 fatal accidents per 100,000 hours flown (year 2000). This contrasts with a rate of 0.63 for instructional flights involving an experienced pilot as well as the student. Of all GA accidents 46.6% involved pilots with 1,000 hours or less total flight time and a higher percentage for pilots with less than 200 hours or less experience. The type of aircraft is also significant: of the 1,527 accidents recorded 82.4% involved pilots with 1,000 hours or less of time in the aircraft make and model involved in the accident. Night-time fatal accidents are more likely than daylight ones and accidents involving weather, disorientation, loss of control, and collisions result in higher levels of injury.

3.3.2 Australian General Aviation

Comprehensive statistics on GA accident and fatality rates were obtained from the Australian Transport Safety Bureau [22], summarised in Figures 3.7 and 3.8.

Accident rate (per 100,000 hours)	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000
GA Charter	8.26	9.09	11.10	11.47	8.96	7.03	10.07	8.24	4.13	5.33
GA Agricultural	22.69	31.24	24.50	18.41	28.10	26.28	24.83	23.73	17.83	18.03
GA Flying Training	6.54	5.85	8.13	6.32	8.25	5.77	8.35	4.96	7.04	9.59
GA Other Aerial Work	12.07	12.12	12.23	8.75	6.13	9.23	10.80	5.32	5.74	9.85
GA Private/Business	27.24	24.01	24.34	18.77	20.31	18.56	16.60	21.18	16.43	21.4
Total	**14.81**	**14.11**	**15.02**	**12.07**	**12.26**	**11.28**	**12.45**	**11.08**	**9.01**	**11.67**

Figure 3.7: Australian GA accidents 1991-2000

Fatal Accident Rate (per 100,000 hours)	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000
GA Charter	0.52	0.49	1.01	1.40	0.64	1.24	0.82	0.40	0.59	0.62
GA Agricultural	0.91	3.36	1.02	4.60	1.94	3.19	3.65	1.36	0.00	2.58
GA Flying Training	0.65	0.23	0.00	0.47	0.23	0.00	0.00	0.21	0.22	0.00
GA Other Aerial Work	0.34	0.38	1.05	1.30	1.29	1.37	0.32	0.63	0.31	0.73
GA Private/Business	2.78	3.89	2.91	1.96	2.71	2.01	1.57	3.72	3.70	2.17
Total	**1.20**	**1.51**	**1.29**	**1.47**	**1.25**	**1.28**	**0.92**	**1.22**	**1.13**	**1.00**

Figure 3.8: Australian GA fatalities 1991-2000

Clearly GA private, business and agricultural operations give rise to the highest rate of accidents and fatalities. The accident rate of GA in Australia is almost double that of GA in the States whereas the fatal accident rate is nearly the same (per 100,000 flight hours). This may be due to different use, traffic density and terrain in the two countries.

3.3.3 UK General Aviation

The Civil Aviation Authority investigates accidents in the UK and produces GA accident statistics. The types of accidents are ranked by their severity, 67.5% of them are either: control flight in terrain (CFIT), loss of control in Visual Meteorological Conditions (LOC VMC), Low flying/aerobatics (LOW/AERO) and Loss of Control in Instrument Meteorological Conditions (LOC IMC). The data for the period 1985-1994 is summarised in Figure 3.9.

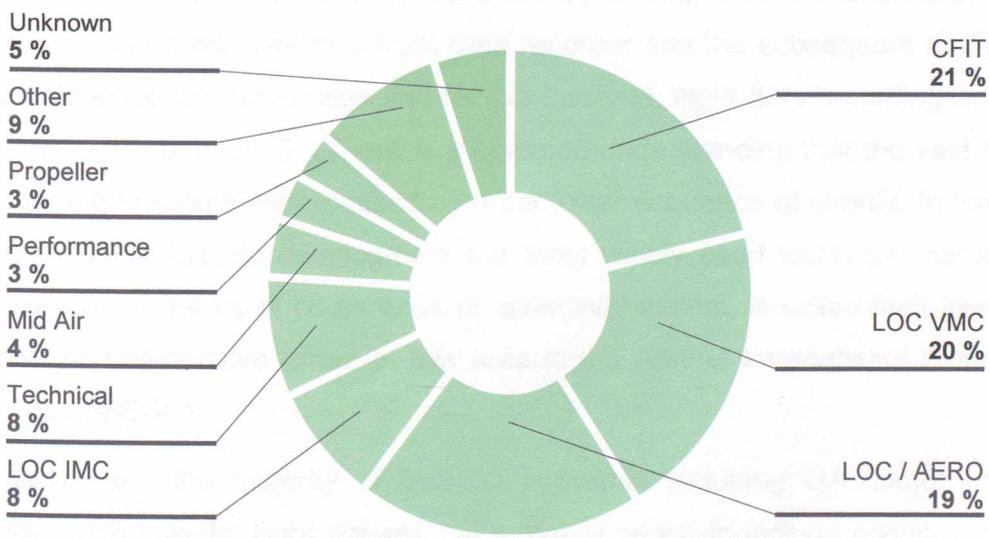


Figure 3.9: UK GA accident types 1985-1994

Loss of control was the predominant factor as this occurred in several of the types of accident, i.e., loss of control in Visual Meteorological Conditions, Instrument

Meteorological Conditions and in aerobatics/low flying accidents. Illegal use of aircraft accounted for 21% of fatal accidents. In many cases pilots were knowingly breaking the law indicating that education and security are likely to be more effective than further legislation or stricter enforcement. Another major factor is poor clarity and availability of information which is poorly distributed to GA Pilots. The third major cause is Human Factors involving either the pilot or maintenance actions between flights.

In summary accident statistics UK 1994-1996 [23], [24] and similar CAA/NTSB data and show that the vast majority of GA accidents occurred during the landing phase ~53% while the most fatal accidents (64%) were related to the initial climb and cruise phases.

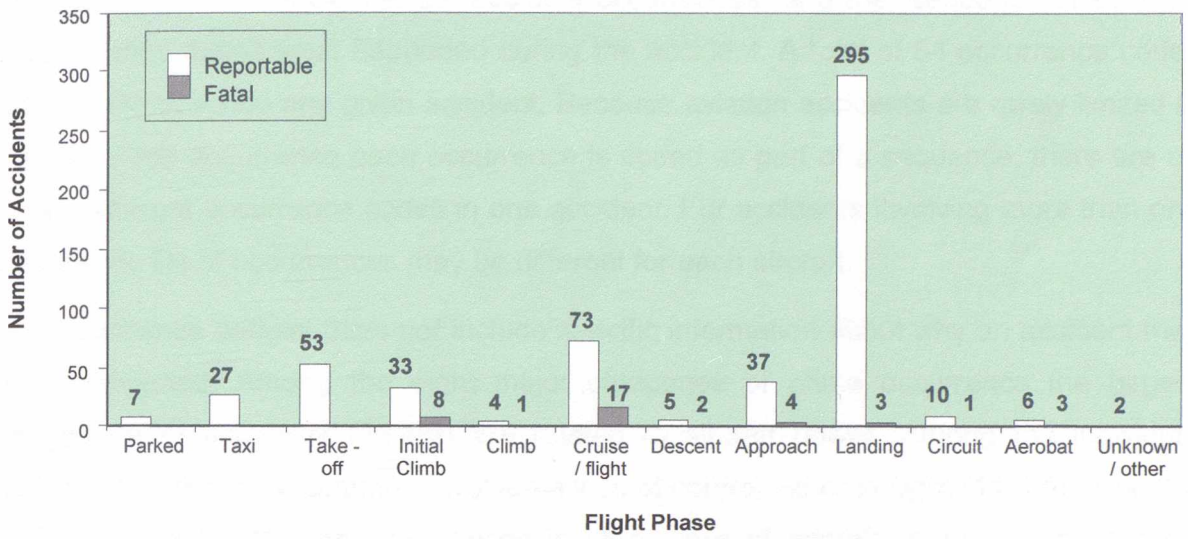


Figure 3.10: UK GA fatal accidents per flight phase 1994-1996

3.4 Flight Risk Analysis

Accident investigators and safety researchers try to determine the causes of accidents. Often this relies on retrieval of a flight data recorder and the subsequent analysis of the data to help establish the causes and factors involved; flight data recording and analysis are reviewed in Appendix 6. There is a common understanding that the vast majority of accidents and incidents were caused by a particular sequence of events. In the literature and conventional system development the most widely used technique for analysis of consequences, in terms of occurrence of 'defective' events, is called fault tree analysis. The most comprehensive forum in this area is the Annual International System Safety Conference (ISSSC).

As already seen the majority of aviation accidents including GA sector usually are associated with specific flight phases. So it makes sense to include possible *sequences of events* when looking for techniques for safety improvement within similar types of aircraft. Also the profile of risk occurrence makes it possible to concentrate on accidents/sequences of events of particular type. Studies by Boeing [25] of accidents of transport aircraft found that most accidents result from a sequence of events rather than a

single catastrophic event. Research identified as many as 20 events in a single flight that directly influenced the subsequent accident. NTSB [26] uses a similar method to break down each accident into "occurrences". Their objective is to try to prevent future accidents by learning from the past.

3.4.1 First Occurrences and Sequence of Events

An accident can also be viewed as a sequence of relevant causal events and the order in which they happened. The events might include a combination of multiple occurrences, with many possible combinations. The US NTSB year 2000 accident data [26] shows that out of 1,822 GA accidents there were 407 unique combinations of accident occurrences. The reports classify accidents as "accident occurrences" and the "sequence of events", together they define what happened during the accident. A total of 54 occurrence codes are used to describe any given accident. Because aviation accidents are rarely limited to a single (first) occurrence each occurrence is coded as part of a sequence, there are up to five different occurrence codes in one accident. For accidents involving more than one aircraft, the list of occurrences may be different for each aircraft.

The occurrence dataset does not include specific information about why an accident may have happened. Among the eight major categories of prime occurrence the largest percentage of accidents (26.4%) are related to aircraft power. Among the individual occurrences, the most common involved a loss of control either in flight (14.4%) or on the ground (12.3%). Although occurrences involving loss of aircraft control on the ground resulted in only 1 fatal accident in year 2000, loss-of-control occurrences in flight resulted in a total of 110 fatal accidents - nearly one-third of all fatal accidents and more than twice that of any other single occurrence. Figure 3.12 displays the percentage of accident aircraft in each phase of flight at the time of first occurrence. The phase of flight can be defined as when, during the operation of the aircraft, the first occurrence took place. The upper figures represent the percentage of all accidents that occurred in each phase, and the numbers in parentheses indicate the percentage of all accidents that were fatal. The landing phase has the largest percentage of total accident first occurrences (27.3%).

The largest percentage of fatal accident first occurrences (33.4%) occurred during the manoeuvring phase of flight, but only 14.8% of all accident first occurrences occurred during this phase. Accidents that occur during cruise and manoeuvring are more likely to result in higher levels of injury and aircraft damage due to the higher speeds and altitudes involved. The likelihood of an aircraft accident first occurrence during each phase of flight varies by aircraft type and type of operation. For example aircraft flying at very low altitudes e.g. while spraying, have an increased risk of collisions with terrain or obstructions. As a result, about 61% of all first occurrences that involved such flights occurred during the manoeuvring phase compared to less than 9% of personal/business

flights and 11% for instructional flights. Conventional approaches make use of the information to improve safety by means of improved procedures and training.

Standing / Taxi / Other	Takeoff	Climb	Cruise	Descent	Maneuver / Hover	Approach	Go-Around	Landing
4.1 %	19.6%	3.6%	14.9%	2.7%	14.8%	11.0%	2.0%	27.3%
(0.6%)	(15.6%)	(6.1%)	(22.3%)	(3.8%)	(33.4%)	(14.3%)	(1.0%)	(2.9%)

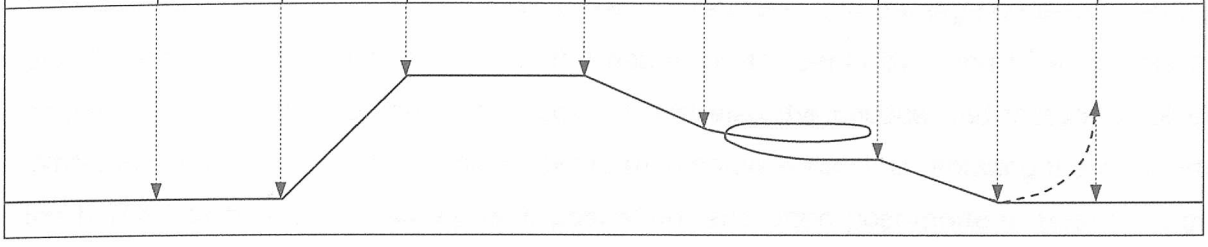


Figure 3.12: First Occurrence and Flight Phase Accident Statistics

3.4.2 Causes and Factors of Accidents

In addition to coding accident occurrences in the US, the NTSB indicates the probable cause based on a determination of why the accident happened. For each accident occurrence any information that helps explain why that event happened is identified as a "finding" and may be further designated as either a "cause" or "factor." The term "factor" is used to describe situations or circumstances that contributed to the accident cause. Just as accidents often include a series of events, the reason why those events led to an accident is a combination of multiple causes and factors. For example an accident sequence might begin with an explosion in the engine compartment of a single-engine aircraft due to a fuel leak. Consequently the aircraft engine might experience a complete mechanical failure and the pilot has to make a forced landing. In these circumstances the pilot may not be able to control the aircraft and so impact with trees during landing. The fuel leak and resulting explosion might be cited as causes in the findings of this accident. Smoke in the cabin, and the pilot's resulting reduced visibility, might also be cited as factors. An oil leak, oil exhaustion, engine bearing over-temperature, fractured connecting rod, and fractured crankcase were all also cited in the findings but were not assigned as causes or factors. The usual method used for such analysis Fault Tree Analysis [28] .To simplify the presentation of probable cause information broad cause/factor categories are used, there are three main groups: aircraft, environment, and personnel. Personnel-related causes or factors were cited in 89% of the 1,758 general aviation accident reports, by far the most significant group. Environmental causes/ factors were cited in 45% of accident reports, and aircraft related causes/factors were cited in 29%. Only 74 of 792 environmental citations (9.3% of all environmental causes/ factors) were listed. For example, rough terrain might be cited as a contributing factor, but not a cause, to explain why an aircraft was damaged during a forced landing due to engine failure. In that case, the origin(s) of the engine failure would be cited as "cause," but the terrain would be cited

as a factor because it contributed to the accident outcome. Weather conditions are the most frequent causes or factors in GA accidents; the three most significant being "crosswind," "gusts," and "tailwind".

3.4.3 Conclusion from Flight Risk Analysis

The review of accident statistics from the UK, USA and Europe show a strong correlation between safety and the phase of flight based on fatalities and damage caused to aircraft and the environment. The analysis of the nature of accidents by using FTA reveals the sequences of events leading to an accident and also the causes and factors involved. Whilst this analysis is useful in the longer term in some sense it is "shutting the door after the horse has bolted", the analysis is post-event and often post-mortem. Based on this situation, and the analysis data reviewed there is a necessity for a more pro-active approach to improved safety management and the safety of flight operations.

3.5 Safety Management Schemes

The process of safety management has two main aspects focused on the development of new regulations and administration of flight operations, e.g. promoting best existing practice, training of pilots, licensing of airports and assurance of airworthiness of aircraft. Aviation safety is becoming more and more complex. The safety management infra-structure in the USA is the best developed so far, this reflects its market domination over several decades. Its general organisation is illustrated in Figure 3.13 from [26].

When an accident occurs the NTSB makes an investigation and based on their findings the NTSB, FAA and NASA provide objective analysis and recommendations (so called 'blue lines') for the consideration of Engine Manufacturers, Airframe Manufacturers and Airlines. They then respond to the requests by proposing practical actions to avoid similar accidents in the future.

Recently Europe has centralised and improved its safety management by expanding the number of bodies and organisations involved in safety regulations and initiatives. In the *2002 European Parliament Directive on "Occurrence Reporting in Civil Aviation" has* established a aviation safety management regime similar to the US. The leading European organisation in air traffic management is Eurocontrol, which during 2002-2004 delegated most of its functions related to aviation safety to new organisations such as EASA and EUROCAE. All three bodies are funded by the EU and national regulatory authorities and work in collaboration with the main European transport regulatory and funding bodies such as DG TREN (www.tren.eu.int). In practice EU initiatives in aviation safety have mainly been concerned with the human factors e.g. training and inspections and sadly have failed to increase safety levels for CA or other types of aviation.

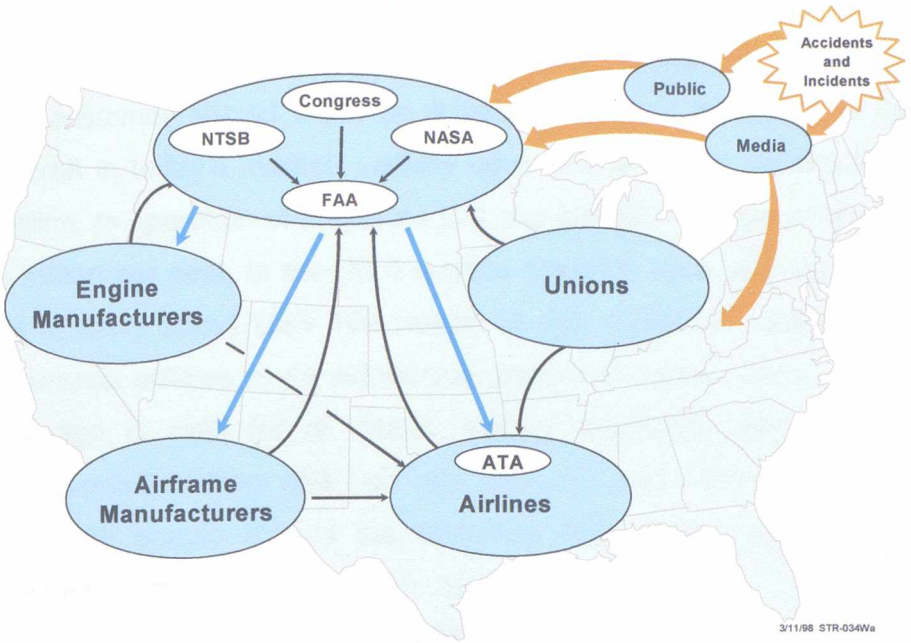


Figure 3.13: Safety Management infrastructure in the USA

In fact, initiatives in both: the US and EU have had only a small impact on aircraft safety in terms of real-time of flight i.e., when safety is most relevant, as shown in Figure 3.1 based on figures from Boeing. They have targeted mainly strategic schemes, improving of aviation safety mostly *in principle* but not *in practice*.

Initiatives to determine the technologies and requirements for safety systems have led to various worldwide safety programs discussed at symposia and aviation forums. Two the most representative ones are: International System Safety Society Conference (US) and Jane's ATC Annual Symposium (Maastricht). The most important fact of modern development of safety management schemes is recognition of requirements for consistent and robust scheme of flight safety management; as pointed out at the Arlington Symposium [29] :

"*Whether or not the aircraft hits the ground should ideally not change the philosophy to determine what, why and how to prevent an accident*".

3.5.1 Insurance, Regulation and Aviation Safety

The most common types of policy for insuring aircraft operations are:

1. "Aircraft Physical Damage Coverage" which covers the risk of potential damage to the aircraft itself and/or the associated equipment.
2. "Aircraft Liability" which covers the risk of potential damage to "third parties", i.e., damage to passengers, crew or other persons and/or their property.

It is only possible to purchase an "Aircraft Physical Damage Coverage" insurance policy when purchasing an "Aircraft Liability" insurance policy. Each insurance policy is provided

on an "Agreed Value" basis, i.e., the insurance company and the customer agree (before a loss) on the insured value of the aircraft. In an aircraft policy, a so-called "replacement value" does not exist. For that reason, when negotiating the policy terms (or the renewal), the customer should insist on a value limit, that would allow the replacement of the aircraft in today's market. Liability coverage limits are provided in increments of US$ 5 million. In operation of corporate jets, the typical limits are considered to be at about US$ 5 million per seat. In the US it is quite common for a corporate operator of an eight-seat jet to carry about US$ 100 million to 200 million in liability coverage. Good aviation insurance policies cover substantial amount of cases. For example coverage of Physical Damage is valid for all cases, except intentional damage or nuclear war. Typical exclusions for "Wear and Tear" are tyre wear and compressor blade erosion. The liability coverage should protect the customer from most lawsuits relating to their aviation operations by employees. For these kinds of claims a special scheme of "Workers Compensation" insurance has become available.

Insurance involvement in CA and BA is well established because of tight regulation which is enforces, GA is in a rudimentary phase. Two main reasons are that GA has a much riskier and less predictable accident rate than any other segment of aviation and also the weakness of its safety management schemes and regulation. To attract insurance companies to the GA market segment will require tighter regulation and more rigorous enforcement. This has already happened in other transport sectors: cars (annual safety tests) and trucks, buses and trains (Tachograph and random weight and driver tests).

3.5.2 Flight Safety and Safety Control Cycles in Aviation

The previous chapters have shown the role and importance of recording flight data for further analysis of flight conditions; the need to understanding the reasons behind accidents is widely recognised. However, the existing schemes of safety management are oriented mostly on post-flight analysis and cannot be used for real time safety monitoring and control of flight safety. In general flight recorder information is overwritten during the next flight and so data for longer term analysis is lost.

A typical cycle of safety management for an aircraft is shown in Figure 3.14. Flight data from the aircraft are downloaded and transported on the ground using a portable carrier such as a tape cassette or solid state memory. More recently the introduction of satellite facilities has provided an opportunity to download flight information in real time via a satellite. Flight Data can then be stored and analysed at a ground data centre to evaluate the safety aspects of the flight, possibly in real time.

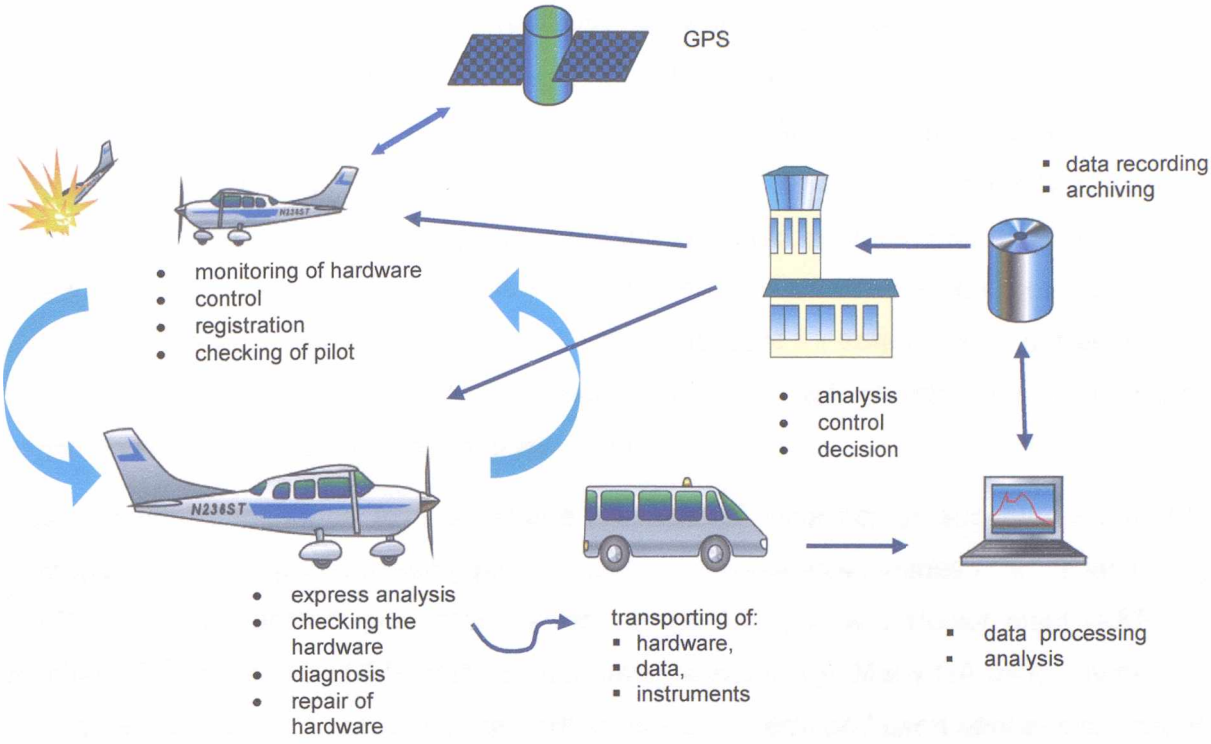


Figure 3.14: Conventional cycle of information processing of Flight Information

At the end of each flight the data can be processed to evaluate flight conditions, for diagnosis of faults in the aircrafts hardware and systems and for recommendations on aircraft maintenance. A licensed engineer then makes the decision whether the aircraft is airworthy. Sometimes, if the facility is available they may call for information from the flight data recorder to evaluated e.g. to determine whether a heavy landing is likely to have done some physical damage. For long-term analysis, processed flight data can be stored in a centralized data repository where it can be analysed for safety trends over several flights or even the lifespan of the aircraft. The media used to record the flight data include various types of data cassettes and portable devices such as autonomous hard disks and, more recently solid state FLASH memories [90].

In general the cycle is designed to assess and improve safety of flight using data analysis after flight. If an accident has happened then a more formal scheme for flight data processing is used. Government accident investigators become involved so the investigation and its results are incorporated into wider safety management schemes.

3.5.3 Constraints and Failures of Safety Management

Although flight safety has improved significantly over the past 50 years, the ever increasing volume of air traffic is causing the number of accidents to rise. This is especially true for GA and private pilots who often have a lax approach to safety and consider regulations to be intrusive, particularly in the USA. Therefore any newly proposed system, such as Active Safety, must offer an unobtrusive yet unprecedented improvement in flight safety if it is to be welcomed and used by them. The costs associated with flight safety equipment are already seen as 'an overhead'. Even though

there are about 300K GA aircraft in the world GA is still considered to be the poor relative by avionics companies. A major problem is the sheer variability between aircraft even of the same type and the need to produce equipment for GA with a much lower purchase cost than for CA. Furthermore GA safety checks tend to be limited as normally there is no flight data recorder and so safety management is based on the experience and visual checking of the mechanics, engineers and pilots involved. The safety cost of this is reflected in the accident statistics: human factors account for some ~ 53% of the primary cause of GA accidents. The 'soft' regulation of GA and lack of strict enforcement also constrain improvements in safety management.

Safety critical negligence issues include the use of incorrect or substandard and/or improperly installed parts, missing parts or failure to follow Airworthiness Directives (ADs) (CFR, 1998). In addition, poor maintenance of the Airframe and Power plant (A&P) by mechanics (regulated by CFR Part 43) is a major safety issue. Many GA pilots, owners or operators fail to adhere to the required 100-hour inspections and even annual inspections and service overhauls. The actual percentages of failures in the practice of Safety Management [26] are listed in the Figure 3.15 below:

Safety Management Failings by Cause	%
Airframe and Power Plants	32.90
Pilot/Owner and operator licensing	12.97
Past overhaul time	3.78
Past or no 100 hour inspection	3.24
Past or no annual inspection	1.62

Figure 3.15: Failures of Safety Management

Figure 3.15 thus confirms that GA safety needs to be managed in a different way, but not necessarily by means of installations of sophisticated and expensive flight data recorders – which are favoured by avionics manufacturers - or by means of new regulations and penalties – favoured by the FAA, NTSB, EAA and EASA. The first option is considered as unacceptable in GA due to its initial costs, installation and maintenance expenses. The second due to the difficulty in implementation – more than a half of the GA pilots/users/owners are using their aircraft in remote areas, in the US only there are more than 19,000 landing fields for GA, many of them are barely more than fuel refilling points. Tracking of aircraft and flight maintenance by regulators is practically impossible. So the old approach continues: the only really objective information related to the safety of aircraft is recorded by flight data recorders and thorough analysis of the data takes place only exceptionally and usually post-accident. Even worse the vast majority of GA aircraft do not have a flight data recorder at all.

3.6 Conclusions on Aviation Safety and Risk of Flight

A classification for aircraft has been proposed with the aim of capturing a technical portrait of a typical GA aircraft including design, technological and management features. The CA and GA often overlap and CA has by far the best safety record in aviation. It is likely that the GA flight data recording and safety management will follow the direction of CA in the future.

Analysis of the Aviation Market shows steady growth both in volume and price of aircraft all segments. As the complexity of new aircraft grows the cost of maintenance will inevitably follow. This is creating a challenge for safety management, making it essential to search for improvement of existing safety management schemes.

Existing schemes of safety management in aviation are oriented on after flight analysis (CA, Military) or are rather weak (GA). All these schemes are easily *avoidable* by GA aircraft owners and users; the 'human' factor being the weakest link in the chain. The situation gets progressively worse as complexity of aircraft grows and they are used more intensively.

Unfortunately in the present situation safety management vies with commercial interests of owners and operating companies involved. Safety margins are being eroded in CA and BA due to tighter turnaround times and lower budgets. In GA the new aircraft are safer than ever, within their class, but new aircraft are becoming popular e.g. personal and business jets, the operation of these introduces new hazards and requires tighter regulation. So far strategic management of safety has not achieved its target, a typical snapshot from the FAA's February 2005 data shown in Figure 3.16 [30] . Even the CA sector suffers from significant incidents, but the GA sector (shaded) has most of the fatal accidents.

So far it seems to be clear that operating within the current regulatory framework for safety and merely collecting flight data is not leading to any overall safety improvement. A new, proactive safety management scheme for aviation at large and GA in particular is required. It is also clear that the level and nature of risk varies according to different operational phases of flight and are a major factor and needs to be taken into account.

Improved regulation and mandatory insurance could contribute to improved safety in General Aviation. Based on this analysis, it is fair to say that there is a need for a method and equipment to improve flight safety. Especially some low cost means of flight data recording and assessment of operational safety in real time is needed.

Topic	Number of Aviation Incidents									
FAA Accident Category	25	24	23	22	21	18	17	16	15	14
All Aircraft Events	3	5	11	29	0	8	7	6	6	19
Fatal Accidents	0	0	2	2	0	1	1	1	2	1
Experimental/Homebuilt	0	0	1	1	0	0	1	2	1	4
FIXED WING										
Airbus	0	0	0	2	0	0	0	0	0	0
Boeing	0	1	1	5	0	0	1	0	0	1
Beech	1	1	1	1	0	1	1	2	2	1
Cessna	2	2	2	4	0	2	1	1	2	4
Piper	0	0	3	6	0	1	1	0	0	3
Other Fixed Wing	0	1	2	8	0	3	2	1	0	5
ROTORCRAFT										
Bell	0	0	0	2	0	0	0	0	0	0
Other Rotorcraft	0	0	1	0	0	1	0	0	1	1

Figure 3.16: Aviation Incident Analysis

Part 2: A Method of Active Safety

Now that the background to safety in aviation has been described in Part 1 it is possible to develop the concept of active safety. The basic idea behind active safety is to reduce risk by improving the reliability of the system at one or more levels of abstraction. Taking aviation as an example there might be the following levels when considering risk reduction:

- *'in the large'* – over the lifecycle of an aircraft
- *'in the medium'* - of an aircraft during an operational flight
- *'in the small'* - of individual pieces of equipment on an aircraft (e.g. avionics units)

The 'proof of concept' experiment described later in this thesis is mainly concerned with the medium level by implementation of an on board system to implement active safety in flight, however the theoretical analysis will concentrate of the medium and large levels. By systematically and actively removing risk in the system i.e., avoiding or compensating for faults as they are detected, the overall system will become as safe as is feasibly possible. PASS in the small is the theme of a separate but related research project [56]. Part 2 explores the Principle of Active System Safety initially from a theoretical perspective and then from a more practical one, leading to the development of the Method of Active System Safety in an aviation context.

4 Principle of Active System Safety for Aviation

4.1 The Scope of PASS

The development and realisation of any new concept or idea follows the standard research practice: review existing phenomena and state of the art, introduce a new idea or concept and then analyse the limits of possible implementation of the new concept or approach. PASS follows the same pattern:

PASS in the large is concerned with taking into account faults that gradually develop over the lifecycle of an aircraft. Such faults may be undetectable during one or even several individual flights. For example a gradual loss of efficiency of engines.

PASS in the medium is a key for implementation on board, based on MASS as defined later in Part 2. Its main concern is with detecting faults during aircraft operation (on the ground or in the air) to reduce the risk of an operational accident.

PASS in the small can be used to reduce the risk and improve the performance of equipment used to implement *PASS in the medium.* Its main concern is to enable a fault tolerant platform to be built to support MASS processing by detecting hardware faults in real time and using redundancy and reconfiguration to mask their effect [56].

In the sections that follow the theoretical aspects of PASS theory are defined, including a more detailed explanation of the concept of an active system safety. Similarities and differences with the so-called fault tolerant system design approach [40], [41] are investigated and analysed and a new, generalised theoretical approach developed, including elements of redundancy theory for analysis of PASS. Account is taken of related work in automotive applications [42], where safety is focused much more on individual passenger survivability, and vehicle health management [43] which focuses on timely maintenance.

4.2 Latency of Faults and Safety Monitoring

The latency period between a fault occurring and its manifestation is of crucial importance for safety management. The old adage that 'prevention is better than cure' has sometimes been forgotten when it comes to flight safety management. A spectacular and rather grim example of this is the Challenger shuttle disaster [44]. In this case, although data had been monitored and recorded continuously the data *were not processed in real time* and consequently vital safety information was simply not available when it was needed most. Even worse, it is quite probable that the crew could have survived if the goal of the safety management system had been to actively avoid risk in real time.

The Challenger case is worth reviewing; if for no other reason than to learn from the mistakes and avoid their repetition. The main elements of Challenger are shown in Figure 4.1. The propulsion elements are two solid-state boosters and an external fuel tank plus

the Orbiting Manoeuvring System which includes two small engines used when changing orbit and guiding the return to Earth.

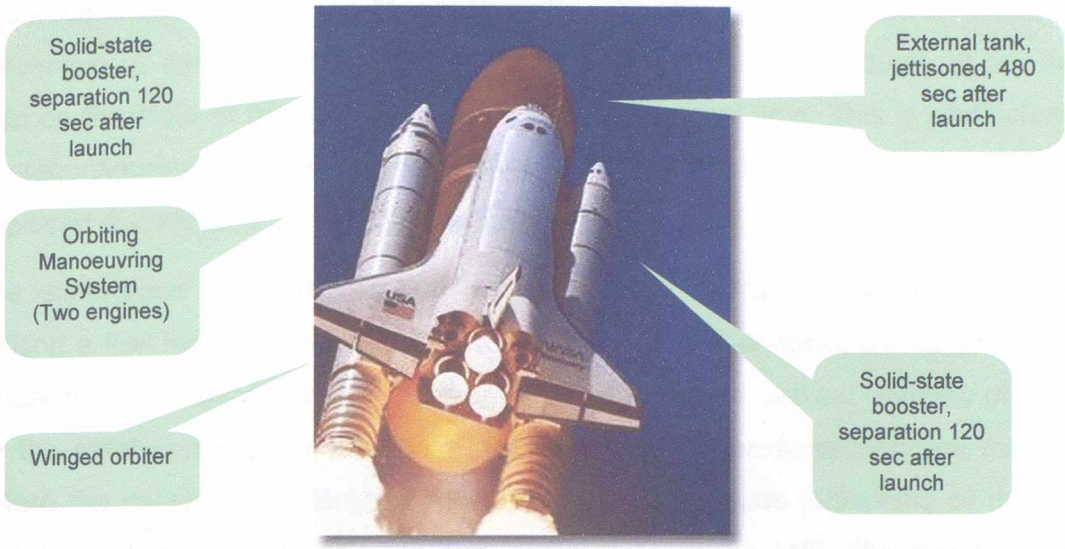


Figure 4.1: Potential for reconfigurability of the Space Shuttle

Two minutes after blast off, the solid-state boosters are jettisoned from the spacecraft. After eight minutes of flight, the external tank is jettisoned. This illustrates that *reconfigurability* is a key feature in the design, function and operation of the Space Shuttle. According to available information about the accident [47], a leakage of gas from an 'O' ring seal (operating at below their design limit temperature) during blast off was recorded by on ground monitoring devices several seconds before its physical manifestation became apparent. The *latency* between the faults occurrence, its manifestation and the actual disaster was approximately 10 seconds. It caused the final explosion in the 72nd second of flight; the sequence of events is shown in Figure 4.2.

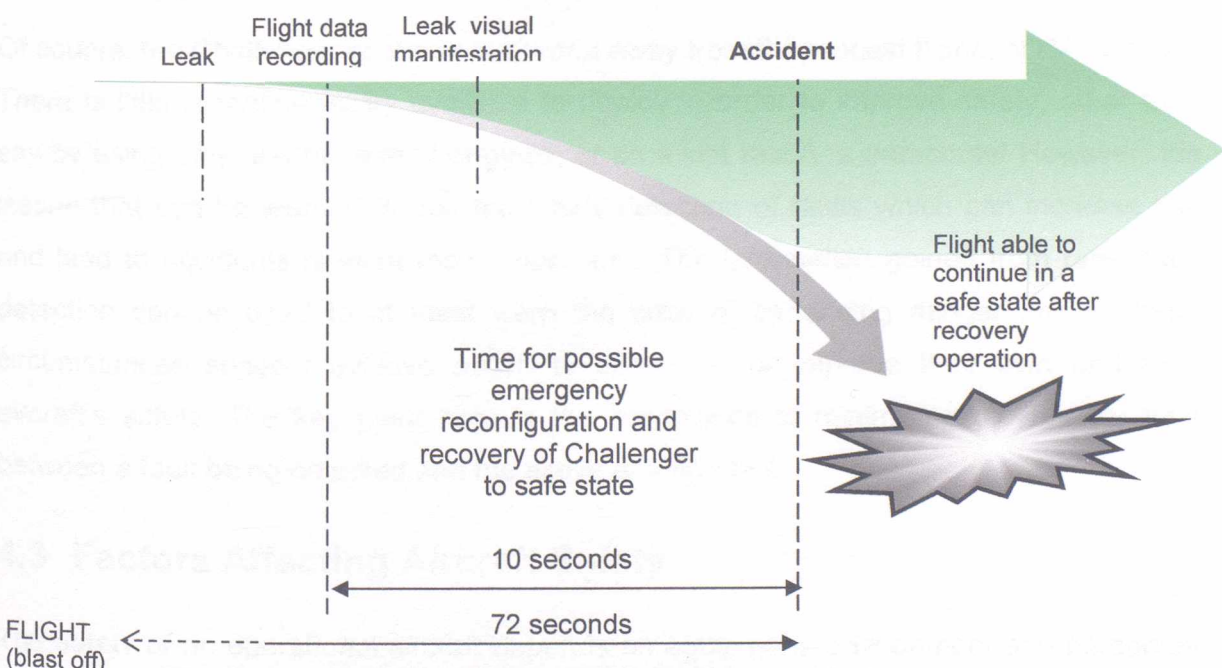


Figure 4.2: Relative timing of the Shuttle accident sequence

The Challenger safety system was (and still is) based on post-flight analysis, *rather than analysis during real time of flight*. Unfortunately this safety management approach was a major contributory factor to the biggest loss in the history of space exploration. No preventive or corrective action was anticipated or taken even though all the necessary data on the state of the spacecraft were available in real time. This is particularly sad as the reconfigurability, on which the Challenger design is based could probably have been deployed dynamically making it possible for the crew to survive.

The experience from the Russian space program indicates that the time required to jettison a fuel tank and/or a stage with a crew onboard is about 0.2 seconds, or slightly longer to avoid fatal G forces. Therefore, there was a 10 second 'window of opportunity' for the safety management system and the ground team to reconfigure the spacecraft before the explosion. Potential options were the immediate jettisoning of the faulty fuel tank and initiation of an OMS-assisted, emergency landing [45]. The moral of the story is that the design of the *safety management system* can have a profound effect on the effectiveness and safety of the system being monitored, this is especially true if the safety system is systematically implemented. In 2005, NASA finally declared that flight data recorders (black boxes) would become an essential element for all future manned spacecraft [46]. Unfortunately, there is not even the slightest hint that the safety management system for the Shuttle program will be redeveloped in terms of active safety... Richard Feynman's incisive comments on the Shuttle accident (Jan 28 1986), [47] are still valid over twenty years later:

"Let us make recommendations to ensure that officials deal in a world of reality in understanding technological weakness and imperfections well enough to be actively trying to eliminate them..."

Of course, the Challenger scenario is a world away from the modest flights of CA and GA. There is little reconfigurability available to deploy in order to improve safety, other than say by using only one of several engines, or as a last resort, a parachute! However, the lesson that can be learned is that the timely detection of faults which can increase risk and lead to accidents is even more important. The information gained from rapid fault detection can be used to at least warn the crew of impending danger and in some circumstances suggest evasive action to conserve, or improve their own and their aircraft's safety. The key point here is the importance of minimising the latency time between a fault being detected and the active reaction to it.

4.3 Factors Affecting Aircraft Safety

The safety of an operational aircraft depends on equipment, environment and personnel related factors. The equipment factors are the behaviour of: the aircraft itself, its main

elements (such as airframe, flaps, landing gear, engines etc). The personnel factors involve the pilot and crew and the passengers. Typical environmental factors are: weather, airport conditions, radio communication faults, ground control faults, GPSS faults, airport service faults caused by random or systematic faults of operational safety management and maintenance. MASS is an on-board active safety system and so is solely concerned with internal aspects of aviation safety. On this basis the safety of flight can be abstracted using a vector:

$S = <S_i, S_e>$

where S_i represents the level of safety determined by on-board conditions and

S_e the level of safety determined by external conditions.

The safety control problem can then be defined in terms of the vector S and a proper reaction to the situation determined when S_i and S_e move toward an unacceptable threshold level of safety. The function of future advanced safety systems is to keep the internal value of S_i as high as possible during the lifecycle of the aircraft, this is illustrated in Figure 4.3.

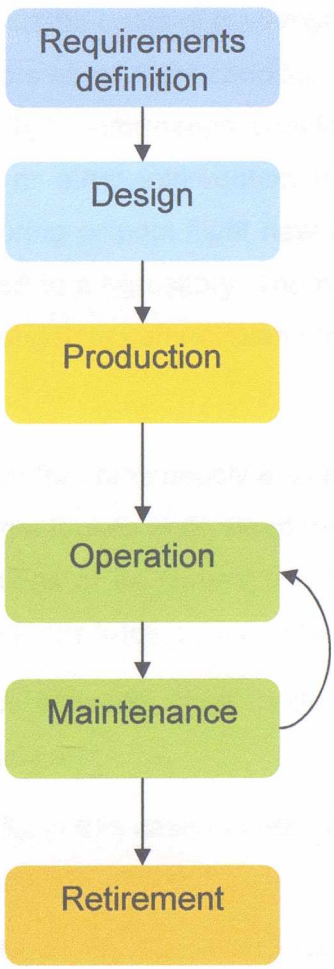


Figure 4.3: The lifecycle of an aircraft

The challenge is to investigate ways in which to characterise and manage safety levels by means of a special monitor of flight safety. **So the theoretical problem of aviation safety is to create a model for flight risk that supports the accumulation and processing of flight data and then dynamically uses it to describe and predict the risk profile in the short term during flight and in the long term over the lifecycle of the aircraft.** The later point is important because some faults will develop over time; their latency is greater than one or even several flights. Also, to avoid endless modifications and patches to compensate for poor design (so-called service packs...) the safety system should be designed based on a generalisation of the flight safety model. Specific parameters should be used to characterise the model for a particular aircraft and its specific configuration. This approach makes it possible to avoid necessary modifications of the main structure of models due to the variety and particular configuration of aircraft in use. So any new system must:

1. use existing flight information
2. accumulate essential information about previous flights
3. process existing and newly received information
4. where possible, make a prognosis concerning the future safety state of the aircraft
5. react in real time of flight on the basis of the prognosis
6. transmit essential indicators about flight conditions both during and after flight.

Another important point is that flight information should be used by the safety system itself, without pilot intervention, or other intervention from the on-ground maintenance personnel during flight. Either during or post flight new and accumulated flight data and information should be downloaded to a repository. The new on-board safety system must be active and ensure that the pilot gets a safer airplane to control.

4.4 PASS Definitions

Definition 1: PASS is an approach for continuously evaluating and processing the state of an aircraft as a system in real time. It uses analysis of the previous and current behaviour of the system to provide indications of its current and future states and then proposes actions to provide safe operation in the known circumstances.

PASS analyses the relationships between three models including their interaction and mutual influence. The three models are:

1. The model of an object M_o, in this case the aircraft is the object. The model for an aircraft is described in detail in Chapter 7.

2. The model of the faults M_f which the object may suffer currently or in the future. The model for faults is described in Chapter 9, section 9.4. More specifically each fault may be modelled of its own lifecycle evolving typically through a set of states

such as normal, marginal and faulty. Fault modelling and detection are also discussed in Chapter 7, section 7.3.

3. The model of active safety M_{as} which might mitigate the effect of faults. This is described in detail in Chapter 7.

In fact, the object and fault models taken together characterise the model of active safety. Their logical dependence is presented in Figure 4.4 below:

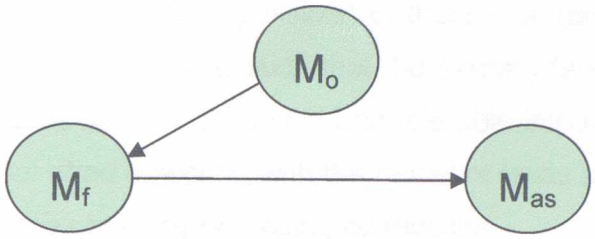


Figure 4.4: The three basic models

First of all the model of an object must be defined, faulty behaviour can then be interpreted based on the behaviour of the model when compared with the currently sensed reality. Then the safety model can be defined to take account of the existing models and seek to conserve or even improve the safety of the system given the set of evident or anticipated faults. If this can be accomplished then, according to Definition 1, an active safety system will have been achieved. On the assumption that all three models are static, i.e., do not change during the operation of the system, Figure 4.4 can be modified to Figure 4.5:

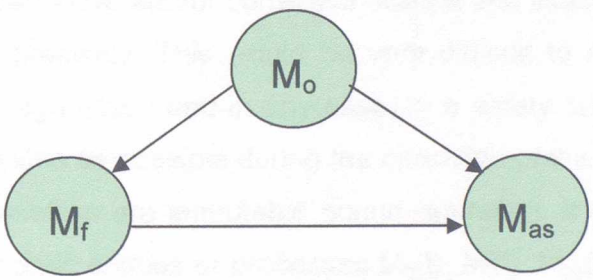


Figure 4.5: Mutual dependence models during operation of an object

Note that it is only possible to achieve active safety if the model of the object M_o is known and constant during object operation as this makes it possible to detect its faulty behaviour. A short description of the M_o, M_f, M_{as} models is presented below:

M_o models the real world object, in this case an aircraft. The challenge is to define the model(s) in such a way that it will be possible to determine the behaviour of the object (aircraft) in presence of a fault or even predict the imminent occurrence and manifestation of a latent fault.

M_f models the set of faults that M_o can suffer and can also be defined as a model itself. To take a simple example the rate of fuel use might be incompatible with the aircrafts airspeed and rate of climb. In analogue devices faults can be described by a threshold

function – less or greater than required limits, or by noise etc. It is assumed that the set of faults of M_o is known or can be derived. Note that faults may not just be manifested in individual values or within absolute limits. There may be dependencies between the parameters used to detect faults; also it may be the rate of change of a value or its long term trend that indicates a fault rather than its current absolute value etc.

M_{as} models the object's behaviour in terms of increased risk which in turn reduces safety. Active safety assumes that the system state is monitored and in the presence of a fault is preserved (or conserved as far as is possible) or there is a transition from correct (fault free) state to another workable state, such that the existing fault does not influence the system's function or does so with a minimal and tolerable impact. So M_{as} represents an interaction of the model of an object M_o with the model of faults (or errors) and as a result may change states of the object by proposing corrections.

Using three such models it is possible to find a way or ways to avoid, exclude or reduce the influence of faults in the object dynamically. This is in contrast to the traditional static approach to safety systems using techniques such as Fault Tree Analysis (FTA) [27], [48], [49] and Failure Mode Effects and Criticality Analysis (FMECA) [50] at design time. Of course they still have their place in the original design of the object, but here we are concerned with the operation of the object over its lifecycle.

So ideally it would make sense to continually perform the FTA and FMECA analyses dynamically throughout the operation of the system to identify impending faults and then determine relevant preventive and/or corrective actions and indicate them to the system's users concisely and precisely. This would be very difficult to achieve in practice (it is difficult enough at design time!) and in any case, in a safety critical system it is best to deduce or change as little as possible during the operation of the system. PASS assumes that the models themselves are immutable during operation. It might seem attractive to consider them as dynamic entities or processes $M_o(t)$, $M_t(t)$, $M_{as}(t)$ to provide longer term interactive 'tuning' of the system. However, their interaction and time dependence can only be taken into account only in discrete increments 'in-between' flight operations because even a static change in one model may imply a change that must be detected and reflected in the others. So any model adaptation needs to be done 'offline' when the aircraft is not in service.

The question now arises what is active safety precisely in terms of the models? Let us apply Dijkstra's method for defining the function of a system [51]. According to this method the function of the system is defined if it is possible to define an algorithm to implement it, the so called algorithmic function definition. The function introduced here is active system safety and so PASS can and will be defined and described by the algorithm used for its realisation.

The Principle of Active System Safety can be implemented using repeated steps outlined in Figure 4.6 below:

LOOP

A: Evaluating the conditions and processes in the system that create or might create a reduction in the current or future safety level (diagnosis and prognosis) using element models of the object to identify faults and thereby hazards

B: Making a decision about trends in the system in terms of safety (and level of danger/risk) using discrete, semantically driven or probabilistic models of the system (or combinations of them).

C: Determination of the reasons (or faults, or event) that cause a detectable reduction of safety or safety level.

D: Analysis of possible reactions and options available, including full or incomplete recovery (management of system deficiency).

E: Formation of the set of actions to restore and/or recover safety.
F: Form and issue advice in the form of safety information
G: Estimation of the level of safety achieved (restored and/or recovered).

END

Figure 4.6: APASS: steps for implementing PASS

The implementation of APASS must execute Step A continuously until the current system state is 'comprehended' and deemed consistent (stable) as a basis for further PASS analysis. In practice the complexity of the PASS implementation will vary depending on the complexity of the object, the set of faults and safety models. Of course hardware support for safety is the most time efficient way to implement PASS; the same is true for fault tolerance as well. The hardware and software platform used to implement PASS will determine the overall system performance possible and thus determine resources required. In order to be effective, the implementation of active safety needs to produce the required results in real time i.e., detection of possible trends, evaluation of possible prognosis and reaction on the existing signals and other information should be completed before any adverse event takes place.

Ultimately the reliability of the system (or object) depends on time to restore normal or acceptable conditions. Thus the length, performance and availability of the APASS implementation become significant in themselves in terms of the reliability of the overall system. This is demonstrated in Chapter 5.

4.5 PASS and Elements of Redundancy Theory

Active safety relies on the monitoring of system state and in the presence of a fault the system state is preserved (if possible) or there is a transition from correct (fault free) state to another workable state, where the existing fault does not influence system's function or does so with minimal impact on safety. In this context the term system state refers to a set of variables which represent the current state of the aircraft and which can be monitored within their expected domains to detect faults or the onset of faults. This is discussed further in Chapter 9.1 and Appendix 4. The transition to another workable state depends on either the availability of a redundant implementation which supports the masking of a fault (e.g., in the hardware) or the transition to an operational state which is achievable and safer (see 7.2).

All steps in the algorithm in Figure 4.6 must be completed within some required time and in such a way that the occurrence of faults and their elimination are transparent to the system. This is in contrast to other known types of systems that are designed to tolerate faults but with a degradation of performance and/or functionality; so called graceful degradation systems [28]. In order to be really effective an implementation of APASS requires *supportive redundancy* using information, structure and time. The classification of redundancy categories (types) and their inter relationships are presented on Figure 4.7 below:

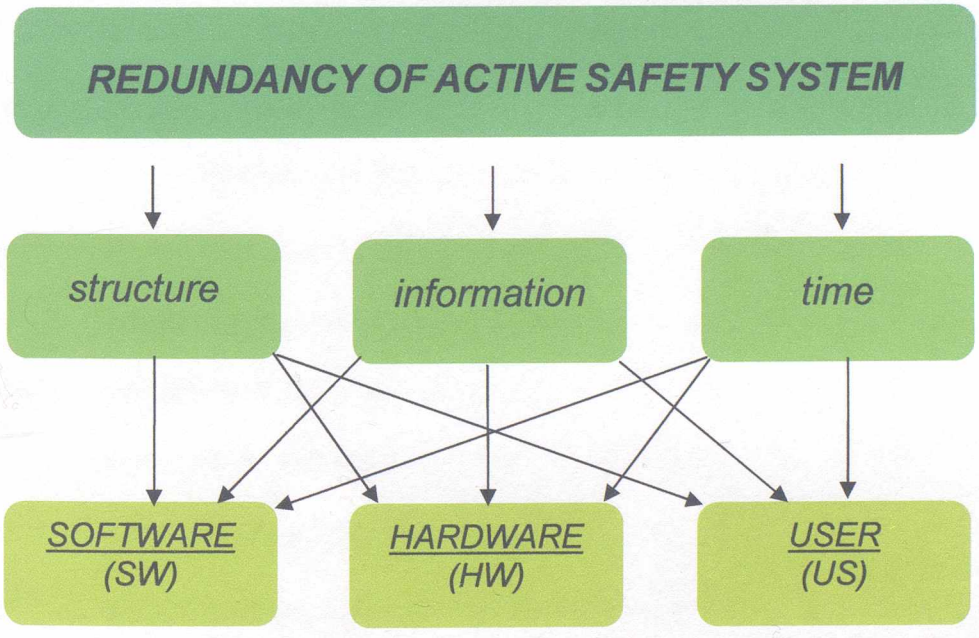


Figure 4.7: Classification of redundancy types and inter-relations

The first level of detail in Figure 4.7 describes the conceptual elements of redundancy used: structure, information and time. So for example an implementation structure in the aircraft might contain redundancy; it might be possible to glide to a safe landing without engine power or to use only a single engine to achieve a safe landing. Each type of

redundancy defined at the second level is implemented concretely either by software, hardware or by user. An example here might be duplicated or triplicated hardware elements such as system RAM memory in the active safety computer. Thus, redundancy has nine basic variants: three based on hardware, three based on software and three based on user involvement in the APASS implementation (i.e., of PASS in the large, medium and small).

The more specific and well defined the redundancy types are, the more characteristics of the system can be expressed in terms of this classification and the more predictions regarding the behaviour of the aircraft can be made in terms of safety (i.e., by making active use of the redundancy to avoid risk). In Table 4.7 below the redundancy types are clarified and further defined using examples from various known and widely used safety systems. In each case the suffix indicates the main type of redundancy involved; (i.e., S = structure, I = information and T = time).

Hardware based redundancy types	
(in this case the whole aircraft is the 'hardware'):	
HW(2S)	structural redundancy of hardware such as duplicated engines;
HW(S1,S2)	hardware system with different (non identical) units for the same function;
HW(I1)	extra information in hardware, to check errors;
HW(nT)	special hardware implemented n-time delay to repeat functions;
HW(dT)	special hardware implemented small delay to avoid malfunction.
Software based redundancy types	
SW(2T)	double repetition of the same procedure to check the results;
SW(I)	informational redundancy of the program: back-up files, recovery points;
SW(S1,S2)	two different (diverse) versions of the program for the same function;
S(dT)	time delays realised in software for waiting a guaranteed result.
User based redundancy types	
US(2T)	double deliberate delay to act, used to check the results;
US(I)	informational redundancy extra information to improve reliability;
US(S1,S2)	two pilots with different functions to increase safety;
US(dT)	small time delay to increase reliability of result.

Table 4.7 Examples of Hardware, Software and User Redundancy Types

4.6 APASS in more detail

The system is considered as safe as possible if and only if APASS is realized in full, i.e., steps A to G, as shown in the Figure 4.6. In addition APASS can be considered to have three very similar parts: one for hardware, one for software and one for the user(s). It is assumed that APASS is applied as long as the system exists, and analysis of the flight data is processed in real time of flight. So APASS uses several processes to generate "triggers":

1. The monitoring of measured aircraft parameters (e.g., as in Figure 9.3)
2. Discrepancies between real and modelled (ideal) behaviour of elements of the aircraft.
3. Correlation between measured values from redundant sources of information (e.g. GPSS position and gyro based position). These might indicate equipment faults.

In practice the actions related to recovery proposed by APASS must be specific and due to the latency of faults the recovery scheme needs to be carefully designed. For example, if the operational state of an aircraft is determined as 'uncontrolled descent' then the action advised would be designed to achieve a state of 'controlled descent' (see Appendix 4 for further details). If successive steps of recovery attempts are not successful and it is not possible to determine a correct state or any acceptable degraded state of the aircraft as a system to allow continued safe operation, then APASS must inform the pilot(s), as in step F of Figure 4.7, and request that they deal with the final stage of exception handling of the situation. The intention is that APASS should propose recovery advice to the pilot related to safety rather than just 'panic signals'.

The problem of determining the set of correct states of the aircraft is particularly difficult and its refinement will be the subject of further research with the aim of producing a software tool that encapsulates the process. The structure of the APASS implementation must reflect the physical structure and features of the aircrafts constituent elements (subsystems) and the errors and faults which APASS is intended to accommodate. This in turn must take advantage of redundancy within the aircraft, when viewed as a system, as a basic means for achieving active safety as a new system feature. Various implementations of APASS may differ in terms of:

- time of completion of different steps.
- types of redundancy used for various steps.
- types of fault and errors tolerated.

The main "ingredients" of the system (user, hardware, software) are the sources of all the possible internal faults. By considering and using various redundancy types the safety of the system can be improved by design and in operation. Thus the elements of the problem become the elements of the solution. Figure 4.8 shows a notional APASS implementation using different redundancy types as a series of protective shells which seek to provide different aspects of safety protection based on user, software and hardware. In each of these shells different redundancy types can be used for a particular implementation that are specific to the user, software and hardware, as outlined above in Table 4.7 above. For example software monitoring of users condition of health, skills etc is widely known; also software that can test and reconfigure hardware and static hardware redundancy is widely used in aviation (the use of multiple engines is primarily justified by safety requirements). All these redundancy types are interdependent, designed in concert and implemented together to achieve final goal - safety and active safety of the system. Naturally every implementation of APASS will differ in system safety features, performance and cost depending on the particular aircraft's fundamental features, its intrinsic redundancy and the relations between its elements (subsystems). The cost of applying various redundancy types will also have an influence on the architecture and engineering solutions selected for safety and active safety systems.

For implementation APASS can be considered to be a triple algorithm, as in Figure 4.6, applied for each part of the system for the user, software and hardware.

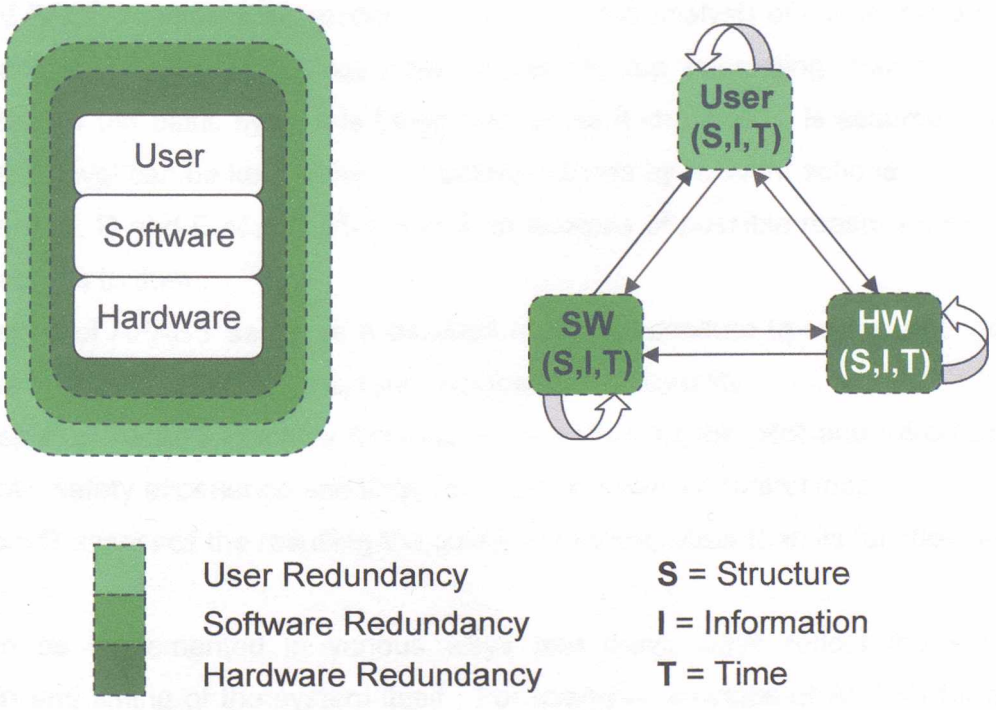


Figure 4.8: Redundancy Types for implementing PASS

4.7 PASS, Dependability and Fault Tolerance

The PASS concept differs from the other known concepts such as dependability and fault tolerance [52], [53]. Dependability assumes that the system tolerates a wide range of various faults after their appearance. Briefly, if the state of hardware is denoted by S_{HW}, the state of software by S_{SW} and the state of user as S_{US} then the system dependability is: $P(S_{SW})$ & $P(S_{HW})$ & $P(S_{US})$, where P represents the predicate of serviceability [28].

In other words this is the *predicate of absence of software errors, hardware faults and user mistakes* in the system and on the set of states of the program. It is defined and then defensive mechanisms are put in place in an attempt to ensure that the predicate is continually true. But dependability in practice ignores an inherent *latency* of faults in the system which in turn reduces the timely responses that can be used to avoid fault manifestation and to conserve or improve the safety of the system.

In *contrast with dependability* PASS is an active part of the system itself; this is based on step A of the algorithm of Figure 4.5. It is *proactive* and operates *concurrently* with the functioning of the system and is based on *diagnosis and prognosis* of actual and potential fault trends in the elements of the aircraft not just on the actual manifestation of faults.

It is also important to understand the difference between *fault tolerance* and PASS. The key difference is that fault tolerance (or reliability or safety) is a feature of the object, while *active safety is a process*. So, referring to Figure 4.6, active system safety differs from *fault tolerance* because:

1. Step A of APASS assumes *proactive* behaviour to search for new potential threats and PASS considers the model of the system and analysis of risk as dynamic with changeable behaviour. These two processes are interacting and the level of safety of the basic system is being tracked as it changes. It is assumed that the safety level can be kept within acceptable bounds by relevant actions.
2. Steps C, D and E of APASS present an analysis of possible reasons/causes and reactions to them.
3. Step E of APASS assumes a decision making procedure to restore the required level of safety in the basic system, not just its functionality.
4. Step F of APASS involves formulation of advice for the pilot and introduces the pilot's safety experience and judgement into the overall control loop.
5. Step G assesses the resulting the safety of system rather than its functionality.

PASS can be implemented in various ways and these ways reflect the structure, information and timing of the system itself. For example, all steps of APASS for a hard real time (RT) system should be also developed as RT, and without any reduction of existing features for the sake of safety. In general the operation of PASS should be

transparent for the basic system, this is especially true for existing systems where we are trying improve safety. However, if the system can tolerate some delays in decision making procedures or accept latent (hidden) erroneous conditions before active phases of the application then some steps of APASS might not need to be completed in real time, for example steps A, B, D, E.

4.8 Improving the Safety of a System

A system that has not been initially designed as safe or that requires greater safety can only be improved if we either redesign it completely (to be *intrinsically* safe) or add a system level that will be able to measure, analyse and amend the safety of the basic system. Complex systems, such as society, defence, transport at large, aviation, aircraft, railways, etc are very difficult to change and it is certainly rarely an option to redesign and replace anything that already exists and is already well established. This is true in particular for aviation, there is no prospect that all existing aircraft can be redesigned, even on safety grounds. The fact is 'we are where we are' and the strategy to improve safety must therefore, in most part, rely on improvement by adding to the existing system. This must not of course unduly affect its original function and availability. So to embed active safety as a new feature of a system it needs to be extended with a Safety Monitor which possesses the capability to use the models mentioned above to identify and reduce risk in the system being monitored. The Safety Monitor implements a practical version of PASS in the medium (i.e., MASS) and *itself must have unique features of safety, reliability and availability* so that it does not also adversely affect the safety of the overall system.

The system (aircraft) without PASS is illustrated in Figure 4.9 below. Here the flight data is collected and presented to the pilot(s), the pilot then interprets the data within the flight context and within their knowledge of the previous history of the aircraft (usually not very much). In some cases an auto pilot may use the same data and be used to control the aircraft on behalf of the pilot. A more detailed version of this diagram is shown in Figure 8.1.

Here the model M_o, see section 4.4, is embedded in the Flight Control System which itself is partly embedded in equipment and mostly in the pilots brain or the autopilot's computer. The aircraft (and pilot for that matter) can suffer from faults, which are either latent or manifested. The pilot, and to a lesser extent the autopilot, can react only to manifested faults and only then when they become conscious of them. Any latent faults remain hidden unless or until they become manifested. So the model of faults M_f that the object may suffer currently or in the future will very much depend on the knowledge and experience of the pilot and the pilot's awareness of the manifested faults. Consequently the awareness of current and future risk is very dependent on human factors and the

nature of the pilot's response to current faults [57]. The evaluation of the implications of the faults/risks is also totally dependent on human factors [58]. There is no 'built in memory' about what has happened during previous use of the aircraft in terms of previous faults and the actual behaviour of the aircraft; once the pilot leaves the aircraft that knowledge is lost.

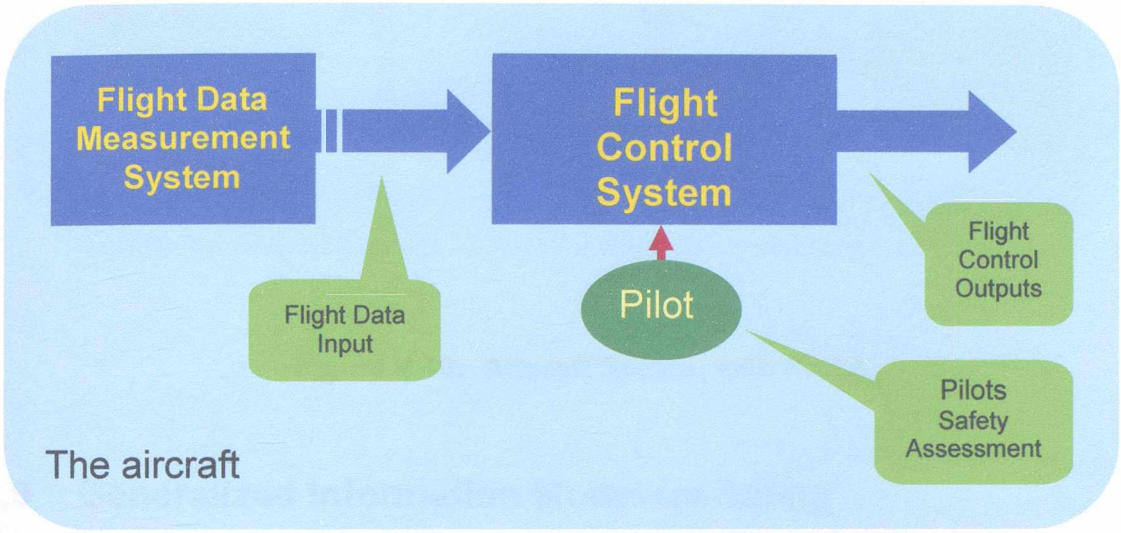


Figure 4.9: Aircraft System without PASS

In contrast an aircraft fitted with PASS is illustrated in Figure 4.10. Here, as before, the flight data is collected and presented to the pilot(s), the pilot then interprets the data within the flight context and within their knowledge of the previous history of the aircraft (usually not very much). However, the flight data is also stored and interpreted by the Active Safety (AS) system which forms a kind of 'safety control loop' around the existing Flight Control System. Now the model of the object (aircraft) is represented in the form of M_o in the AS, of course there is still a less detailed and less consistent version in the pilot's brain too. The model of faults M_f is also contained in the AS and again is more complete and consistent than the version in the current pilot's brain. Most important the model of active safety M_{as} is also in the AS, and it evaluates and interprets the short and long term flight data to extract information regarding both current and latent faults without dependence on human factors during flight.

It also contains an 'active memory' which not only stores data collected on the current flight but also a condensed form of the data relating to previous flights i.e., the aircraft's previous lifecycle of behaviour, its saga. Again, this is without reliance on human factors.

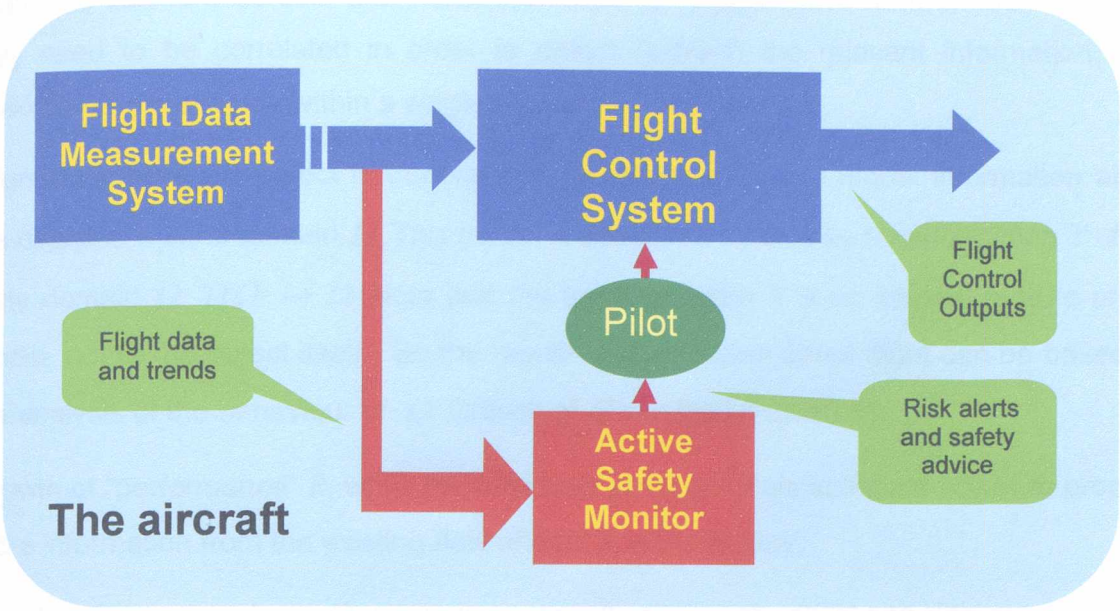


Figure 4.10: Aircraft System with PASS

4.9 Generalized Information Model for Safety

This section presents a generalisation of the role of information in the process of safety management. The models presented so far have not illustrated the role of information in terms of determining the risk of flight. In fact there are two main sources of information relevant to the condition of the aircraft; either incoming information or existing information that has been derived and processed during flight. Consider now some generalization of the relation between information and safety in flight safety.

An object (aircraft) can be described as an abstract model by a set of states Ω and a "reflection" (R) of real object information into its model presentation. There is an opinion, often instinctively true, that the more data a model accumulates about an object, the greater will be the possibility to predict the behaviour of the real object based on the model. Note that the reflection process R is about transformation of real data into data of the model for further processing. In aviation R is implemented by scanning the input sensors and building up flight data frames. The rate at which data must be sampled must take account of its intrinsic information content as established by Shannon in the 1940s [54] to ensure that it is captured. For example, in aviation equipment the data sampling period is either 1 or 8 times per second depending on the application. In General Aviation where speeds are much slower 1 sample per second is adequate to faithfully capture the data trends. However in Commercial and Military Aviation 8, or even 16, samples per second are required due to the higher speeds encountered and the faster response times required. The number of information sources is not the key issue here, the most important feature of each source is that it must contain information that is relevant for detecting user

mistakes, software defects and hardware faults. Of course several information sources may need to be correlated in order to detect (extract) the relevant information; it is unlikely to be contained within a single source.

Information from the object is transformed by means of R into model information about the object in a state domain Ω. This model is described by its own transformation T of the state domain Ω: $T(\Omega) \rightarrow \Omega$. Note that the transformation T is an internal feature of the model, not of the object itself. So the model of information about flight can be based on the analysis of the behaviour of Ω. Growth of Ω can be achieved by:

Growth of "performance" R, while the reflection procedure has sufficient power to process more information from the existing flow of data in a timely way;

Growth of time t to form Ω using the same R, while one is able to use more time to provide more precise prognosis i.e., the results are not required urgently;

Auto-generation $A(\Omega) \rightarrow \Omega+$, $\Omega+ \supset \Omega$ where a new state of domain $\Omega+$ is generated based on the existing Ω in an attempt to achieve some additional meaning or benefit.

With flight safety in mind the third variant of $\Omega+$ growth seems questionable as it does not involve receiving any new information from the object for its translation into information for the model. This is a well known phenomenon in any system where the human factor is involved, for example bureaucracy tends to create more bureaucracy but not efficiency...

The two other options are much more attractive: growth of time t having the same R increases set Ω up to $\Omega+$, and if $\Omega+ \supset \Omega$, it means that new information about the object is presented in the model. On the other hand, growth of performance of R so that $R \rightarrow R+$ changes the pair $\{R, \Omega\}$ into the pair {R+,Ω+}, where $\Omega+$ can also be substantially bigger than Ω. *Some correlation measure between the "physical" state of the object (aircraft) and its level of safety needs to be established.* Let us assume it is P the probability of successful flight completion; now flight safety improvement is concerned with analysis of $\{R, \Omega, T(\Omega), P\}$ and the other terms are presented above.

Practically useful directions of flight safety theory development are:

1. To change Ω so that $\Omega \rightarrow \Omega+$ to increase P to $P+$;
2. To change $T(\Omega)$ to provide growth Ω to $\Omega+$ and P to $P+$;
3. To vary Ω and T to achieve a maximum of $P \mid P$: $\Phi(\Omega, T(\Omega)) \rightarrow Pmax$.

Here Φ is a subset of the states in Ω that describe faulty behaviour. Together Φ and Ω define a probability function of successful flight. The transformation of existing space Ω by means of T to $T(\Omega)$ describes the role of safety model and can be used for evaluation of achievable flight safety and the efficiency of the model itself. The connection of these tasks to real flight data is determined by the size of Ω, the performance of algorithms and hardware ($T(\Omega)$) and, from an empirical viewpoint, the statistics of aviation crashes. So in terms of information the task of analysis of flight safety can be described by:

$$Io \rightarrow R_o(Io) \rightarrow Im \rightarrow Rm(Im) \rightarrow \Omega \rightarrow T(\Omega) \rightarrow P$$

where:

Io , Im are real information about the object and model information respectively, and

Ro , Rm are the reflections (transformations) of the features of the object into features of the model, and

$T(\Omega)$ is the transformation of the set of states in the model for further analysis of the probability of successful flights.

Growth of Ω into $\Omega+$ might infer an indirect increase in information about the object, but only within the limits imposed by physical laws. The number of states connected with crashes is presented in the model as Φ, and $\Phi \subset \Omega$ and $\Omega \subset \Omega+$. This means also that $\Phi/\Omega > \Phi/\Omega+$ and a model with a larger set of states should make it possible, at least in principle, to reduce the risk of an accident because it becomes possible to detect adjacent bordering states. The growth in the number of states is determined by $(\Psi/\Phi)/\Omega+$ where Ψ goes from $\Psi/\Omega+ = \Phi/\Omega$, the relationship between the sets of states is illustrated in Figure 4.11.

When $\Phi \subset \Psi$, then there is an option for prognosis of system state and success will be more likely when the "smoother" and "regular" set of states Φ is enclosed by set Ψ. It is worth pointing out again that Φ represents the set of accident (risk) states and fortunately it will not grow when $\Omega+$ grows.

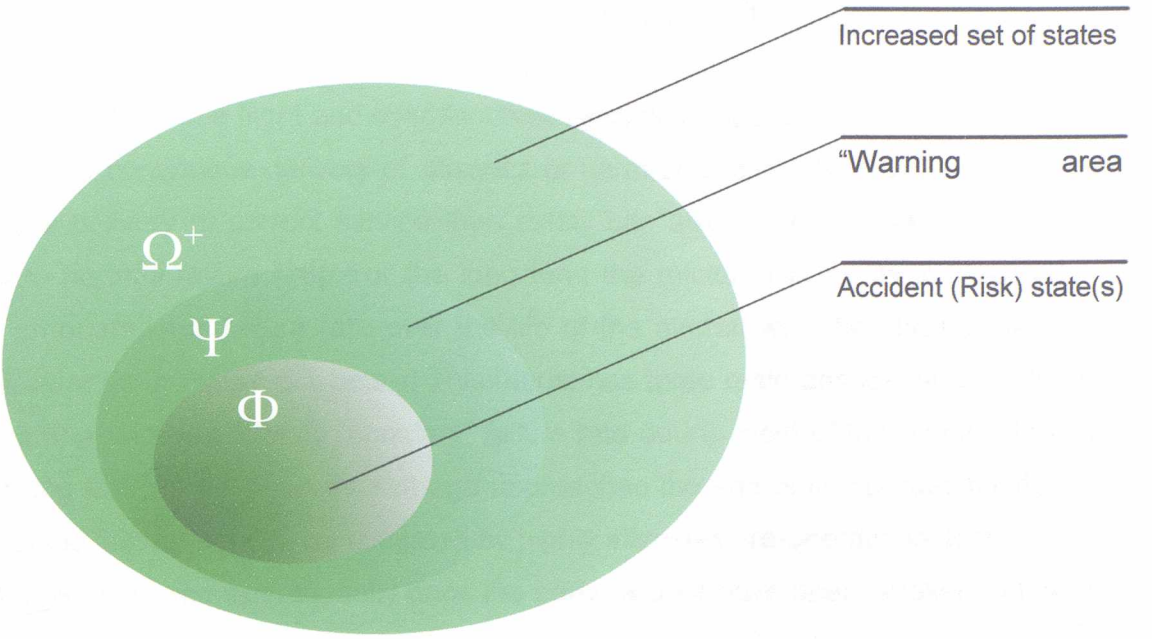


Figure 4.11: The relation between different kinds of states

5 An Operational Reliability Model for Aircraft

One of the objectives of the active safety approach is to improve the operation safety of an aircraft both within a flight and over its whole lifecycle of operation. Given that safety is a measure of continuous delivery of absence of harm and reliability is a measure of the continuous delivery of correct service then safety can also be viewed as reliability with respect to harmful failure [28]. For the long term the reliability of an aircraft is likely to exhibit an operational failure rate over the life of the aircraft with the classic "bath tub" shape illustrated in Figure 5.1 below. This model has three main phases: an initially high failure rate, a relatively steady "constant" failure rate during most of the overall life cycle and a rising failure rate when aircraft age approaches the end of its operational life. The impact of the first phase can be mitigated by highly intensive pre-operational testing of the aircraft. It is only used operationally once the early failures have been 'shaken out' to the steady failure rate λ that is assumed to be constant.

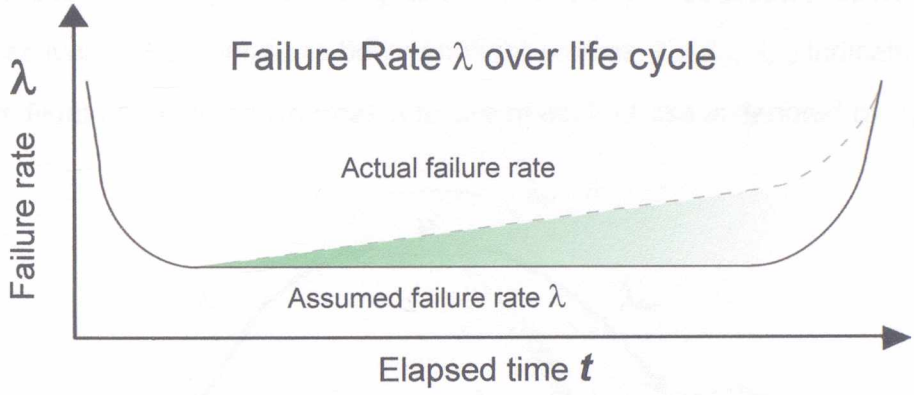


Figure 5.1: Actual and assumed failure rate of aircraft

In practice, because of factors such as wear and ageing of parts, the actual failure rate is often more like the upper 'real' curve of Figure 5.1; where the failure rate gradually increases as parts wear out and fatigue mechanisms become significant. The reciprocal of the diagram in terms of reliability is shown in Figure 5.2.

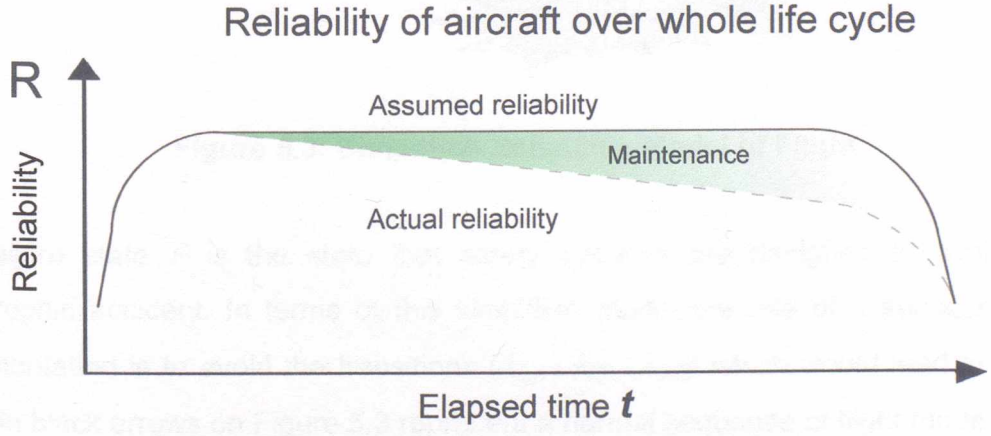


Figure 5.2: Actual and Assumed Reliability of Aircraft

The reliability of the aircraft has two components. Firstly the 'physical' reliability due to faults developing in its elements (engines, undercarriage etc); this depends to an extent of proper maintenance; secondly the reliability of its operational use. The aircrafts lifecycle is now modelled as a series of flights each with many small segments associated with a phase within the flight. This can be refined to describe the dependency between flight phases as the accident (failure) rate varies between flight phases, see section 3.2 and Figure 3.5 and 3.6.

5.1 A Reliability Model of a Flight

Reliability models are usually developed based on a number of assumptions and must take into account the resources available (and types of redundancy possible). An individual flight can be described by a simplified Markov chain model of flight safety [27], see Figure 5.3. For illustration three generalized *flight phases* are proposed: take off, in flight and landing, each phase having its own *probability* of successful completion: P_{to}, P_{if}, P_{lnd} respectively. The *transitions* between flight phases λ_{to}, λ_{if}, λ_{lnd} indicate a successful taking off, flight and landing whereas a failure of each phase is denoted by λ_{tof}, λ_{iff}, λ_{lndf}.

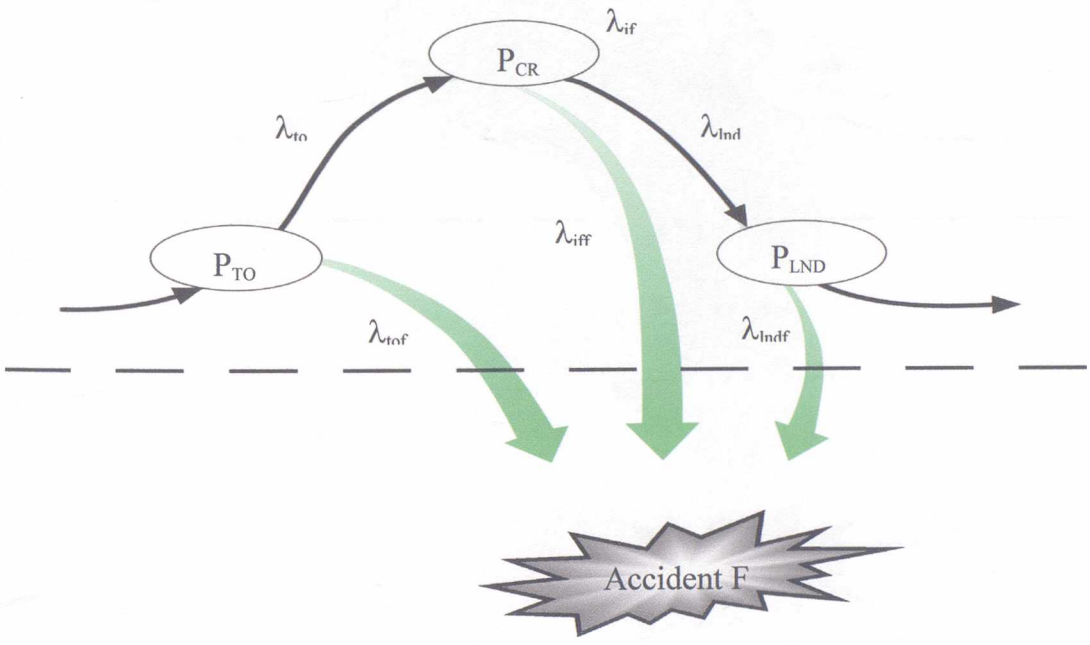


Figure 5.3: Simplified Reliability Model of Flight

The failure state F is the state that safety systems are designed to avoid, i.e., a catastrophic accident. In terms of this simplified model the role of a successful PASS implementation is to avoid the transitions (λ_{tof}, λ_{iff}, λ_{lndf}) which would lead to accident. The thin black arrows on Figure 5.3 represent a normal sequence of flight mode changes. The broader arrows are sequences of flight mode changes caused by emergencies and faults experienced by the aircraft and pilots; they represent the probabilities of accidents.

In terms of this model the successful completion of a flight assumes the normal sequential change of flight phases:

$$P_{success} = \Pi (P_{to}, P_{if}, P_{lnd}) \text{ and,}$$

$$P_{success} + P_{accident} = 1.$$

Then the ideal flight safety system in reliability terms has to exclude the probability of accident: so the goal is to achieve $P_{accident} \rightarrow 0$ or at least minimise it.

In practice the flight phases can be further refined as shown in Figure 5.4. This also shows some flight mode transitions that are not 'normal', for example:

- An emergency procedure involving a change from Take-off to Landing.
- An aborted Landing followed by emergency Take-off

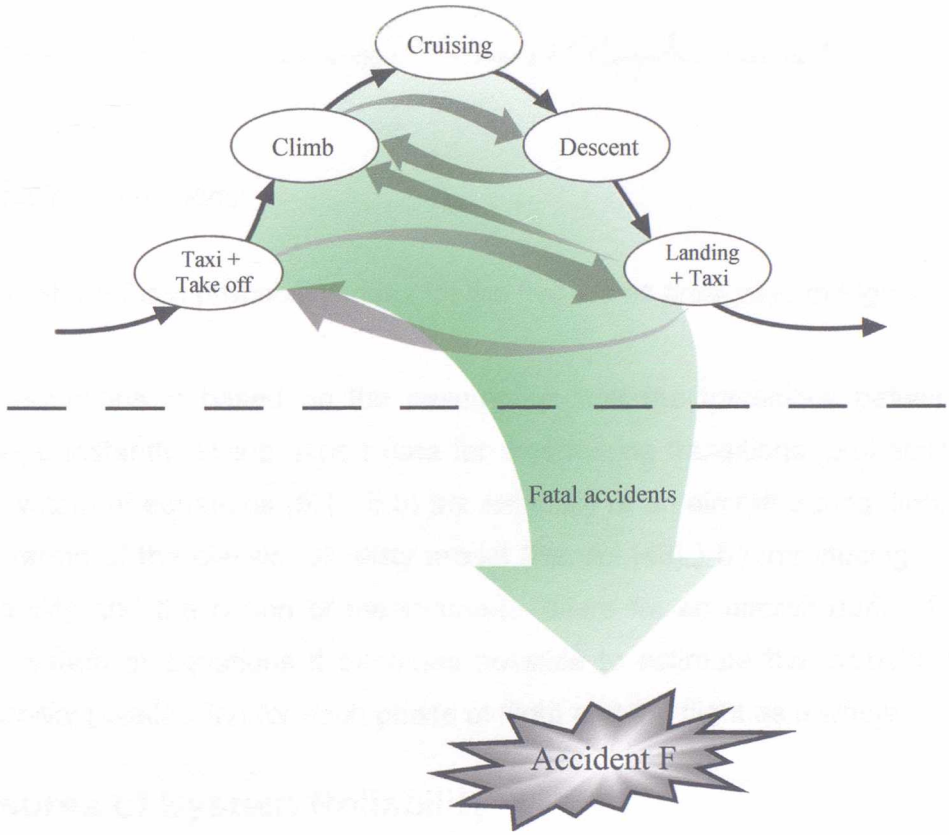


Figure 5.4: Flight mode Sequences and Interdependence

5.2 Operational Reliability Model Equations

The reliability of a flight is the product of the reliability of each of its flight phases. Assuming Markovian [63] properties for flight phases (and their changes) the set of equations below describe flight mode and transition probabilites using Kolmogorov [64] forward differential equations to characterise the transition rates between states:

$$\frac{dP_{taxi-out}(t)}{dt} = -P_{taxi-out}(t)(\lambda_{taxi-out-taxi-in} + \lambda_{taxi-out-c\lim b} + \lambda_{taxi-out-F}) + P_{taxi-in}(t)(\lambda_{taxi-in-taxi-out}) \quad (5.1)$$

$$\frac{dP_{c\lim b}(t)}{dt} = -P_{c\lim b}(t)(\lambda_{c\lim b-in-flight} + \lambda_{descent} + \lambda_{c\lim b-F}) + P_{taxi-out-c\lim b}\lambda_{taxi-out-c\lim b} + P_{descent}\lambda_{descent-c\lim b} + P_{taxi-in-c\lim b}\lambda_{taxi-in-c\lim b} \quad (5.2)$$

$$\frac{dP_{in-flight}(t)}{dt} = -P_{in-flight}(t)(\lambda_{in-flight-descent} + \lambda_{in-flight-F}) + P_{c\lim b}\lambda_{c\lim b-in-flight} \quad (5.3)$$

$$\frac{dP_{descent}(t)}{dt} = -P_{descent}(t)(\lambda_{descent-taxi-in} + \lambda_{descent-c\lim b} + \lambda_{c\lim bdescent-F}) + P_{in-flight-descent}\lambda_{in-flight-descent} + P_{c\lim b}\lambda_{c\lim b-descent} \quad (5.4)$$

$$\frac{dP_{taxi-in}(t)}{dt} = -P_{taxi-in}(t)(\lambda_{taxi-outt} + \lambda_{taxi-out-c\lim b} + \lambda_{taxi-out-F}) + P_{descent}\lambda_{descent-taxi-out} + P_{taxi-out}\lambda_{taxi-out-taxi-in} \quad (5.5)$$

and normalization conditions:

$\sum_{i=1}^{5} P_i + F = 1$ where i is a probability index for the five states presented in Figure 5.4.

This set of equations is based on the assumption that the transitions between flight phases change instantly. Using expert data for determining transitional probabilities and solving the system of equations (5.1 - 5.5) the reliability of an aircraft during flight can be analysed in terms of the classic reliability model (Birolini [48]) by introducing point and mission reliability and the notion of mean-time-to-failure for an aircraft during flight. By solving this system of equations it becomes possible to estimate the probabilities and thus the reliability (availability) for each phase of flight and the flight as a whole.

5.3 Measures of System Reliability

The classic measure of Mean Time To Failure (MTTF) and also the point and mission availabilities can also be derived from the equations above [64] and from classic reliability theory of Birolini [48]. However there is the issue of the relationship between availability and safety. Availability for an aircraft, which is not repairable in flight, is calculated as the sum of probabilities for each sequential flight phase from the beginning (taxi-out phase) to the end (taxi-in phase) of flight. Availability and reliability here are calculated assuming their sequential processing. There are two measures of availability that may be immediately useful in this respect, they are: *point availability* and *interval availability*.

5.3.1 Point Availability

The point availability $PA_0(t)$ is defined as *the probability that an aircraft is failure free and remains in the main (normal) phases of flight from the beginning of the flight up to the moment t of observation.* Assuming that the aircraft is new (i.e., 'as good as new' at each renewal point i.e., after maintenance) then the point availability is:

$$PA_0(t) = Pr\{up\ at\ t \mid new\ at\ t=0\} \tag{5.6}$$

Now if the probability of no failure in the interval $[0,t]$ is $1 - F(t)$, the probability that every renewal point lies in the interval $[x, x+dx]$ is $nnf(x)dx$ and $1-F(t-x)$ is the probability that no further failure occurs in the interval $[x,t]$ is $1-F(t-x)$ then the following holds at the end of the interval 0,t:

$$PA_0(t) = 1 - F(t) + \int_0^t nnf(x)(1 - F(t-x))dx \tag{5.7}$$

5.3.2 Mission Availability

The mission availability $MA_0(T_0, t_{flight})$ is defined as *the probability that in the mission of total operating time T_0 each failure can be repaired within a time span t_{flight}.* Hence, considering that the aircraft is 'as good as new' at $t = 0$,

$MA_0(T_0, t_{flight})$= Pr {each individual failure during the mission of total operating time T_0 can be repaired in time $\leq t_{flight}$ | new at t = 0} (5.8)

Mission availability is important for flight because interruptions of flight phase $\leq t_{fligh}$ might be necessary, for example the landing phase of flight might be interrupted and then take-off resumed. The only condition required to estimate mission reliability is that at the end of the period T_0, the total time of the flight, no failures have occurred. If $G(t_{flight})$ is the probability that all flight phase reiterations (loops) will be shorter than t_{flight}, and the failure rate is assumed constant and equal to λ, the mission availability is:

$MA_0 (T_0, t_{flight}) = e^{-\lambda T_0(1-G(t_{flight}))}$ (5.9)

5.3.3 Joint Availability

Joint availability $JA_0(t,t+\theta)$ gives *the probability of continued operation at the time points $(t, t+\theta)$.* Assuming that the aircraft is 'as good as new' at $t = 0$ then it is:

$JA_0(t,t+\theta)$ = Pr{ up at t $\cap$ up at t+θ | aircraft new at t=0} (5.10)

Again, assuming a constant failure rate the two events *"up at $t = 0$"* and *"up at $t+\theta$"* are independent (assuming Markov properties) then:

$JA_0(t,t+\theta) = PA_0(t)PA_0(\theta)$ (5.11)

Unfortunately, the estimation of availabilities described by in equations 5.8 to 5.11 does not consider failure rates for permanent faults and malfunctions separately. There is no doubt that a permanent fault of almost any main aircraft element would cause some kind of accident. However, malfunctions (caused by aircraft hardware, software, and user (pilot)) might be tolerated if some redundant resources are available to affect some level of effective reconfiguration. Therefore, analysis of safety and the safe completion of flight using classic availability definitions must be used with caution and carefully qualified.

The issue of different failure types, malfunctions and permanent faults, requires the introduction of conditional probabilities to differentiate them in equations 5.1 to 5.5; this unfortunately creates a substantial growth in the set of states describing aircraft conditions. Achieving a solution of these new equations during flight to produce some kind of index of reliability is indeed problematical. At the same time, having further details of failure "semantics" provided by after flight analysis in terms of reliability trends for an aircraft might be extremely useful for analysis of flight safety and relative involvement of all aircraft elements.

6 Theory and Modelling of PASS *in the large*

This chapter introduces a reliability model for the aircraft operational lifecycle based on further development of Birolini's methods [48]. The role of maintenance is analysed as well as the concept of improving overall reliability by applying the principle of active safety. The effect of applying PASS is modelled based on assessing and anticipating potential faults during the aircraft's longer term lifecycle of flights and maintenance sequences.

6.1 The Conditional Maintenance Cycle

Maintenance for GA aircraft should be performed periodically according to the schedule defined by the manufacturer, including intermediate checks based on the actual load of flights and also annual checks, for example see [92].

Even if an aircraft is properly maintained its operational safety takes no account of flight data. In other words the flight safety management system takes no account of information about faults that the aircraft may already have, or is developing. This creates a situation where the decision to use the aircraft for the next flight is taken *more or less on trust*. Note that the quality of certification depends heavily on the human factor such as experience and qualifications. Two idealistic approaches which might improve aviation safety are:

- changing human nature (i.e., unfounded optimism) or,
- changing the world (i.e., improving the quality of maintenance and upgrading landing strips to airfields with proper maintenance facilities).

Neither approach is realistic nor feasible!

What is possible is to provide automated processing of flight data from aircraft devices using existing and new information technologies. The objective is to provide the flight crew and aircraft operators with relevant information regarding the current state of the aircraft and enable correct decision procedures for each aircraft *before* each flight and each maintenance session. Additionally this procedure can run continuously on board and *make requests for servicing* when necessary. This concept is well known in aviation as "conditional maintenance", but is rarely used in practice. It is however used more and more widely in the automotive sector based on knowledge of wear of parts and the amount of use a vehicle has had [42]. The proposal is to use PASS, to implement an automatic safety monitor for aviation.

However, in order for a safety monitor to have any credibility it must be ultra reliable in three ways:

1. It must always be available, even if the aircraft is not serviced to schedule.
2. It must always offer safe and relevant advice based on the current situation and also based on previous flight data and analysis.
3. It must present action(s) to conserve or improve safety which is credible in its own right and transparent and clear to the operators, pilots and crew.

So far it has been assumed that it is 'common sense' that the only way to improve the availability of aircraft and maintain its safety level is by monitoring the aircraft's actual use and then advising on its future safe use. This introduces the notion of *Point Availability* i.e., the continuous and instantaneous assessment of the aircraft reliability. The first part of our proposal is to take into account and use current and accumulated flight data to assess point availability. Also in order to improve *Mission Availability*, i.e., the probability of successful completion of the flight, it is necessary to predict potential risks/faults and anticipate corrective or preventive action to improve the safety of operation. This can be achieved by using current and accumulated flight data along with knowledge regarding the potential faults and their relations to assess and improve mission availability.

6.2 Basic Philosophy: Preventive – vs- Active Safety

Aircraft fly in real time and therefore MASS, the implementation of PASS, must operate in real time in order to be effective. There are some systems that allow delays in decision-making procedures and which can accept latent (hidden) fault conditions before active phases of the application take place. In such systems some steps of the PASS algorithm might not need to be real time, for example steps A, B, D, E in Figure 4.5. Clear fully real time implementation would be highly desirable but it might be prohibitively expensive to achieve.

Before it can be understood and used the PASS algorithm requires a further detailed analysis of the methods and means for realising its steps. Note that the Algorithm of Fault Tolerance (as introduced in [40][55]) also has similar steps, even with similar names but a totally different meaning. The realisation of FT and PASS algorithms relies on redundancy in the system. Such redundancy, as described earlier might have several types [40], these types may also be used in implementation of various steps of the PASS algorithm to analyse behaviour of the object i.e., model the object's behaviour in the presence of fault(s). The limit of redundancy types has the effect of limiting the number of solutions available for the design, or re-design, of an object with new features.

Some systems that have not been designed initially as safe or that require greater safety can be improved if they can either be completely redesigned or if a new subsystem can

be added that will be able to measure, analyse and contribute to the safety of the main system. The obvious question is: *how can an active safety system and its safety monitor be connected with the reliability of an object?* A simplistic answer is that it identifies risk and therefore makes it possible to avoid risk (when feasible) and hence reduce harm and improve safety. A more substantial answer to this question follows.

The primary function of a Safety Monitor is the evaluation of quality and management of preventive maintenance. An aircraft is an object which in normal use has a cyclic operation and requires a preventive maintenance scheme to ensure its continued safe operation. The approach to periodic maintenance is based on assumptions about the guaranteed occurrence and high quality of maintenance which are sometimes quite naive and over-optimistic. Even when preventive maintenance does take place the state of the aircraft can be very difficult to analyse as, until now, there is no instantaneous evidence about its condition and devices before, during, and after flights. At the heart of the preventive maintenance approach is the notion that it is possible to gain a level of understanding and confidence about the aircraft's state by using and analysing a model of the elements from which it is composed. The aim here is to develop an aircraft model as a set of models of its key elements and then to make an estimation of its potential impact and efficiency for PASS implementation.

The approach taken is to:

1. Define the form of the probabilistic model for preventive maintenance.
2. Define a set of reasonable assumptions that relate to preventive maintenance.
3. Estimate the main factors that influence the period of preventive maintenance.
4. Investigate the impact of PASS on the policy of preventive maintenance.
5. To justify implementation of PASS we have to answer the following questions:
6. Can better reliability be achieved than with classic preventive maintenance?
7. Can the period of maintenance inspections be varied as a function of the condition of the aircraft proven/evaluated/estimated during flight by means of flight data processing?
8. What level of point availability for GA aircraft can be achieved?
9. What level of overall availability and mission availability can be achieved?

It is certain that full coverage of all possible faults cannot be achieved in practice. It is also certain that 100% level of confidence of our estimates cannot be guaranteed. So what can be done? Is it possible to provide a clear and substantial automatic coverage of faults and predict trends leading to possible faults to provide a basis for changing the

period of preventive maintenance? If this can be achieved to any significant extent and safety can be improved then the economic case for using PASS would be credible.

It is at least intuitively clear that implementation of PASS makes possible an increase in flight safety based on effective use of existing and real time flight data. It also supports required maintenance by location of possible faults, potentially reducing the turnaround inspection time and the level of qualification of maintenance personnel involved. It may also have an impact on the *design* of aircraft by checking the design as it evolves using PASS techniques. A benefit of this approach would be that aspects of the aircraft safety could be evaluated at the design stage when changes to the design have a relatively low cost. Once the production and operational stage are reached then changes to the design and retrofitting of parts becomes extremely expensive.

6.3 Reliability Modelling and Maintenance

The purpose of maintenance is to improve the reliability and availability of the system. Three strategies are considered to achieve this: preventive, conditional and PASS assisted maintenance.

Preventive maintenance is carried out to pre-empt failures due to factors such as wear and tear and aging. A description and analysis of it is included in Appendix 7 section 19.1.1. Immediately after maintenance there is an apparent improvement in reliability, this is illustrated in Figure 6.2; the gradual degradation is due to the fact that maintenance does not restore the reliability to the 'as new' level.

Conditional maintenance takes account of the current condition of the item being maintained based on some criteria. When the criteria are met then the maintenance is performed, in this way maintenance can be tailored more closely to actual needs resulting in a variable time between maintenance activities. A description and analysis of it is included in Appendix 7 section 19.1.2.

PASS assisted maintenance is where PASS is used to monitor the fault status of the system during its operation and to contribute to the criteria for initiating maintenance. So PASS introduces a new process in aircraft management: *on-line checking of the aircraft's fault status and safety condition*.

Preventive maintenance is necessary to avoid failures and defects due to wear and tear, i.e., due to wear and aging of materials and the effects of utilisation. Its aim is to anticipate, locate latent (hidden) faults and arrange to avoid their occurrence in a timely way and thus avoid actual fault occurrence. The so-called latency of the fault here is considered to be the phenomena of the possible presence of a hidden fault or trend of a parameter which is related to a fault (or faults). Latency is also about the situation when a

fault is not detected fully i.e., it exists but is not yet apparent in its effect e.g. when the aircraft is used in limited modes of flight or recorded variables are not representative etc.

Initially, to investigate the properties of preventive maintenance, let us consider a simple model. An aircraft as a repairable structure with periodic preventive maintenance at T_{PM}, $2T_{PM}$,..., when the aircraft was 'new' $t = 0$. The aircraft's failure free time is a distributed function *(d.f)* $F(t)$ accordingly with density $f(t)$; assume that repair time has the distribution *d.f* $G(t)$ with density $g(t)$. Initially we analyse the aircraft reliability assuming that the elapsed time of preventive maintenance is negligible in comparison with the time of aircraft operation – this is quite a realistic assumption as roughly 300 flight hours correspond to 0.5 hours of maintenance in GA.

6.3.1 Classical Preventive Maintenance

The assumption that negligible time is taken for preventive maintenance is that it only occurs when faults become apparent and are notified. Four options are possible here:

1. PM is not performed and the aircraft is considered as-good-as-new.
2. PM is not performed and the aircraft is considered as unsuitable for further flights (e.g. because some resource necessary for flight is exhausted).
3. As a result of testing procedures the aircraft is considered not to be flight worthy due to insufficient test completeness or trustworthiness, so PM is not performed.
4. The aircraft is considered to be potentially not flight worthy and PM is performed instead of a full-scale repair.

The fourth assumption is now explored: the reliability of the aircraft has renewal points (at times 0, T_{PM}, $2T_{PM}$, $3T_{PM}$, $4T_{PM}$,...,) and at these points it is considered to be 'as good as new'. So, the reliability function without preventive maintenance is [48]:

$$R(t) = 1\text{-}F(t) \qquad (6.1)$$

where $F(t)$ is the distribution function of the failure-free operating time of a single item structure and, for simplicity, it is assumed that it is represented by the exponential distribution $F(t) = 1 - e^{-\lambda t}$ in the period t of operation. Introducing preventive maintenance changes the form of the reliability function for the aircraft as follows:

$$R_{PM}(t) = R^n(T_{PM})R(t\text{-}nT_{PM}) \text{ for } nT_{PM} \leq t < (n+1)T_{PM} \text{ and } n \geq 1 \qquad (6.2)$$

If the system has no maintenance or repair then its reliability in its simplest form (assuming the rate of fault occurrence is constant) can be presented by the classic reliability function. For this case the reliability function is given by equation 6.3:

$$R(t) = e^{-\lambda t} \qquad (6.3)$$

where $R(t)$ is the reliability of a system, and λ is a parameter or function of the system's features, in this case the set of faults. The reliability curve is then illustrated in Figure 6.1, here with $\lambda = 0.3$ and time parameter $t = [0...10]$.

It has the form of the classic reliability function, where the curve is the reliability with a threshold Ro superimposed as a horizontal line. The intersection of the curve and threshold represents the case where when Ro is reached the system is taken out of service. The threshold function Ro introduced on Figure 6.1 represents the minimum level of system reliability required to continue operation. Here with $Ro = 0.2$ the reliability approaches the threshold Ro at time 5.4.

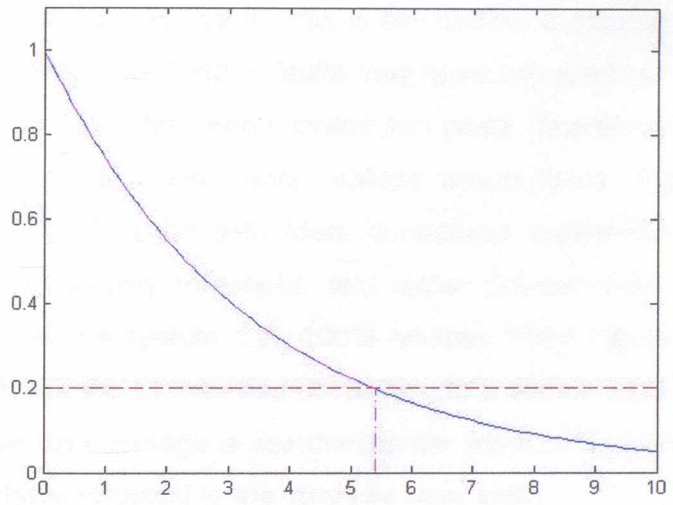


Figure 6.1: The Classic Reliability Function

However this particular example is far from reality; aircraft in modern management schemes are assumed to be serviced when their condition reaches a certain level, this approach is well documented [69], [70] and is widely known as conditional maintenance. Such evaluation is generally optimistic as it assumes that maintenance is ideal, eliminating all possible faults in the aircraft, and that the aircraft does not change its condition except with the constant rate λ. This makes it possible to set maintenance procedures periodically, at times when the model shows that reliability has probably reached the necessary point for maintenance.

Note that these assumptions of perfect maintenance, constant failure rate and minimum level of reliability are combined to define the size of intervals between maintenance activities. In practice all these intervals tend to be equal. Formally, the Reliability Function for Conditional Maintenance is based on the following assumptions:

Assumption 1: 100% coverage i.e., maintenance restores the system completely.

Assumption 2: The interval between two successive maintenance inspections is constant

Assumption 3: Maintenance is instantaneous, not delaying the aircrafts use schedule.

Suppose the reliability function is given by:

$$R(t) = e^{-\lambda(t-nT_{PM})}, \quad nT_{PM} \leq t < (n+1)T_{PM} \tag{6.4}$$

where n corresponds to the n-th maintenance inspection, and n = 0 means the system is just deployed or considered to be 'as good as new'. The reliability curve is then illustrated in Figure 6.2 where the assumptions about λ are the same as above. Here conditional maintenance is assumed periodic and restores the system to the state 'as good as new'. For aviation this reliability model is quite optimistic and can at best only serve as a guide: firstly intervals between maintenance inspections are rarely equal because an aircraft is now used heavily e.g. in chain flights. In GA aircraft suffer from sporadic and far from perfect maintenance, the main cause for this is the human factor, i.e., the maintenance personnel and pilot. Additionally, hidden faults may have occurred but the latency period for various types of fault range between minutes and years. Therefore the reliability of an aircraft needs to be analysed with more realistic assumptions. Figure 6.2 gives an example of the reliability function with ideal conditional maintenance, the horizontal dashed line is the acceptability threshold, and upper dot-and-dash line indicates the perfectly reliable state of the system, i.e., 100% reliable. From Figure 6.2, one can see that, when the reliability of the system has decreased to a certain level then maintenance is carried out. Because full coverage is assumed under ideal conditional maintenance the system is deemed to have returned to the 'good as new' state.

6.3.2 Conditional Maintenance with Incomplete Coverage

Firstly we introduce an assumption that coverage, a measure of maintenance quality denoted as α, is not perfect. The reliability function assumptions are formally presented below for conditional maintenance with incomplete coverage:

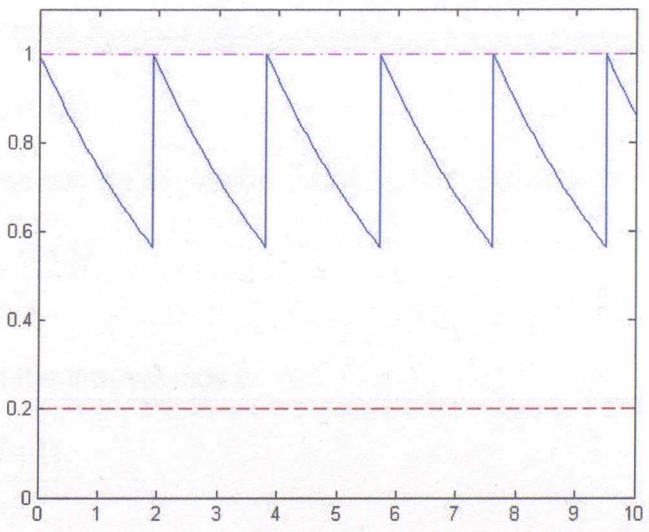


Figure 6.2: Reliability Function with Ideal Conditional Maintenance

Assumption 1: Coverage is not 100%. Coverage percentage is $100\alpha_M\%$, where $0<\alpha_M<1$ and is assumed to be constant over the whole lifespan of the aircraft and represents the gradual degradation of the effectiveness of maintenance of the system.

Assumption 2: Maintenance is instantaneous, not delaying the aircraft use schedule.

Assumption 3: A threshold of acceptable reliability R_0 exists for $R(t)$.

Assumption 4: T_{PM} is not a constant but a variable, actually, a function of several variables, including α, λ and R_0. Reliability is then calculated according to:

$$\begin{cases} R(t)=\alpha^{(n-1)}e^{-\lambda(t-\sum_{i=1}^{n}T_{PM}(i))}, & \sum_{i=1}^{n}T_{PM(i)}<t \\ R(\sum_{i=1}^{n}T_{PM}(i))=R_0, & n=1,2,\ldots,m \end{cases} \tag{6.5}$$

The resulting reliability curve for this case is presented in Figure 6.3. It is now assumed that maintenance takes place when the system (an aircraft) reaches the threshold reliability i.e., when R(t) $\geq$ R_0.

This case has some theoretical interest, as it might be useful to analyse the role of all the variables that define behaviour of period of maintenance T_{PM}. Calculating $T_{PM}(i)$, for i = 1,2,...,n, and taking into account the role of the other variables such as R_0 and α; then T_{PM} (i) is given as:

$$T_{PM}(i)=-\frac{1}{\lambda}\ln R_o\alpha^{(1-(i-1))} \tag{6.6}$$

This model is more realistic; in principle it is now possible to schedule maintenance when the threshold of acceptable reliability is reached. Note that the interval between maintenance inspections is shrinking significantly:

$$\Delta T(i)=T_{PM}(i)-T_{PM}(i+1) \tag{6.7}$$

The relative decrease can be evaluated by the rate of decrease of $T(i)$:

$$\Delta T(i)=\frac{T_{PM}(i)-T_{PM}(i+1)}{T_{PM}(i+1)} \tag{6.8}$$

or by the function of the interval index:

$$\Delta T=\frac{T_{PM}(i)-T_{PM}(i+1)}{i} \tag{6.9}$$

Figure 6.3 shows the reliability function under conditional maintenance with incomplete coverage using the previous assumptions. In Figure 6.2, once the threshold was reached, maintenance was carried out. But now, because of incomplete coverage, the reliability of the system can not return to 100% after maintenance, and the amplitude of coverage the maintenance can achieve gradually reduces over time.

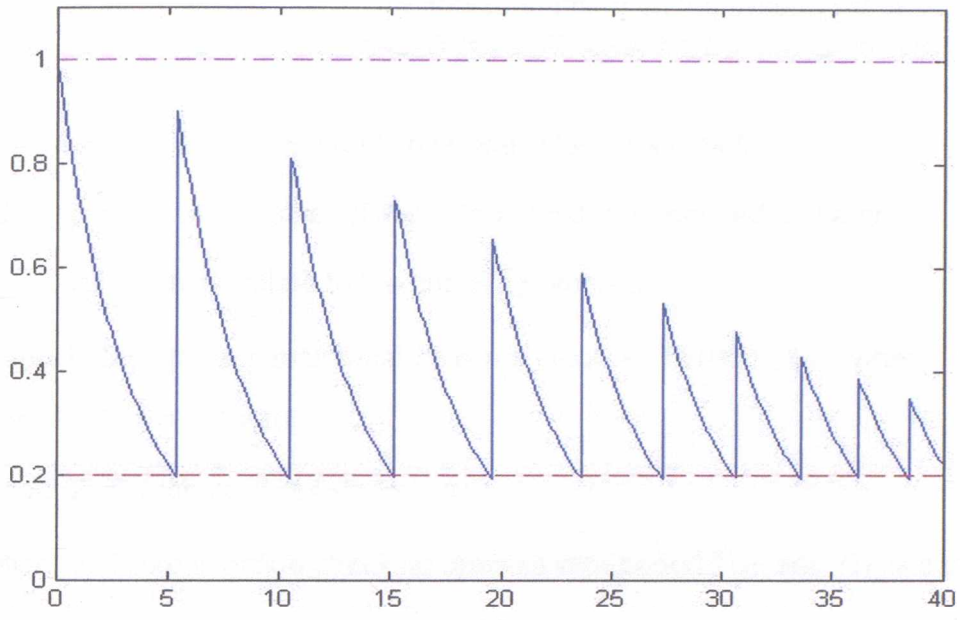


Figure 6.3: Conditional Maintenance with Incomplete Coverage

The actual condition of aircraft use depends on the defined reliability threshold R_o and the interval between two sequential maintenance inspections when the mean mission (flight) duration approaches ΔT. When the aircraft reliability approaches R_o just after a flight it should be grounded in the interests of safety.

6.3.3 Preventive Maintenance with Implementation of PASS

So PASS introduces a new process in aircraft management: *on-line checking of the aircraft's fault status and safety condition*. On-line checking is a process of checking of the aircraft's main elements in real time, including aircraft hardware (in general), avionics and pilot during the flight. The aim of checking within the system is detection of degradation or change in *behaviour* and, if and when possible, *corrective* recovery of the suspected element and therefore conservation of the system's reliability. When recovery is not possible the *preventive* nature of PASS promotes actions to reduce the level of danger, risk etc – aiming for graceful degradation of service to the aircraft's users.

The process of checking reliability degradation and the process of maintenance are of course independent in principle so they can be considered concurrently or sequentially. Each activity can be started when required, when possible or just when convenient. The

main idea here is to perform checking well in advance when current reliability R_T is higher than threshold reliability and in such a way that during T_{PC} the aircraft does not reach the threshold reliability i.e., during a flight. What is interesting here is that the processes of checking and preventive maintenance when combined change the estimated reliability of the system. The gradient of this change is a function of the quality of checking (coverage) and the quality of maintenance.

When considering the impact of PASS implementation on the system we assume:

1. a constant failure rate,
2. maintenance is not ideal and coverage is less than 100%,
3. the minimum acceptable reliability threshold is introduced as before.

Some other assumptions relate to the checking process:

Assumption 1: Coverage of maintenance is not ideal i.e., is $100\alpha_M\%$, where $0<\alpha_M<1$ and is assumed as a constant.

Assumption 2: Threshold R_0 exists for $R(t)$.

Assumption 3: There is online checking process with period T_{PC}, and T_{PC} is a constant.

Assumption 4: After each online checking, the confidence about the system's conditions is increased, therefore $R(t)$ is also increased, and this confidence is $100\alpha_C\%$, while $0<\alpha_C<1$ and α_C is a constant.

Assumption 5: The period between two successive maintenance inspections is $T_{PM}(i)$. $T_{PM}(i)$ is a variable, actually a function of i, R_0, α_C, α_M, λ and T_{PC}.

The reliability function for the aircraft is then calculated according to:

$$R(t)=R_I\alpha_C{}^{(n-1)}e^{-\lambda(t-nT_{PC})}, \qquad nT_{PC}\le t<(n+1)T_{PC} \tag{6.10}$$

For $R(t)$ in equation 6.10 signifies the n-th on-line checking period, and n_{FAM} signifies the first online checking period after the latest maintenance inspection, i.e., the n_{FAM} th on-line checking period. For a brand new system, $n_{FAM}=0$. R_I is the initial value of reliability at the beginning of a maintenance period, or the reliability level as reassessed after the latest maintenance inspection has been carried out, so $R_I=1$ for a brand new system. After that, R_I gradually decreases over time because the coverage of maintenance is not 100% and there is a continual natural ageing process at work.

Actually, R_I can be calculated by an equation like:

$$R_I(i) = \alpha_M{}^{i-1} \tag{6.11}$$

where i corresponds to the i-th maintenance period. It is easy to see that R_I denotes the initial value of reliability at the beginning of *a maintenance period*, while $R_I\alpha_C{}^{(n-n_{FAM})}$ denotes the initial value of reliability at the beginning of an *online-checking period.*

When the reliability of the aircraft reaches the threshold R_o it should be grounded awaiting maintenance, and so:

$$R((n+1)T_{PC}) \le R_0 \tag{6.12}$$

From a practical point of view, the online checking period should be constant, and the checking procedure should start at the end of each online checking period, in other words at the beginning of the consecutive period. Suppose the checking takes (relatively) no time, and maintenance will be immediately carried out when $R((n+1)T_{PC}) \le R_0$.

Even if a time delay due to the checking process has to be considered, we still assume that the maintenance is carried out only at the end of the following online-checking period. This means the maintenance period is composed of a certain number of online-checking periods. Let index n be the serial number of an online-checking period, and index i be the serial number of a maintenance period, the online-checking period T_{PC} and the maintenance period $T_{PM}(i)$ are the points of interest. The difference and relationship between T_{PC} and $T_{PM}(i)$ is that:

the online-checking period T_{PC} is a constant, whereas the maintenance period $T_{PM}(i)$ is a variable;

$T_{PM}(i)$ contains a certain number of T_{PC}.

$$\begin{cases} T_{PM}(i) = (n+1)T_{PC} - T_{PM}(i-1), & i > 1 \\ T_{PM}(i) = (n+1)T_{PC}, & i = 1 \end{cases}$$

$R(t) = R_I\alpha_M$ then $R_I = R(t)$. (6.13)

Under these assumptions the reliability function is then illustrated on Figure 6.4 which shows the reliability function for preventive maintenance with on-line checking, where the solid curve is the reliability curve, the lower line is the threshold, and the upper line indicates the 'as new' reliability of system. During each online checking period the latest system states are measured and analysed to provide an awareness and confidence about the reliability of the system (subject to no faults being detected). When the nominal

reliability reaches the threshold, maintenance is carried out just as with conditional maintenance in Figure 6.3.

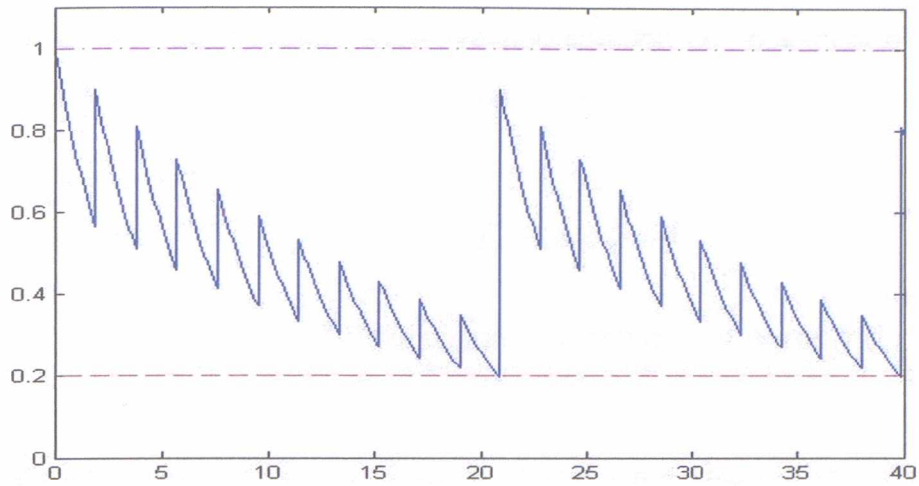


Figure 6.4: Preventive maintenance using on-line checking

When no maintenance takes place for a long time (the actual situation in GA) the reliability of the aircraft will reach the lower threshold R_o. The rate of reliability decrease is in fact faster than with on-line checking. The gap of confidence between a point in time before and after checking is now referred to as a *corridor of confidence* or, more exactly, a *corridor of reliability. It is the safe operational area where the reliability curve is normally expected to stay during operation of the online-checking scheme.*

6.4 The Reliability Corridor – introduction and definitions

The basic model of a reliability corridor δ is defined using practical assumptions and a set of scenarios as in the previous sections. The reliability corridor provides an estimate of where the reliability (curve) could reach in each on-line checking period, and therefore could effectively help to decide when maintenance is necessary in order to avoid violating the given reliability threshold. On the other hand, the 'width' of the reliability corridor will help to define the requirements for software and hardware in terms of allowable data processing time delays. The corridor is plotted in Figures 6.5 to 6.10 using the same layout conventions as before. The limits of the corridor are shown with dotted lines above and below the reliability trace on the graphs.

Definition 1: In each online checking period, the width of the corridor δ is a constant and does not depend on time. During the n-th online checking process the reliability corridor $\delta(n)$ is a function of n and given as:

$$\delta(n) = R(nT_{PC}) - R((n+1)T_{PC}) \qquad (6.14)$$

Clearly the corridor under this definition becomes too conservative at the end of each online checking period because the amplitude of coverage by on-line checking shrinks as time goes on, as illustrated in Figure 6.5.

Definition 2: Here we introduce a time-varying corridor, i.e., the width of the corridor δ varies over time within each online checking period. $\delta(t)$ for the nth online checking process is given as:

$$\delta(t) = R(nT_{PC})\alpha_C^{(t-nT_{PC})/T_{PC}}(1-e^{-\lambda T_{PC}}),\ nT_{PC} \le t < (n+1)T_{PC}. \qquad (6.15)$$

Actually, $R(nT_{PC})\alpha_C^{(t-nT_{PC})/T_{PC}}$ in equation 6.15 defines the upper limit of the corridor at time t.

Assume a ghost system has a reliability of the same value at the upper limit of the corridor at time t, then $R(nT_{PC})\alpha_C^{(t-nT_{PC})/T_{PC}}e^{-\lambda T_{PC}}$ is the reliability of the ghost system after an online checking period T_{PC}. The width of the corridor at time t, $\delta(t)$, equals the difference between the upper limit of the corridor at time t and the reliability of the ghost system at time t + T_{PC}. It is evident that the width of corridor varies over time. The resulting corridor of the reliability curve is illustrated in Figure 6.6 where the corridor more closely matches the reliability curve compared with Figure 6.5 and crosses the lower threshold later. Note also that with each major cycle the best reliability achievable gradually decreases.

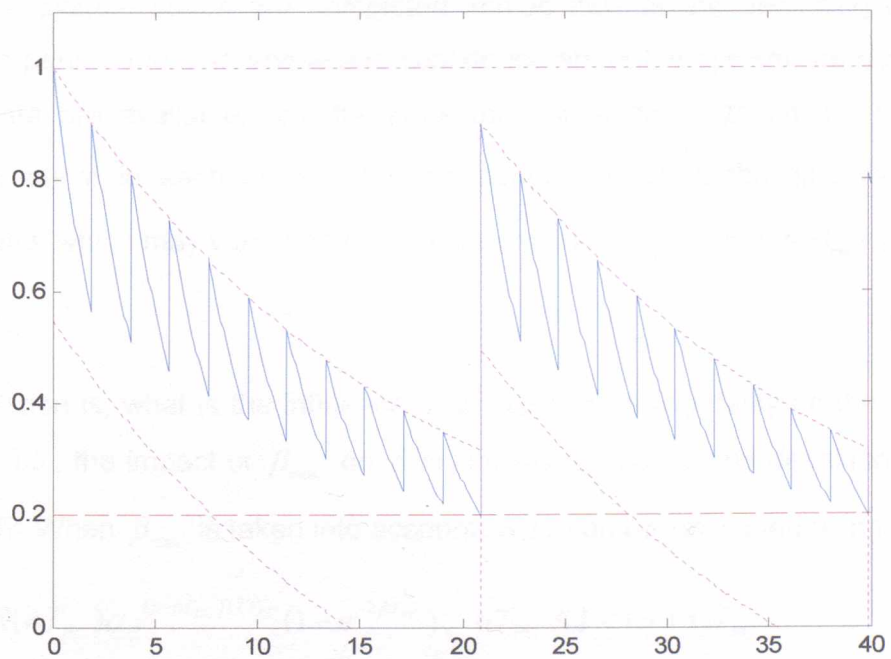


Figure 6.5: Reliability Corridor as a Function of Number of Iterations

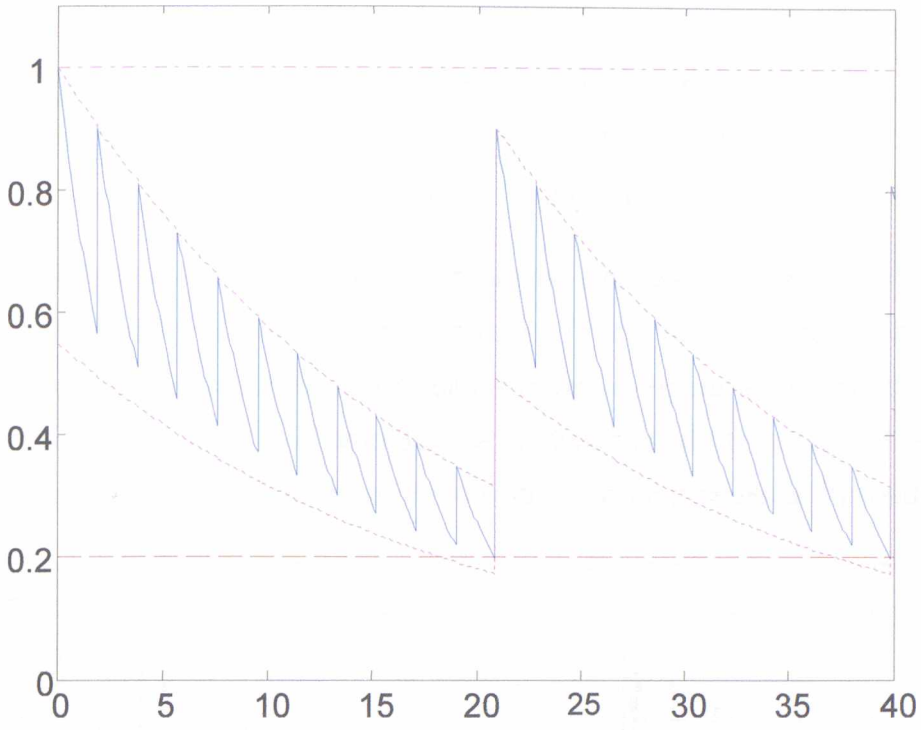


Figure 6.6: Reliability Corridor as a Function of Time

6.4.1 Defining the Frequency of the Checking Process

Assumption 1: Online checking process starts at the beginning of each online checking period. Due to the time consumed by online data processing, the real reliability curve is more like that illustrated in 6.7, where the dotted vertical lines indicate each on-line checking period, in this case 2-time-units long. Because the measurement and analysis of the latest system states are completed immediately at the beginning of each on-line checking period, the awareness and confidence about the system are not improved until these data are available, and therefore there is a delay β on the coverage of the reliability curve in each online checking period. So β is the time required for data processing, which may vary, and has an upper bound $\beta_{\max}$ and $\beta \leq \beta_{\max}$; at worst:

$$\beta_{\max} = T_{PC} \tag{6.16}$$

The question is, what is the influence of a data processing delay on the definition of the corridor, i.e., the impact of $\beta_{\max}$ on $\delta(t)$, assuming the second definition of a corridor is adopted? When $\beta_{\max}$ is taken into account, $\delta(t)$ can be calculated using:

$$\delta(t) = R(nT_{PC})\alpha_C{}^{(t-nT_{PC})/2T_{PC}}(1-e^{-2\lambda T_{PC}}), \quad nT_{PC} \leq t < (n+1)T_{PC} \tag{6.17}$$

Compared with T_{PC} in equation 6.15, $2T_{PC}$ in equation 6.17 embodies the maximum delay due to online data processing of the data collected in real-time from the aircraft. In

practice the cycle time of data processing (once per second) will be much smaller than any realistic maintenance period (days to months).

6.4.2 *Avoiding R_0 being breached when a Delay Occurs*

For PASS to be practical it is crucial that the reliability should not fall below the threshold R_0 even in when $\beta_{\max}$ is taken into account. This could be achieved in one of three ways:

Method 1: Within each online checking process, after data processing is finished, check whether the reliability is below the threshold R_0. In this case, due to the delay caused by data processing, the threshold could still be violated. Figure 6.7 shows that when online checking is carried out (e.g. at time 30) the modelled reliability is above the threshold but then goes below the threshold when the online checking process is finished at time 32.

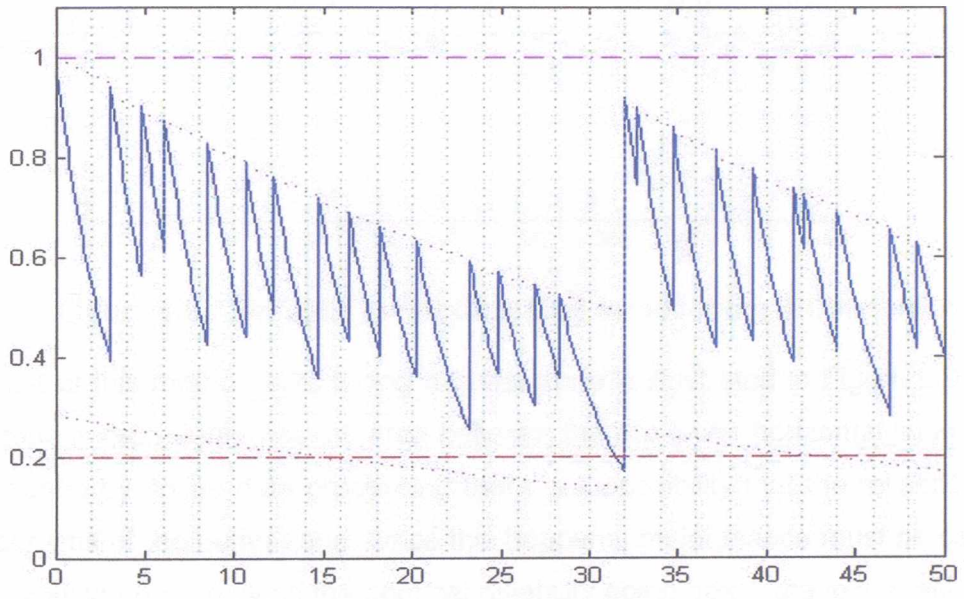


Figure 6.7: Reliability with Calculation after Checking Period

Method 2: In each online checking process, check whether the bottom line of the corridor is below the threshold R_0, i.e.:

$$R_1 \alpha_C^{(n-n_{FAM})} \alpha_C^{rem(t,T_{PC})/T_{PC}} - \delta(t) \leq R_0 \qquad (6.18)$$

where the first term on the left hand side of the relation defines the top of the corridor, and "rem" signifies the remainder after dividing t by T_{PC}. The result of applying this method is illustrated in Figure 6.8. The maximum delay, i.e., T_{PC}, is taken into account when defining the width of corridor in (equation 6.17) so that the reliability is always covered by the corridor even when there is data processing delay. Consequently the reliability never reaches the lower threshold because maintenance is carried out in time before the bottom of corridor reaches the threshold.

Method 3: Define a buffer zone, i.e., $[R_0, R_B]$ then in each online checking process, check whether the reliability is within the buffer zone, i.e.,

$$R((n+1)T_{PC}) \leq R_0 + R_B \tag{6.19}$$

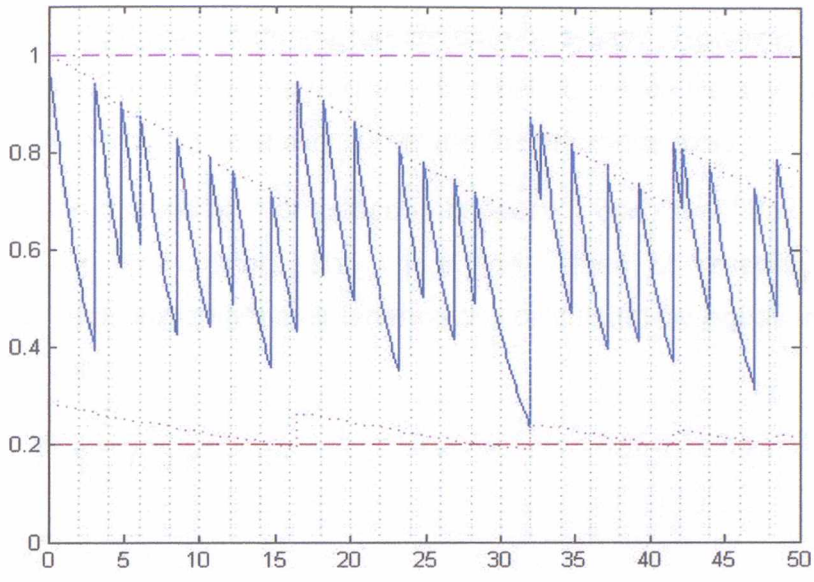


Figure 6.8: Reliability with Checking for reaching Threshold R_0

The result of this method introducing a buffer zone is illustrated in Figure 6.9, where the buffer zone is represented as the area between the two lower horizontal lines. Due to the delay caused by online data processing there is a possibility that the reliability fall below the upper limit of the buffer zone. Once this happens, maintenance must be carried out in a timely way in order to avoid the nominal reliability going below the low threshold limit.

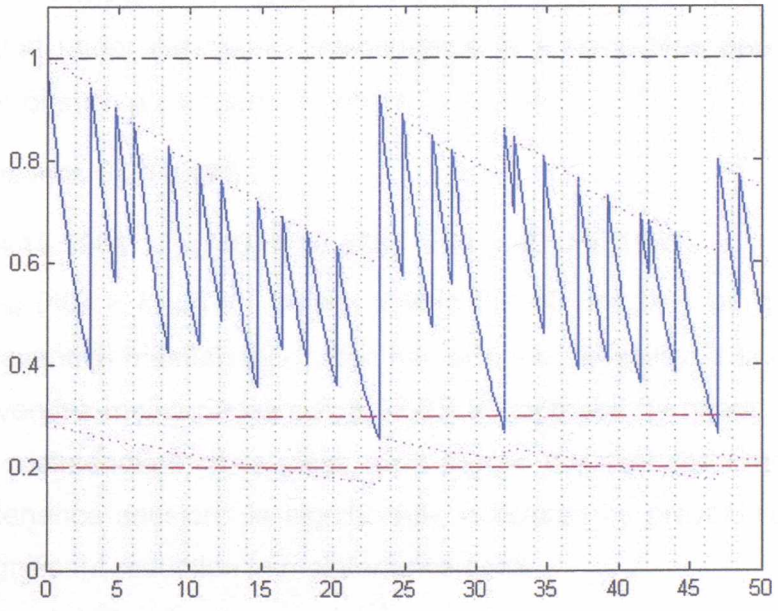


Figure 6.9: Reliability with checking in buffer zone

6.5 Conditional Maintenance versus PASS

From the previous sections it should be evident that preventive maintenance is more efficient than conditional maintenance. The quantitative analysis in this section will help to make the picture clearer. First of all, some criteria are needed in order to carry out a fair comparison. For example, the time between two successive maintenance sessions, the lifespan of the system under a certain maintenance strategy, and how many times maintenance is carried out during the life time of system. However an effective index is the integration of reliability over a given time period, which literally means the volume of the area enclosed by the reliability curve and the reference axes.

The key reason this index is proposed is because it can reveal how reliable a system is during a given time period. The integration values of reliability under conditional maintenance and preventive maintenance are calculated by equation 6.20 and equation 6.21 respectively:

$$V_{CM}(T_1) = \int_0^{T_1} R_{CM}(t)dt \qquad (6.20)$$

$$V_{PM}(T_2) = \int_0^{T_2} R_{PM}(t)dt \qquad (6.21)$$

Where $R_{CM}(T)$ and $R_{PM}(T)$ are given by equations 6.5 and 6.10.

The improvement of efficiency of preventive over conditional maintenance can be assessed from:

$$y(T_1, T_2) = \frac{V_{PM}(T_2) - V_{CM}(T_1)}{V_{CM}(T_1)} \qquad (6.22)$$

First, let $T_1=T_2$, this means the reliability of system under preventive maintenance is compared with that under conditional maintenance in a same time period. Figure 6.10 gives an example of such a comparison, where $T_1=T_2=40$.

According to equations 6.20 and 6.21 :

$V_{CM}(40) = 15.5961$, $V_{PM}(40) = 18.5084$ and $y(40) = 0.1867$

The fact that V_{PM} (40) > V_{CM} (40) means that in the 40 unit time period specified the system under preventive maintenance often has a higher reliability. It is evident that the efficiency of preventive maintenance using PASS is improved by nearly 20% compared with conditional maintenance. It is clear from Figure 6.9 that the time between two sequential maintenance sessions is significantly increased by preventive maintenance, which infers a significant reduction in maintenance costs.

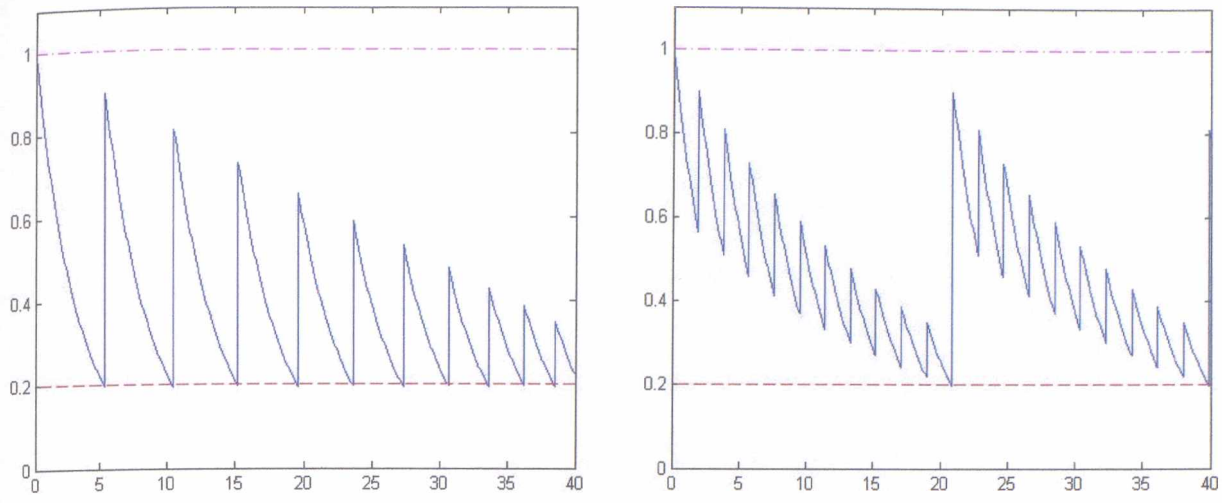


Figure 6.10: Efficiency of Conditional and Preventive Maintenance

Let $T1$ and $T2$ be the lifespan of the system under preventive maintenance and conditional maintenance respectively. Then the value of y in equation 6.22 can be used to assess how much gain in reliability is created by the adoption of preventive maintenance relative to a conditional maintenance scheme. For example under the conditional maintenance the reliability curve will be no longer able to recover after the time 44.6, whereas under the preventive maintenance, the critical time is 129.1. It follows that:

$V_{CM}(44.6) = 16.6707$ and $V_{PM}(129.1) = 50.2670$, and so

$$y = \frac{V_{PM}(129.1) - V_{CM}(44.6)}{V_{CM}(44.6)} = 2.0153.$$

In this sense, the efficiency of preventive maintenance is improved by over 200% compared with conditional maintenance. Figure 6.11 shows the result in a more intuitive form. The indexes defined in equations 6.20, 6.21 and 6.22 can be extended to compare preventive maintenance with the classical reliability function. Firstly comparing them in the same time period, as illustrated in Figure 6.12, based on equations 6.20 and 6.22:

$V_{CRF}(40) = 3.3336$ and $V_{PM}(40) = 18.5084$ and so

$$y(40) = \frac{V_{PM}(40) - V_{CRF}(40)}{V_{CRF}(40)} = 4.5521$$

Then the reliability preventive maintenance gained can be calculated compared with the classic reliability function. Since the classical reliability function reaches the threshold at the time 5.4, it is apparent that under the preventive maintenance curve will no longer able to recover after the time 129.1, and then one has:

$V_{CRF}(5.4) = 2.6739$ and $V_{PM}(129.1) = 50.2670$ and so

$$y = \frac{V_{PM}(129.1) - V_{CRF}(5.4)}{V_{CRF}(129.1)} = 17.7991.$$

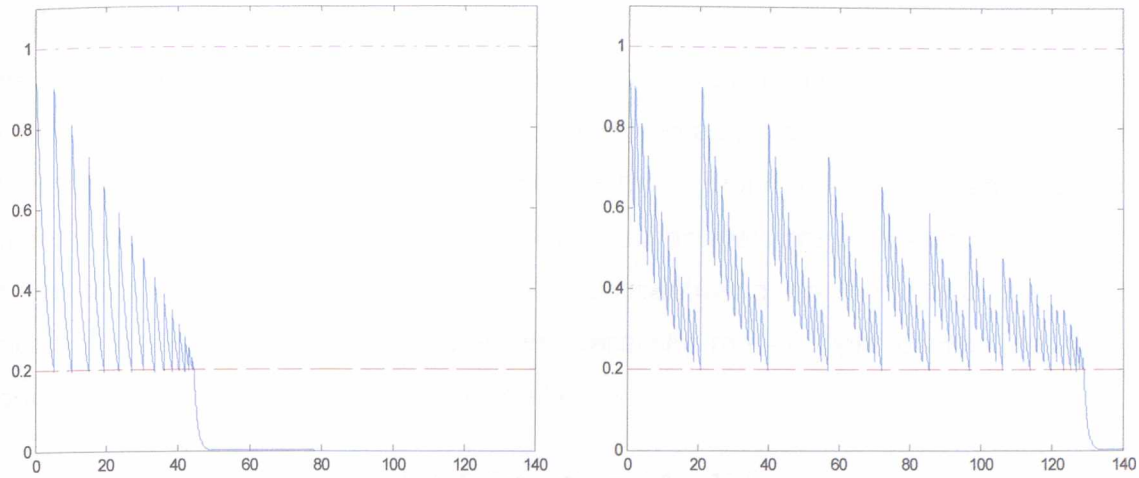


Figure 6.12: Conditional and Preventive Maintenance Efficiency

The significant advantage in efficiency of preventive maintenance when compared with the classical reliability function is illustrated in Figures 6.13 in the shorter term and in Figure 6.14 over the whole operational life of the system.

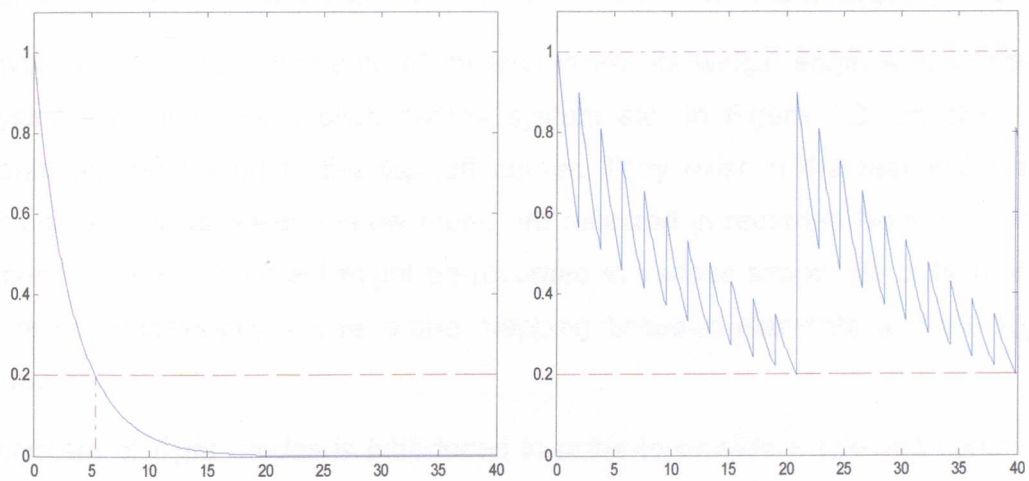


Figure 6.13: Classical Reliability versus Preventive Maintenance

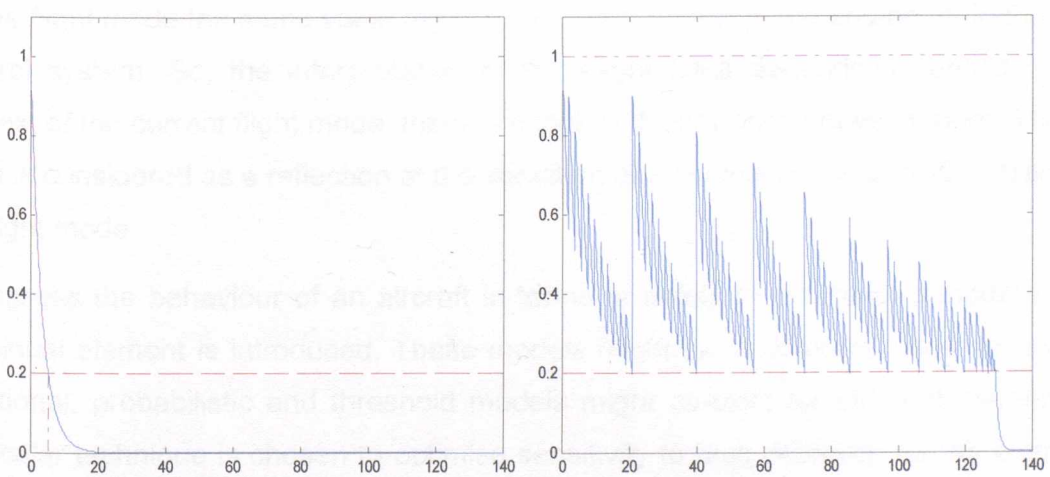


Figure 6.14: Classical Reliability versus Preventive Maintenance over Lifecycle

7 PASS *in the medium*

This chapter sets out the theory behind PASS in the medium, i.e., how information-driven, conditional flight safety monitoring can be implemented for aircraft. First of all, the flight information model is introduced then schemes for flight information flow and processing are described. The basic techniques for flight data analysis are developed, with the need for real-time flight data analysis in mind, concentrating on the operational aspects including: the flight information model, the reliability model, flight phases, reliability of prognosis, and also point and mission availability.

7.1 A Process Oriented Information Model

The implementation of PASS assumes that some aspects of the condition of an aircraft can be predicted using flight data and thus some events that would reduce safety can be avoided. Figure 7.1 presents the structure of the models that support MASS; comprising an object (in this case, an aircraft), its elements, the functional models of the elements, the operational flight modes, real-time flight data, predicates of an object and element states, a dependency matrix defined on the object elements and a recovery matrix. .

The typical component elements of an aircraft are its wings, engines, generators, fuel subsystem, landing gears, pilot, control system etc. In Figure 7.2, an object and its elements are presented in the top left corner. They exist in the real world and their conditions, as far as we can know them, are reflected in recorded flight data. Note that the condition of one element might be recorded in various snapshots of flight data, i.e., there is not necessarily a one-to-one mapping between elements and the flight data recorded.

The concept of *flight modes* is introduced in order to provide a relevant context for the particular risks associated with different phases of flight and also to gain sensitivity in the detection of faults between expected and actual operational behaviour. For example, an engine speed of 15,000 r.p.m. during take-off might be considered normal, but during the cruise flight mode the same value might indicate some fault in the engine, or in the engine control system. So, the interpretation of the Flight Data depends *dynamically* on the context of the current flight mode: there is a logical dependence between them. The Flight Data is considered as a reflection of the condition of elements of the aircraft characterized by flight mode.

To assess the behaviour of an aircraft in terms of safety in real time, a model for each individual element is introduced. These models might be of different types; for example, functional, probabilistic and threshold models might co-exist for different elements, the particular technique is chosen to optimise sensitivity to fault detection for the element. In turn these can provide the basis for safety prognosis, each with different qualities which might include: precision of result, depth of prognosis, reliability and performance.

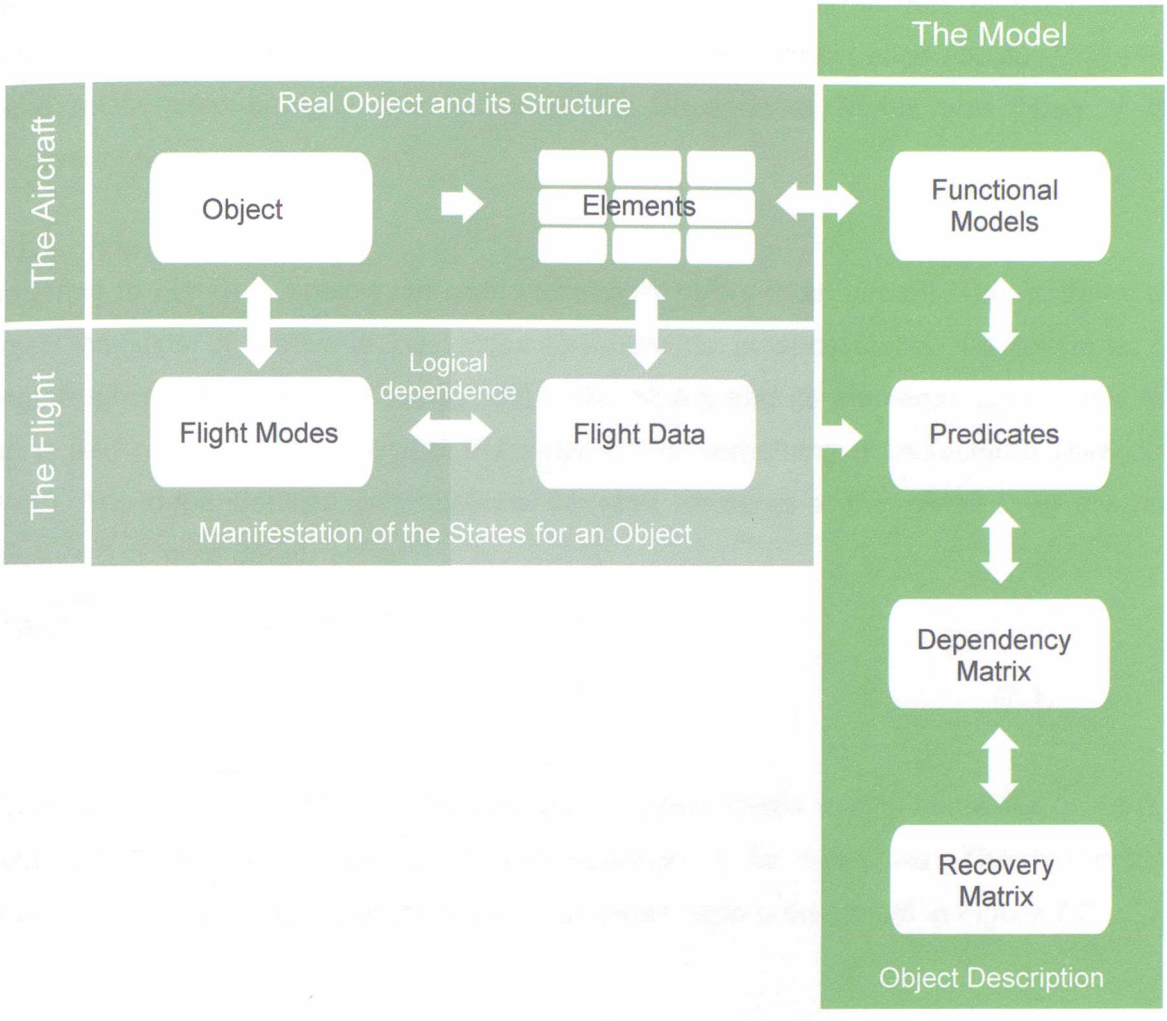


Figure 7.1: The internal structure and models for MASS

The functional and other models make it possible to evaluate the condition of the elements and then assess each element as good, or faulty. The conditions form a vector of predicates, the so-called *syndrome of object*. The syndromes are the MASS snapshots that describe the condition of the aircraft in terms of the faults of their elements.

There is inter-dependence between elements of an aircraft in terms of sequences of possible events that they can be involved in, or suffer from, and also the faults they can experience. The inter-dependence varies with the flight mode which may characterise the faulty behaviour's impact. The inter-dependence between impacts is reflected in the matrix of mutual dependence between elements - the Dependency Matrix.

A faulty element can cause various kinds and levels of harm, which may also vary by flight mode. The dependencies can be represented in a graph, with nodes as elements and the arcs showing the relations between them. The graph can, in turn, be represented by a Dependency Matrix.

The alternative ways to react to the object's condition in order to conserve or improve safety are defined in the Recovery Matrix. The use of the Recovery Matrix makes it possible to analyse "what should be done" when a particular situation occurs. There is a close relationship between the nodes of the Dependency Matrix and those of the Recovery Matrix.

7.1.1 The Object

Referring to Figure 7.2 below the term object here refers to an aircraft. The model of the object consists of elements i.e., major components or subsystems, for example: an engine, pilot, wing flap, fuel supply, etc. The object and its elements exist in the real world and represent the physical manifestation of something manufactured (even the Pilot!). The dependencies and relations between elements at the model level are now described in more detail.

The object is composed from a set of elements:

$$\mathbf{O} = \{e_1, e_2, e_3, \ldots, e_k\} \qquad (7.1)$$

Every element of the set **O** is defined by one or more models which makes use of a set of data parameters, see Appendix 3 and Appendix 6 for examples. The hierarchical dependence of an object, elements and data parameters is presented in Figure 7.2.

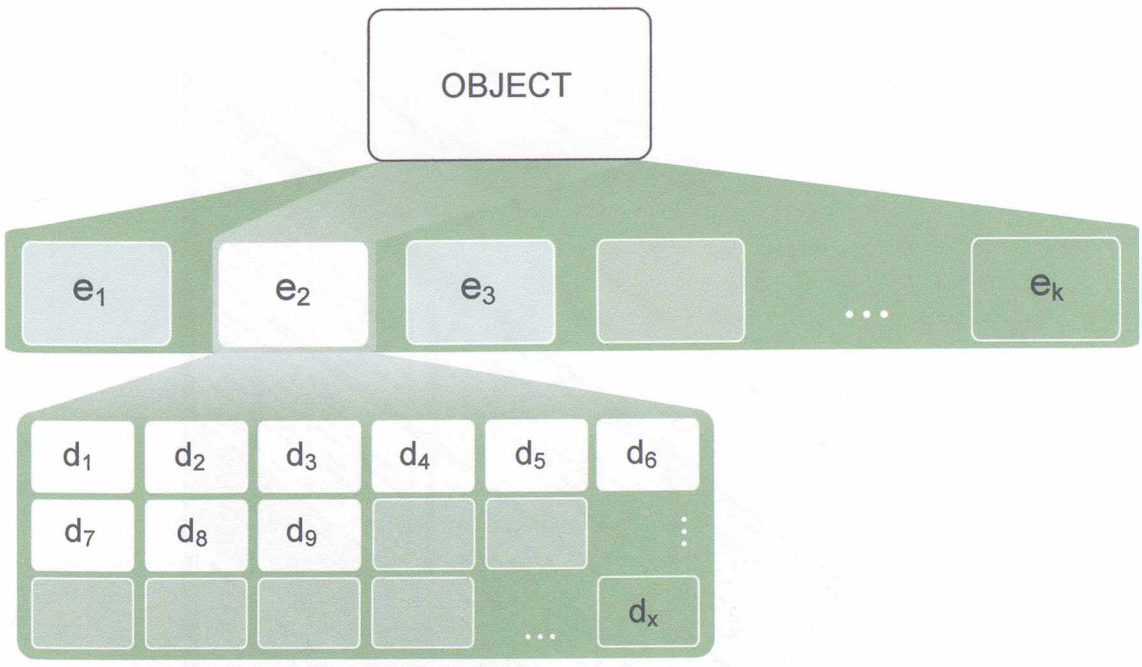


Figure 7.2: Hierarchical structure of an object and its elements

The object and its elements exist in terms of flight in various flight modes. During these different flight modes, flight data which reflects the state and condition of each element

are recorded, typically every 8 times per second, in the form of standard data frames (records).

7.1.2 The Flight Data

During operation data values from the object's sensors, and external sensors such as GPS, are stored in the data parameter fields of *Data Frames*, a data frame is considered to be a set of vectors, or multidimensional array of flight data and denoted as:

$$\text{Flight data frame } \mathbf{D} = \{d_1, d_2, d_3, ..., d_x\} \qquad (7.2)$$

where **x** is the number of flight parameters recorded during each cycle of data collection (and possibly transmission to a ground station). For GA, there are typically between 5 and 88 parameters, see Appendix 3 for details. A time sequence of recorded frames is illustrated in Figure 7.3; this is called a *Flight Data Memory*. The content of the frames and the condition of the object and its elements are related. In addition several flight data records taken together may provide evidence of a trend in a parameter or correlation between two or more of them.

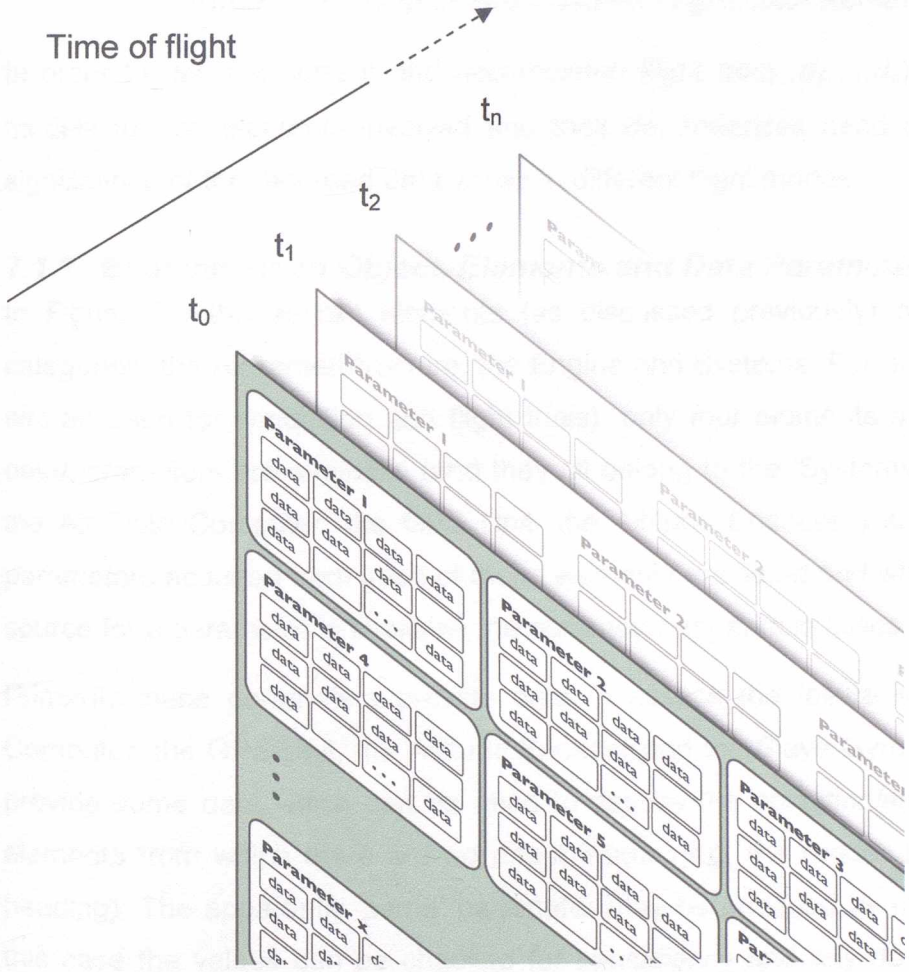


Figure 7.3: Flight Data Array Recording

Each element may share the value of one, or more data parameter values as illustrated in Figure 7.4

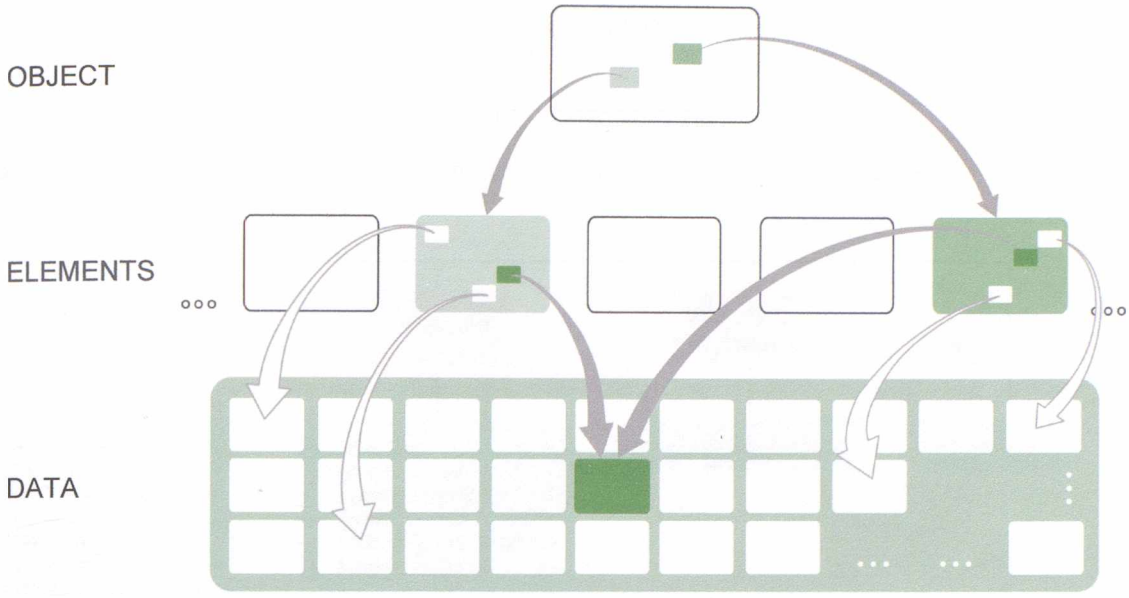


Figure 7.4: Object and Element Flight Data Relationships

In order to use the current and accumulated flight data $(d_1, ..., d_y)$ in real time of flight, models for the elements involved and their dependences need to be developed. The significance of the recorded data varies in different flight modes.

7.1.3 Example of an Object, Elements and Data Parameters

In Figure 7.5 the aircraft elements (as discussed previously) are divided into three categories: the Airframe/Structure, the Engine and Systems. For our specific case (of the aircraft used for simulation and flight trials), only four elements are identified for which data/parameters are available (and they all belong to the 'Systems' category); these are the Air Data Computer, the GPS Unit, the Altitude Encoder and the Slave Gyro. The parameters acquired from each of these elements are listed and wherever more than one source for a parameter is available the parameter appears in italics.

Primarily these parameters provide data to assess the failure status of the Air Data Computer, the GPS Unit, the Altitude Encoder and the Slave Gyro. The parameters also provide some data which can be used to assess the condition/status of further aircraft elements from which there are no direct inputs, e.g. the rudder (via rate of change of heading). The apparently 'same' parameter may be provided by multiple instruments, in this case the values can be checked for consistency and any deviations will indicate a fault or malfunction.

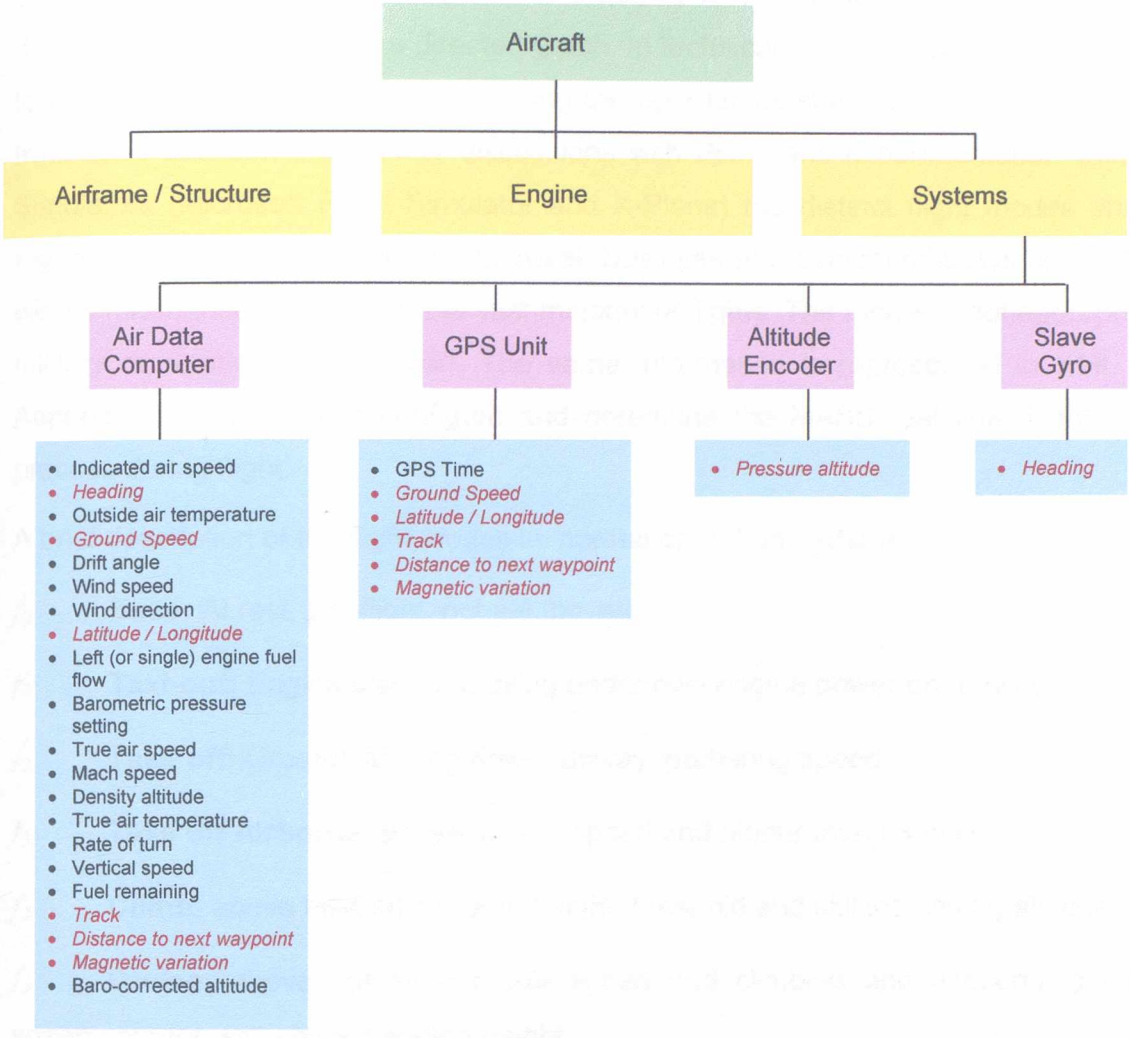


Figure 7.5: An Aircraft as an Object, Elements and Data Parameters

7.2 Flight Modes and the Aircraft Operational Flight Model

It was demonstrated in Chapter 3 that aviation accident statistics show a correlation with the phase of the flight during an aircrafts operation. It is also clear that the stresses on the aircraft and crew vary greatly too, landing being the more challenging operation and cruising being perhaps the most boring (which has its own dangers). This is also true for say the propulsion system (engines, fuel pumps etc) where revolutions/sec are expected to be in a narrow but high range of speeds during takeoff, but also relatively low during cruising. So it is essential to know what phase of flight the aircraft is in at all times, *this flight mode* can then be used to refine:

- The nominal limits of individual parameters within in each flight mode
- The expected correlation of each models parameter values in each flight mode
- The accuracy of modelling of each element model

In this section a more refined model of flight modes is introduced based on experimentation with the Microsoft Flight Simulator. A flight starts in the Base flight mode and proceeds to any other sequence of states by following the arrows, in this sense the diagram can be considered a directed graph. In technical terms it may also be considered to be a finite state machine representing the operational states of the aircraft, and valid transitions between them. After discussions with Pilots and experimentation with Flight Simulators (Microsoft Flight Simulator and X-Plane) the distinct flight modes shown in Figure 7.6 have been derived for General, Business and Commercial Aviation with fixed wing aircraft; this accounts for the vast majority of flights. The model is not appropriate for military or rotating wing aircraft. The same information is represented in XML in the Appendix 4; it is used to configure and determine the MASS real time flight analysis process during flight.

A brief description of the flight modes in 'normal operation' order is:

f_0 **Base:** At rest, pre-flight, not yet moved

f_1 **Taxi-out:** Engine started, moving under own engine power on runway

f_2 **Take off:** Ground: Moving down runway, gathering speed

f_3, **Take off Airborne:** above takeoff speed and higher than runway

f_4 **Climb:** above take off airborne height threshold and still increasing altitude

f_5 **Cruise:** above minimum cruise speed and climbing and descending within a speed corridor, still above Landing height

f_6 **Controlled Descent:** gradually loosing altitude in controlled flight

f_7 **Landing:** below landing threshold speed and height threshold, loosing altitude

f_8 **Taxi in:** on ground after Landing

f_9 **Uncontrolled Descent:** loosing altitude unexpectedly and at too great a rate, physical attitude and accelerations out of normal thresholds

f_{10} **Air accident:** unexpected abrupt change in height, speed or attitude

The latter two states are exceptional; ideally they should never happen as the usually lead to catastrophic accidents. However in some cases 'uncontrolled descent' is recoverable e.g., flying through a small 'air pocket'. An air accident is rarely recoverable other than by extreme means such as use of an ejector seat. The aim of active safety is to increase the probability that the aircraft will remain in one of the normal flight states at all time and to provide timely warning (as far as possible) of impending transition to an exceptional flight mode state. For most applications it is not possible to differentiate between Taxi-in and Taxi-out and so in the diagram these states are combined. The

reason for this is that it is the Pilots intent that determines the purpose of taxiing, it is not possible to determine this just by observation of the aircrafts movements.

The predicates that define the conditions for transition from one state to another depend to some extent on the characteristics of the aircraft and of the environment e.g. take off speed and barometric pressure (which affects lift). These along with the flight modes constitute an *Aircraft Operational Flight Model*. The XML file includes a declarative specification of the flight modes and state transition conditions.

More formally denote the set of the modes as FM:

$$\mathbf{FM} = \{f_1, f_2, \ldots, f_y\}, \qquad (7.3)$$

Where f_1 to f_y are the flight modes described above and defined in Figure 7.6

It is assumed that an object starts from the Base state. Each change from one flight mode to another is assumed to be instantaneous. The set of Flight Modes FM contains three subsets: main Fm, supportive Fs and exceptional Fe. The object (aircraft) itself is in the subset of main modes Fm during take-off, cruising and landing, it is in Fs when the preparatory or post-flight procedures are taking place and in Fe when an emergency situation occurs. In terms of the flight modes listed above:

$$\mathbf{Fm} = \{f_3, f_4, f_5, f_6, f_7, f_8\},\ \mathbf{Fs} = \{f_1, f_2, f_9,\} \text{ and } \mathbf{Fe} = \{f_{10}\} \qquad (7.4)$$

The dynamics of sequential changes between modes is described by probabilities Pij that connect different phases of flight and thus provides a basis for estimating reliability and success of flight.

The normal transitions between flight modes are shown in the thicker grey lines of Figure 7.6. The dotted lines denote unusual flight sequences, such as a 'touch down landing followed immediately by a take off. The thinner (red) lines represent emergency and emergency recovery situations. The emergency states have a line around their perimeter.

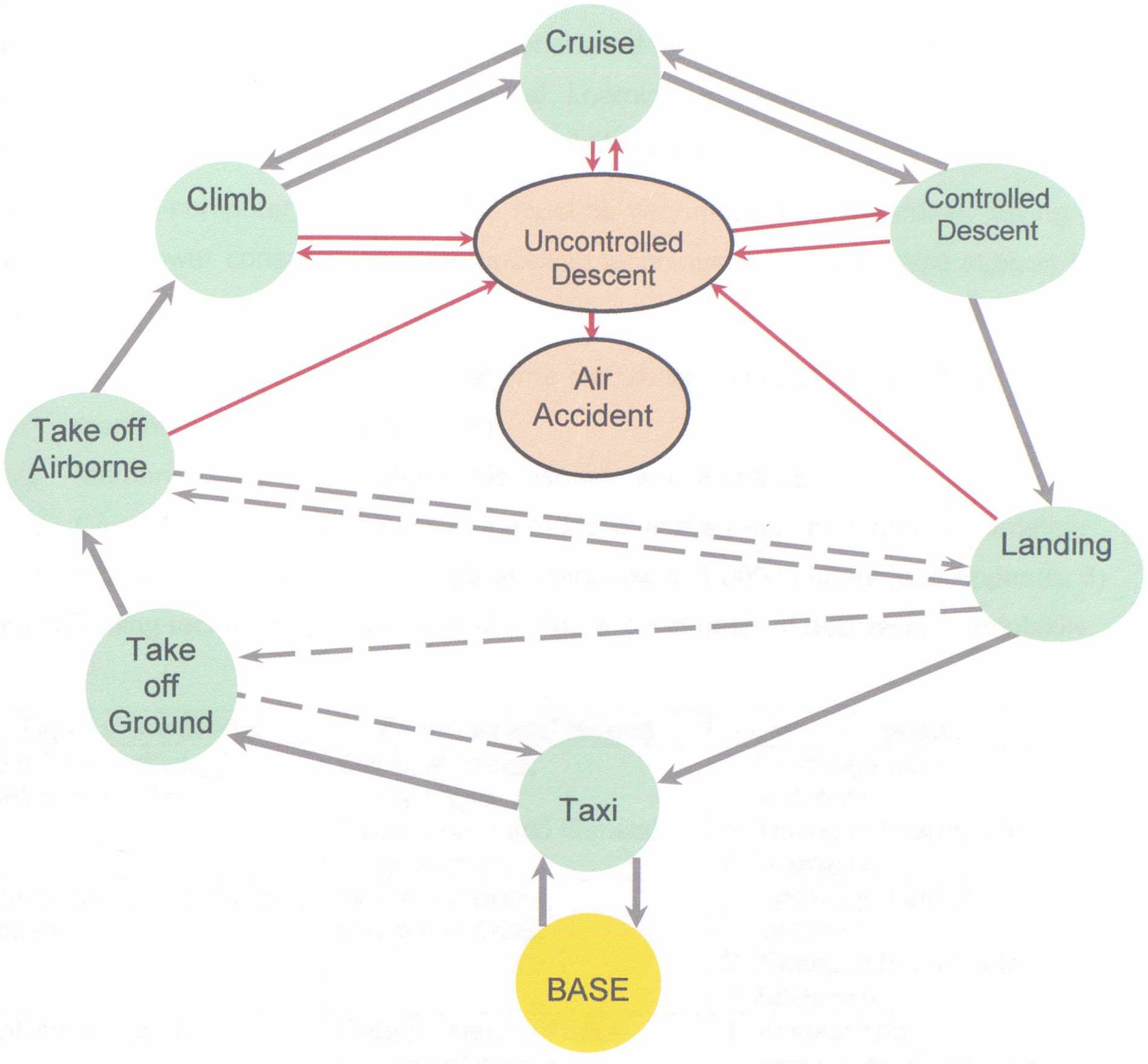


Figure 7.7: Flight Modes and Transitions for GA, BA and CA

7.3 Techniques for Modelling Element Behaviours and Faults

The safety of an aircraft depends on the condition of its constituent elements both singly and in concert. Every element $e_i \mid e_i \in O$ and $i = 1,...k\text{-}1,k$ is defined by a model which has state. The purpose of each model is to provide a 'benchmark' of expected normal behaviour against which the actual behaviour of the element during flight can be compared. In addition the Flight Data Memory content can be used to tune the models in the long term, for example to correct for gradual drift in parameter checking limits and changes in element dependencies.

During operation each element is considered to be in either a faulty, or normal state. The current state of each element is derived by its model taking its inputs in real time from the Flight Data Memory and any relevant outputs from the other element models (so long as 'circular feedback' relations due to co-dependency are avoided). So our objective is to determine when each element becomes faulty or normal in terms of safety of flight.

There are many alternative ways to model an element in order to make it possible to determine the fault status. The ones considered are based on techniques such as Artificial Intelligence Modelling, Statistical Learning Modelling, Statistical Modelling, Functional Modelling and Threshold Functional Modelling.

The on board computer used for MASS must be very modest in its facilities having low weight and power consumption. The modelling techniques used must also support this, some essential characteristics are:

1. Time determinacy – due to real time calculation constraints (i.e., 0.125 seconds maximum for the whole analysis)
2. Memory usage determinacy – this resource will be scarce
3. Coverage i.e., completeness of the model over the range of parameter variation
4. Scalability from 88 flight data parameters now to 1,000 in future (see Appendix 3)

The modelling techniques are described in Figure 7.8 in order of decreasing complexity.

Type of the Model	Features and Issues	Issues
Real Time Artificial Intelligent Model	Decision Trees, Fuzzy Logic, Evolutionary and Genetic programming	1. Coverage hard to estimate 2. Timing indeterminate 3. Scalability
Computational Learning Models	Neural networks; System of ODE	1. Coverage hard to estimate 2. Timing indeterminate 3. Scalability
Statistical Models	Categorisation of data, Volume of simple calculations	1. Volume and complexity of calculations 2. Availability of statistical basis and data
Functional Models	Based on ODE or PDE Euler method of ODE	1. Volume and complexity of calculations 2. Timing indeterminate
Threshold Functions for elements	Discrete analysis, N-dimensional matrix	1. Possibly scalability

ODE and PDE are abbreviations for Ordinary and Partial Differential Equations

Figure 7.7: Characteristics of Element Modelling Techniques

7.3.1 Artificial Intelligence Modelling

At first glance, the Artificial Intelligence Models look as though they provide an ideal fit for the implementation of PASS and so form the core of MASS: "...the objective of developing prediction and classification rules for various problem domains pursued by statistical and machine learning"...[7]. Unfortunately, a closer examination quickly reduces any initial optimism, because:

1. AI decision trees are based on sets of inference rules which assume the inter-dependency relation are known and stable.
2. Recursive programming for separating of data into different groups is complex even using Boolean logic separators.
3. Pattern for partitioning as well as for the formation a training set – choosing pattern for further steps of prognosis is often optimistic and the value of prediction using recursive formation of pattern is uncertain.
4. Generic Programming relies on random introduction of the fittest pattern and it is stochastic by nature; different runs may produce different results.
5. Time and hardware costs of AI schemes are significant: best results so far have been achieved using a neural network of parallel processors.
6. Coverage is hard to estimate and timing and function are non deterministic.

On this basis such techniques are deemed unsuitable for use in MASS models.

7.3.2 *Statistical Learning Modelling*

The concept of recognising trends within data samples (in our case flight data), using a generalisation of the data sample sequence as several possible distributions, looks impressive. If it is possible to discover a distribution for data samples with any required precision using a fast converging procedure, then this helps to determine the actual trend for every element. The idea was introduced by Chervonenkis and Vapnik in 1971 [59].

In a later development by Haussler [60], it was shown that if the number r of hypotheses is finite (certainly true for the behaviour of elements on board) then the probability that any hypothesis with an error larger than ε is consistent with the target concept on a sample of size m, is less than $(1 - \varepsilon)m\, r$. Thus, with the growth in the volume of flight data and a fixed number of hypotheses, it should be possible to identify the actual trend for every element and therefore make a judgement as to its fault status and hence reliability. Unfortunately, to develop an acceptable hypothesis, sets of training and testing data are needed. Speeding up the converging process here requires a recurrent neural network of dynamic elements that is described by means of systems of ordinary differential equations (ODE). Therefore this most suitable theoretical concept is unlikely to be applicable in practice due to the difficulty of characterising the system and the computing resources needed in real time for fault detection.

7.3.3 *Statistical Modelling*

Statistical Models seem to be suitable for MASS being oriented towards the categorisation of data. The flight data accumulated regarding each element of the aircraft are called observations. The set of such observations could be classified as belonging to

one of a finite number of possible categories there is such a set. Models of this type are used to discover probabilities within categories. Figure 4.11 has already shown how to use categories of data for PASS. In this case, there are three subsets of states that might be defined: normal, warning and dangerous: $\Omega+$, Φ *and* Ψ respectively. The credible estimation of flight data and its categorisation depends directly on the volume of flight data received and processed.

Interestingly, to implement this kind of model, a vast number of simple calculations are required, such as sums, differences, exponential and combinatorial. Even if not processed during real time of flight, these statistical category-defining models should be processed immediately after flight in order to detect and determine any slow-developing trends with respect to elements. This technique may be used in further stages of the Active Safety research programme to detect such trends.

7.3.4 Functional Modelling

An element model can be implemented as a functional model represented using a set of ordinary differential equations (ODE). The analysis and application of the functional model to element behaviour analysis can then be broken down into the classic steps [61]:

1. Model the phenomena as a set of ODE
2. Solve the set of ODE
3. Impose the given data
4. Interpret result

The advantage of using functional models based on analytical equations ODE (or partial differential equations (PDE)), is the possibility to achieve continuous modelling to any required precision of element behaviour. The disadvantage is the requirement for a numerical solution as, in practice, even the simplest numerical solution of ODE where derivatives are replaced by difference quotients, proposed by Euler, is not easy to apply.

Functional models defined by ODE, or PDE may be designed as open- or closed-loop systems. The problems of a functional model based on the open-loop approach are instability and the need for periodic recalibration. Functional models with inheritance are also called closed-loop systems. In contrast with open-loop models, closed-loop models do not require calibration of input and output to obtain the required accuracy. Closed-loop models are usually considered as self-calibrating, assuming of course, that they are stable and convergent. The modelling of 80 or more flight data, or up to 1000 or so in future, would be prohibitively slow, requiring very high performance hardware and consuming a great deal of power. Also use of ODE requires a floating point arithmetic processor in order to process the data in real time. On this basis the functional modelling technique is unsuitable for MASS.

7.3.5 Threshold Function Modelling

Threshold-based models define a threshold function with limits that characterise the normal and abnormal functioning of an element. Some systems use 2 levels of threshold, the first being a warning zone (marginal discrepancy) and the second indicating a definite fault. In addition, associated with each element, both extremes of each flight data parameter's value can have such thresholds.

Suppose the flight parameters form a set $(d_1(t), d_2(t), \ldots, d_x(t))$ and suppose that flight parameters values drift during aircraft operation. In effect, a random vector process describes the time behaviour of parameter:

$D(t) = (d_1(t),\ldots,d_x(t)), t \geq 0$ with an initial state $\vec{D}(0) = (d_1,\ldots,d_x)$

We suppose that the use of statistics is sufficient to estimate the type of processes, $\{D(t)\}$ and dependencies between them. System operation is considered to be successful during the flight if both parameters and their different combinations do not leave given domains within Euclidian spaces of appropriate dimensions. In other words, it is defined by a set:

$M = \{(r; d_{i_1},\ldots,d_x)\}$ with r indicating the dimension of the cut set.

With any cut set $s = (r; d_{i_1},\ldots,d_x)$ one associates a domain $Ds \subset Rr$. Thus, if T denotes the flight time of the aircraft, then the systems failure-free operation means that:

for any $s = (r; d_{i_1},\ldots,d_x) \in M$ and any $t \in [0,T]$ the relation $((d_1(t),\ldots,d_x(t)) \in D$ holds with initial state $d_1(0) = d_{i_1},\ldots,d_x$.

If, for at least one of $s \in M$, the corresponding relation is violated then a failure has occurred. The purpose of this generalised threshold theory is to develop a procedure to evaluate the risk of failure. The model has to be connected with a control process which continually monitors the data and evaluates the threshold function for each element in terms of the thresholds of the relevant set of data parameters. So the object can be modelled as a set of element models which form a set

$M = \{m_1, m_2, \ldots, m_k\}$ and taking into account the elements

$M = \{m_1(e_1), m_2(e_2), \ldots, m_k(e_k)\}$

Assuming that each element in the object is described by a functional model then:

$M(0) = \{m_1(e_1(d_1)), m_2(e_2(d_2)), \ldots, m_k(e_k(d_k))\}$

Introducing time into each model gives:

$M(0(t)) = \{m_1(e_1(d_1(t))), m_2(e_2(d_2(t))), \ldots, m_k(e_k(d_k(t)))\}$

To provide an analysis of the current situation on board during operation, it is necessary to obtain real snapshots of flight data. With this data, it is then possible to analyse the statistical mutual dependencies and hence, the role of every element in the objects behaviour. With this knowledge, there is the opportunity to avoid the consequences and/or mitigate the effects of a potentially dangerous flow of events.

In order to make this technique practicable it is necessary to characterise each element model in terms of the thresholds of each of its data parameters over the range of values experienced in both normal and abnormal operational conditions. This has been achieved in practice by using an experienced Pilot and flight simulator and a systematic plan to reveal and record the data required. This technique is *essential* for modelling some operational areas e.g. unsafe or even disastrous areas of flight operations.

On the basis of practicality this technique has been selected as the best choice for implementation as it exhibits the required properties.

7.4 Predicates and the Dependency and Recovery Matrices

Now there must be some set of criteria for evaluating the safety of the elements and some means of capturing the interdependencies between elements, e.g. the probability of one element propagating a fault or symptom of a fault to one or more other elements. One form of this is a graph where the elements are the nodes and the edges connecting the nodes represent the dependencies, see Figure 7.8 below. Another form of the same data is as a square matrix with indices representing the elements and the contents representing dependencies, see Figure 7.9 below. This is more convenient from a mathematical and algorithmic viewpoint and has the merit that the matrix can potentially contain all possible 'edges' i.e., dependencies between all nodes of the graph.

Now say a vector of *element model predicates* $\{P\}$ defines the condition for each element $e_i \in O$ and has the form:

$P = \{p_1(m_1(e_1(d_1(t)))), p_2(m_2(e_2(d_2(t)))), ..., p_k(m_k(e_k(d_k(t))))\}$

The PASS algorithm requires an analysis of possible faults and their consequences for every element e_i *in* O, which in MASS is called a Dependency Matrix.

7.4.1 The Dependency Matrix

The Dependency Matrix R describes possible dependencies (relations) between the elements of an object O, in terms of fault influence and propagation. The simplest version of R is a square matrix that has k columns and rows and describes possible dependencies of k elements in the object $\{O\}$. In the case of an undirected graph, every matrix element r_{ij} is defined according to the rule: r_{ij} = 1 when an object element e_i functionally relates to another elementary object e_j. A relation may also be associated with

each pair of elements which characterises their interaction in terms of induction of faults; this could be a logical or probabilistic relation. Note that the direction of the links in the matrix R is not presented. This generalization allows a path of possible dependencies to be traced through the matrix from any element y when its predicate is false:

$P_y(m_y(\ e_y(d_y(t))) = \text{False}$

In fact, the matrix R is a form of the graph of all possible connections between elements of the set O, written in terms of fault propagation consequences. The deliberate omission of a directed link on the graph R allows for the generation of possible sub-graphs starting from any $y\text{-}th$ node to support analysis of the consequences of a fault in the element y. This analysis can be done in real-time of flight, as long as it takes a determinate time of and makes it possible to react to an event, or event sequence before the situation on board develops to an accident level.

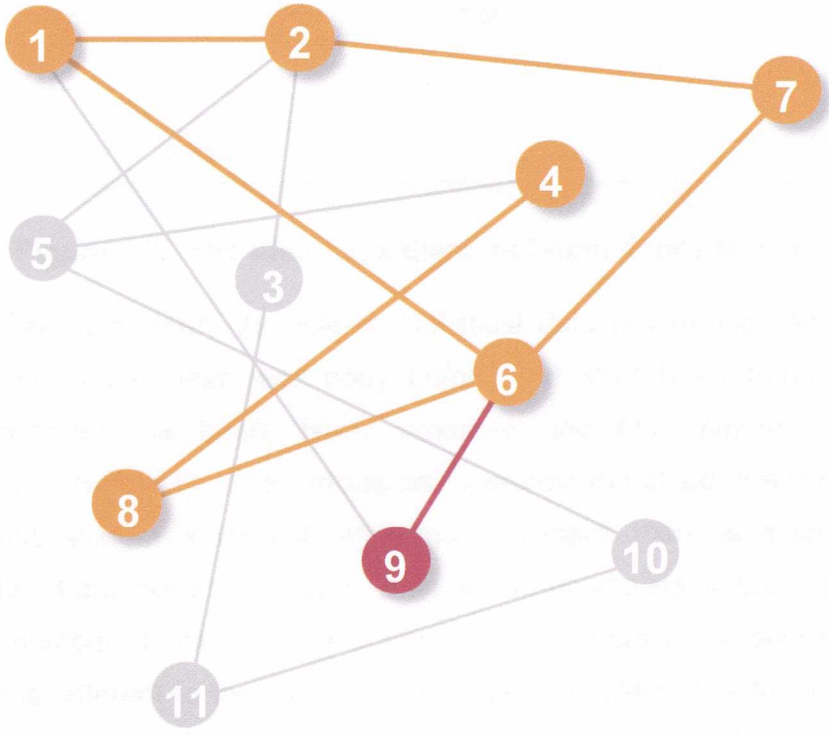


Figure 7.8: Graph of Dependencies between MASS elements

The Dependency Matrix describes the relations between the elements of an object. However it can be updated as the dependencies between elements change (for example, faulty elements are replaced by new elements and wearing elements suffer from aging processes). Also, the original matrix may not have been quite correct because of the limitations in expert knowledge at the time it was defined and because of more accurate dependencies between elements have been derived from the accumulated flight data. The dependencies are otherwise assumed to be invariant with time.

	1	2	3	4	5	6	7	8	9	10	11
1	P_{11}	P_{12}				P_{16}			P_{19}		
2	P_{21}		P_{23}		P_{25}		P_{27}				
3		P_{32}									$P_{3,11}$
4					P_{45}			P_{48}			
5		P_{52}		P_{54}						$P_{5,10}$	
6	P_{61}						P_{67}	P_{68}	P_{69}		
7		P_{72}				P_{76}					
8				P_{84}		P_{86}					
9	P_{91}					P_{96}					
10					$P_{10,5}$						$P_{10,11}$
11			$P_{11,3}$							$P_{11,10}$	

Figure 7.7: The Element x Element Dependency Matrix

An analogy may help clarify the role of statistical data processing. An example from human anatomy is the heart and body before and after heart transplantation. The connection between the heart, blood pressure and the immune system is not straightforward. Before the heart transplant operation the blood pressure in abnormal, but the immune system is normal. After the transplant, there is a changed relation between the heart and body indicated by a more normal and stable blood pressure and a much greater number of immune cells in the blood. The body's operational 'normal' after the transplant is different to the 'normal' before the transplant. Any further diagnosis, or prognosis has to take account of the heart transplant and that ambient conditions have changed.

The probability matrix makes it possible to define diagnostic features of the MASS for each particular type of aircraft. It generalises the well-known fault tree scheme and introduces a flexible ordering on $\boldsymbol{R}$ and enables dynamic analysis.

Two processes can be applied to the matrix $\boldsymbol{R_P}$ to analyse possible consequences of faults that apparently occur in an element, they are:

- Searching for possible consequences of a fault, "who is affected"
- Determination of "who is guilty", the locus or loci, of faults

The first process is about making a prognosis about a possible impact of fault events as a consequence of a detected fault. It is initiated when an element model, on analysing the flight data, indicates a significant discrepancy that indicates an apparent fault. The second process implements the evaluation of a possible cause(s) or reason(s) for the discrepancy.

7.4.2 The Recovery Matrix

The Recovery Matrix $\boldsymbol{R}_M$ determines the reactions to the detected, or suspected faults and is defined as k by k and has the same form as matrix $\boldsymbol{R}$. However each cell of the Recovery Matrix contains two values: the identity of the program components that are activated when firstly MASS analyses the probability of possible success of recovery and secondly when it produces safety related advice to attempt recovery. MASS assumes that there is a possibility for non-absolute recovery. A successful recovery procedure is a recovery with probability Pr_{ji} where:

$$Pr_{ji} >> 1 - Pr_{ji} \qquad (7.6)$$

The success of MASS can then be defined via the analysis of both matrix $\boldsymbol{R}_p$ and $\boldsymbol{R}_M$: the events detected and recovered are the justification for the existence of these matrices. Of course it relies on the experts' knowledge about the aircraft and so ultimately it is the quality and relevance of values initially provided for the matrix and algorithm which define the fault coverage.

7.5 The PASS Algorithms

In order to implement PASS the element models are used to detect a discrepancy in behaviour that indicates a fault, then two algorithms are used to evaluate the situation and recommend action(s) to conserve or improve safety. The overall process is shown in Figure 7.8. Initially the system must be characterised and configured for the specific aircraft type, this relies on their specialist knowledge, the aircraft's elements and the static and dynamic dependencies between them. During the lifecycle of a flight (before take off to after landing) the PASS system actively samples the flight data, evaluates the element models for indication of a fault, and then uses the dependency and recovery matrices to evaluate the nature of the fault and decide on the recommended action to take. After each flight there is then the opportunity to review the dependencies actually monitored between the elements and possibly update the dependency and recovery matrices.

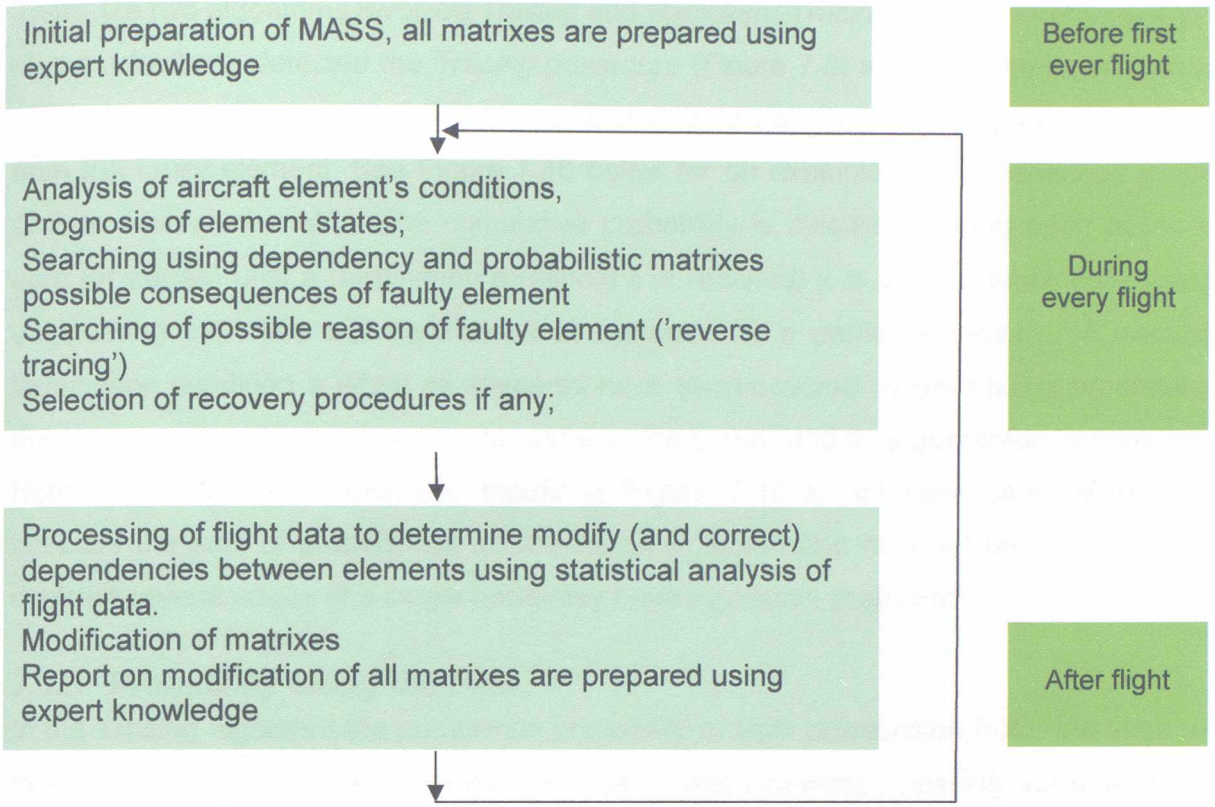


Figure 7.8: Overview of MASS processing with PASS

7.5.1 Algorithm Design Constraints

There are several practical constraints on the algorithms. The PASS analysis must be performed continuously and the normal rates for capturing and recording flight data are either 1 or 8 times per second. The performance analysis of the prototype software in Chapter 8 indicates that 8 times per second may be feasible, and once per second is definitely achievable. So the crucial design constraint on the algorithm is that its execution time must be less than ~100ms and must be deterministic. This must be achieved for dependency graphs with up to at least 100 nodes, and possibly in the future 1000 nodes. A further constraint is that loops within the dependency graph must be handled. The strategy for achieving this is to only use each path from one node to another at most once, this is justified on the basis that the only paths of interest are the ones with highest probability of fault propagation and the insight that the same fault cannot be propagated multiple times. *The structure of the algorithms is implicitly defined by these constraints.*

An alternative approach would be to 'flatten' the dependency graph when the system is initialised by converting the dependency graph into a series of trees and pre-evaluating and storing the cumulative probabilities for every path. Unfortunately this could consume huge amounts of memory and so has not been used. It may be useful in future for handling very large dependency graphs due to reduced computation in real time of flight.

7.5.2 How the PASS algorithms work

There are two algorithms involved *Tracing* and *Backward Tracing*. When symptoms of an element fault are detected the *Tracing* procedure (Figure 7.9) searches the Dependency Matrix for consequential faults in the other elements to identify the *consequences*, starting from the faulty element. See Figure 7.10 below for an example of a dependency graph and its equivalent matrix. The cumulative probability is calculated along each possible path (of edges) until a termination threshold ε is reached; it is defined empirically using engineering expertise and considered as constant for a particular aircraft. A second termination condition is when all elements have been covered by the tracing procedure, this is to avoid endless loops (circular paths in the graph) and thus guarantee termination. Note here that the probabilistic matrix in Figure 7.10 is not necessarily Markovian because the sum of probabilities on the edges at each node may not be equal to 1; in contrast several edges of a single node may have significant probabilities.

7.5.3 Probability along the Path

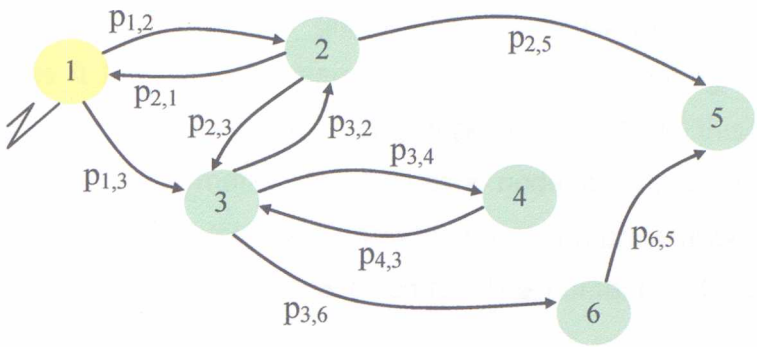
In the Tracing algorithm the cumulative probability of fault propagation from one element to another along the edges from the suspected node i to node , *possibly via a series of other nodes*, is defined as $\Pi(p_{i,j})$. When several paths lead from node di to node d_j all possible $\Pi(p_{i,j})$ are ranked and nodes along the paths are included into the set of suspected nodes. The algorithm called Tracing is shown below in Figure 7.9, it covers both termination conditions and meets the constraints defined in section 7.5.1.

Initially, every node (element) in the graph is considered as safe. All nodes of the graph are put into a priority queue Q (line 3). For the suspected node the probability is initialised to 1 (line 4) and D_s is initialised to "empty" (line 5). The queue is updated by a special function "delete from the queue". Initially the first tracing node s is the active node (line 8). Inside the tracing loop for every node probabilities for all possible paths are calculated. The highest probability of these paths defines the next step of the algorithm; the node along highest probable path is assigned as active and thus it is deleted from the queue. Thus the probabilities of all the adjacent nodes (minor to major (i.e., high risk)) with active node are calculated (line 11). To avoid looping during the analysis, the adjacent nodes that have been visited are excluded from further tracing (line 11). When a loop is detected, a production $\Pi(p_{i,j})$ is calculated excluding the last probability. All the remaining nodes will be traced; probabilities along their paths (from starting node) are updated (line 14). As already mentioned tracing terminates when the probabilities $\Pi(p_{i,j})$ of reaching the remaining nodes are less than ε.

```
Algorithm Tracing (s, D(N),Ds, {Π(ps,x), x□Ds } )
// Input: Dependency matrix D(N) with N elements of a weighted
graph G=<V, E>
// Input: The start node s and the reaching node j
// Output: The set of nodes Ds where x □Ds and Π(ps,x)> ε
// Output: The highest probability Π(ps,j) of node j reached by
node s
Q  // a priority queue based on the higher probability of nodes
reached by s
L  // the set of nodes already visited, used to avoid tracing
loops
Initialize(Q)  // initialize nodes priority queue to empty
1 For each node v in V do
2   ps,v ←ε; // set default probability to ε
3   Insert (Q,v,ps,v) //initialize the priority queue
4   ps,s ←1; Increase(Q,s,ps,s)  //update priority of s with ps,s
5   Ds←Empty // presume all elements are safe
6   L←Empty
7 for i←0 to N-1 do
8    a*←DeleteMax(Q)  //delete the maximum priority element
9    while pi,a*>ε
10     do
11     Ds←Ds□{ a*};L←L□{ a*}; Π(ps,a*)=pi,a*
12     for every node a in V- Ds- L that is adjacent to a* do
13        if ps,a* * Da*,a> ps,a then
14        ps,a = ps,a* * Da*,a;
15        Increase(Q,a,ps,a)
16      end for
16   end while
17 end for
18 Terminate
```

Figure: 7.9: Tracing of possible consequences

An example on how the Tracing Algorithm works is illustrated in Figure 7.10 which shows a graph for 6 elements and a set of transitions between them representing the probability of fault propagation between the related elements. The lower part shows the same information in matrix form. Figure 7.11 shows how the tracing progresses step by step using the same example. Let us assume that node d_1 manifests the fault, impact of this is evaluated by searching from d_1 to all directly or indirectly connected nodes (elements).



$$D^{(6)}= \begin{pmatrix} p_{1,1}, p_{1,2}, p_{1,3}, p_{1,4}, p_{1,5}, p_{1,6} \\ p_{2,1}, p_{2,2}, p_{2,3}, p_{2,4}, p_{2,5}, p_{2,6} \\ p_{3,1}, p_{3,2}, p_{3,3}, p_{3,4}, p_{3,5}, p_{3,6} \\ p_{4,1}, p_{4,2}, p_{4,3}, p_{4,4}, p_{4,5}, p_{4,6} \\ p_{5,1}, p_{5,2}, p_{5,3}, p_{5,4}, p_{5,5}, p_{5,6} \\ p_{6,1}, p_{6,2}, p_{6,3}, p_{6,4}, p_{6,5}, p_{6,6} \end{pmatrix} = \begin{pmatrix} 0.00, 0.30, 0.50, 0.00, 0.00, 0.00 \\ 0.60, 0.00, 0.50, 0.00, 0.02, 0.00 \\ 0.00, 0.70, 0.00, 0.60, 0.00, 0.80 \\ 0.00, 0.00, 0.40, 0.00, 0.00, 0.00 \\ 0.00, 0.00, 0.00, 0.00, 0.00, 0.00 \\ 0.00, 0.00, 0.00, 0.00, 0.01, 0.00 \end{pmatrix}$$

Figure 7.10: A Dependency Graph and Equivalent Matrix

The result of the search is the 'consequence' of the fault in the form of a ranked list of the nodes most likely to be affected. As the fault paths from each node are evaluated only the edge with the highest probability is followed at each node. At most each node is only ever included once in any path to ensure termination in a graph which contains loops.

The algorithm proceeds as follows, each step is illustrated in Figure 7.11:

Step 1: Node (element) 1 is assumed to be the one manifesting the symptoms of a fault (an element predicate failure). Initially all the nodes are given their default edge information and entered into Queue; the probability of the suspect node is initially set to 1.0 and the probability of all the other nodes is initially set to the threshold value ε. No edges have yet been traversed. The Result contains only the tuple for the initial suspect node, in this case node 1.

Step 2: If the (highest) probability of the top tuple in Queue is less than ε then the process is terminated, otherwise node 1 is the active node and its edges $P_{1,2}$ and $P_{1,3}$ are compared, with $P_{1,3}$ being the greater as shown by the bold line. Now Queue is updated by moving the highest priority tuple to Result, in this case node 3, and updating the edge information (predecessor node and cumulative probability) for the nodes visited in this step (nodes 2 and 3) based on the probability along each edge, these are shown in italics in the Queue column. The content of Queue is now re-ordered by probability value.

Step 3: If the (highest) probability of the top tuple in Queue is less than ε then the process is terminated, otherwise node 3 is the active node and its edges $P_{3,4}$ and $P_{3,6}$ are compared, with $P_{3,6}$ being the greater as shown by the bold line. Node 2 is not considered as it has already been taken into account during step 2. Now Queue is updated by moving the highest priority tuple to Result, in this case for node 6, and updating the edge information (predecessor node and cumulative probability) for the nodes visited in this step (nodes 4 an 6) based on the probability along each edge, these are shown in italics in the Queue column. The content of Queue is now resorted by probability value.

Step 4: If the (highest) probability of the top tuple in Queue is less than ε then the process is terminated, otherwise node 6 is the active node and its sole edge $P_{6,5}$ shown by the bold line. Now Queue is updated by moving the highest priority tuple to Result, in this case node 2, and updating the edge information (predecessor node and cumulative probability) for the nodes visited in this step (node 5) based on the probability along each edge, these are shown in italics in the Queue column. The content of Queue is now re-ordered by probability value.

Step 5: If the (highest) probability of the top tuple in Queue is less than ε then the process is terminated, otherwise node 2 is the active node and its sole edge $P_{1,2}$ is shown by the bold line. The edge $P_{2,3}$ also provides part of a path from node 1 to node 2 and this is shown as a dotted line in Figure 4, step 5. The cumulative probability of the path $P_{1,3}(0.5)$ and $P_{3,2}(0.3)$ is 0.15 which is less than the alternative path $P_{1,2}(0.3)$ and therefore it is discounted. Now Queue is updated by moving the highest priority tuple to Result, in this case node 4, and updating the edge information (predecessor node and cumulative probability) for the nodes visited in this step (in this case none) based on the probability along each edge, these are shown in italics in the Queue column. The content of Queue is now resorted by probability value.

Step 6: If the (highest) probability of the top tuple in Queue is less than ε then the process is terminated, otherwise node 4 is the active node and its sole edge $P_{3,4}$ is shown by the bold line. When only a single tuple remains in Queue and in this example it is assumed its probability is less than ε and so it is not moved to the Result. Now the Result contains the list of elements forming the most likely path of the fault, the *consequence* of the fault manifestation in node (element) 1.

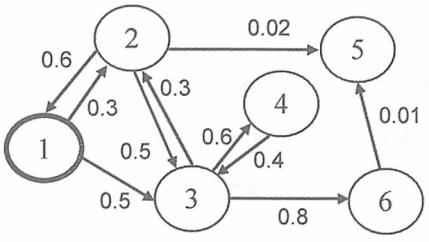
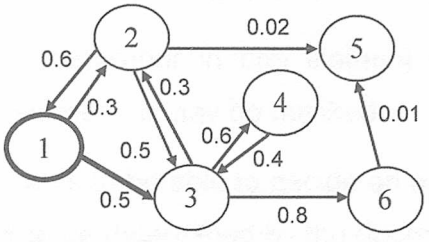
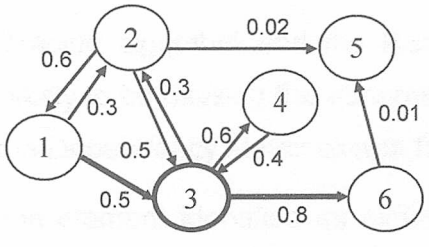
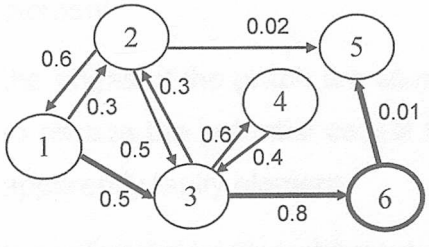
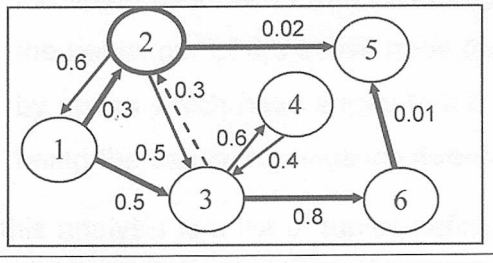
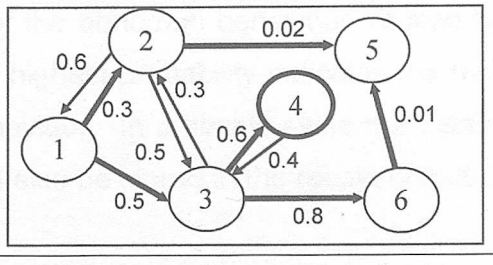
Steps	Tracing Progress	Queue Node List	Result Node List
1th		***1(-,1)*** 2(-,ε) 3(-,ε) 4(-,ε) 5(-,ε) 6(-,ε)	**1(-,1)**
2nd		***3(1,0.5)*** *2(1,0.3)* 4(-,ε) 5(-,ε) 6(-,ε)	**3(1,0.5)** 1(-,1)
3rd		***6(3,0.4)*** 2(1,0.3) *4(3,0.3)* 5(-,ε)	**6(3,0.4)** 3(1,0.5) 1(-,1)
4th		**2(1,0.3)** 4(3,0.3) *5(6,0.004)*	**2(1,0.3)** 6(3,0.4) 3(1,0.5) 1(-,1)
5th		**4(3,0.3)** *5(2,0.006)*	**4(3,0.3)** 2(1,0.3) 6(3,0.4) 3(1,0.5) 1(-,1)
6th		**5(2,0.006)**	4(3,0.3) 2(1,0.3) 6(3,0.4) 3(1,0.5) 1(-,1)

Figure 7.11: A step by step analysis of the Tracing algorithm

7.5.4 Algorithm of Backward Tracing (Recovery)

Now that the 'consequence' set of elements affected by the element's abnormal behaviour has been determined by the dependency analysis, further analysis can be performed to evaluate the set of elements most likely to be causing the element's abnormal behaviour, the 'influence'. This information can then be used to determine the action to conserve or improve the safety of the object by adjusting the way it is operated to mitigate the short and longer term effect of the abnormal operational behaviour of the system. The reasons are as follows:

1. An element sensor or its evaluation model may be inaccurate.
2. Abnormal behaviour in one element may not manifest abnormal behaviour in another element, it may be masked.
3. It is desirable to be able to decide on a recovery action based on the set elements of significance determined by the dependency and then the recovery analysis.

The *Reverse Tracing* algorithm and the Recovery Matrix are used to find the set of elements most likely to be causing the abnormal behaviour. The Recovery Matrix has the same form as the Dependency Matrix except that:

1. the element identified as exhibiting a discrepancy is the initial "suspect" element
2. the edges of the graph are searched in the opposite direction (backwards) to retrace the potential causal flow of abnormal behaviour influencing the apparently faulty element
3. the value associated with each edge is now viewed as the probability that the behaviour of the active node (currently being considered) is influenced by nodes which have edges to it a different threshold value ρ is used, this being the causal significance threshold

The result of this analysis is a list of tuples defining the set of nodes which are the most likely cause of the abnormal behaviour, ranked by cumulative probability of cause. The tuple with the highest probability indicates the node which is the most likely cause of the abnormal behaviour. In a simple system an action could be associated with each node and this could also be stored in the recovery matrix.

The Backward Tracing algorithm is as follows:

```
Algorithm Backward Tracing (s, R(N), Ss, {Π(ps,x), x∈Rs } )

// Input:  Recovery matrix R(N) with N elements of
           a weighted  connected graph G=<V, E>
// Input:  Suspected node s and the fault originating node j
// Output: Set of nodes Ss in which x ∈Ss and Π(px,s)> ε
// Output: Highest probability Π(pj,s) of node j reaching node s

Q // Priority queue ordered on the higher probability of
     nodes reaching s
L // Set of nodes that have been visited.
     It is used to avoid loops in the tracing.
Initialize(Q)  //initialize nodes priority queue to empty

01 for every node v in V do
02   pv,s ←ε;
03   Insert(Q,v,pv,s) //initialize the priority queue
04   ps,s ←1; Increase(Q,s,ps,s) //update priority of s with ps,s
05   Ss←Empty //initialize the set of originating node to empty
06   L←Empty //nodes have been visited is set to empty
07   for i←0 to N-1 do
08     a*←DeleteMax(Q) //delete the maximum priority element
09     while pa*,i>ε do
10       Ss←Ss∪{ a*};L←L∪{ a*}; Π(p a*,s)=pa*,i
11       for every node a in V- Ss- L that is adjacent to 'a* do
12         if pa*,s * Ra,a* > pa,s
13           pa,s = pa*,s * Ra,a*
14           Increase(Q,a,pa,s)
15         else
16           Terminate
17         end if
18       end for
19    end while
20   end for
21 end for
```

Figure 7.12: Backward Tracing to Find the Causes

When a high probability of system failure is discovered measures such as emergency landing might be recommended. If the result of the backward recovery algorithm shows that there was no significant (above the threshold) sequence of faults, then the only action needed is to record the suspect event being recorded. However if an 'influence' of significant cause was found then recovery actions from a list of legitimate and relevant actions will be reported to the crew, pilot and maintenance engineer. In a more sophisticated system the information could be relayed to a ground station via radio or satellite.

An approach to improving the discrimination of the system would be to monitor several different aspects of it simultaneously, for example e.g. electrical, hydraulic, mechanical,

and so on. This is already done in CA with special monitors for the engine system and hydraulics being provided on some modern aircraft, however, there is still a need for an active safety system to monitor all such subsystems. Each aspect being monitored will have its own dependency graph (with its own set of nodes and weights on the edges). In such a case there would be multiple evaluations of these graphs to find the likely cause from each viewpoint. The set of results could then be correlated to get a clearer picture of the nature of the fault and so give more appropriate safety advice. Another technique called 'zonal analysis' is used for safety design. This entails reviewing the physical routing of mechanical, electrical, optical and hydraulic linkages in the aircraft to determine how a failure in one system might affect others due to proximity effects. The dependency graphs of each aspect of the system can then take account of such 'proximity' co-dependencies of faults in the system.

8 An Experimental MASS Implementation

In order to support the demonstration of MASS a system has been built based on prototype hardware from ETH and a prototype software system written by ETH, London Metropolitan University and Robinson Associates [75]. To prove the MASS concept an aircraft flight mode model was built and a dependency and recovery matrix generated for a sample aircraft, the Piper Cherokee Lance [92]. This aircraft was chosen because a low cost simulator was available (Microsoft Flight Simulator 'A Century of Flight') and also it is feasible to flight test the whole system at some point in the future at a reasonable cost. This chapter describes the prototype system and experimentation.

8.1 MASS in the Aircraft - System Block Diagram

A block diagram of a MASS implementation within the aircraft is illustrated in Figure 8.1. The upper part of the diagram shows the existing sensors, the flight control system, the control system actuators and the human-machine interface (HMI) indicators for the crew. Typically sensors might be for altitude, air speed (in 3 dimensions), heading, position, engine revs etc. A Flight Control System (FCS) processes this sensor data and provides information via the HMI to the crew. It also monitors actuators such as engine throttle, brakes, landing gear etc. The flight crew use the FCS and their own experience, skills and judgment to make decisions about how best to fly the aircraft.

The key parts of the MASS system:

The aircrafts Flight Data Interface (FDI) which provides the physical interface with the data sensors in the aircraft, its purpose is to manage the variation normally found in GA aircraft. It samples the data and then presents the data values in a standard form [38] to the active safety monitors own Flight Data Interface and the MASS system which:

1. monitors the data stream provided by the aircrafts FDI and its own sensors (optionally)
2. applies the PASS processing to both short term and longer term data
3. stores the relevant data in the Flight Data Memory (FDM)
4. provides an indication of safety information to the flight crew

Flight Data Memory (FDM) which retains the flight data during each flight and also over the lifespan of the aircraft's use. This must be resilient enough to survive a crash, be locatable and of course ultra reliable. It provides the data storage equivalent of a flight data recorder, for details see Appendix 6.

It is important to note that it is the responsibility of the flight crew to monitor the MASS safety indicator(s) and to act on them either before the flight (by simply not using the aircraft if it is found to be in an unsafe state) or during flight (via the flight control system);

this is referred to as Level 1 Active Safety. In future, subject to evaluation of MASS and its effectiveness, it may be possible to extend to Level 2 Active Safety so the system would interface directly with the flight control system, and thus become an extension of it.

The Flight Data Memory stores data collected during each flight and accumulates a condensed version of it over the life of the aircraft. It is somewhat similar to a flight data recorder, however it is anticipated that further safety related data/information can be retrieved from it. The information in the FDM is physically stored in solid state memory chips within a housing that can survive a crash (including a resulting fire). Its data can be analysed between flights and/or after a crash by means of the MASS Analysis Workstation (MAW). There is also potential to dynamically download data during a flight by either satellite, SMS messages or radio link but this is outside the scope of this work.

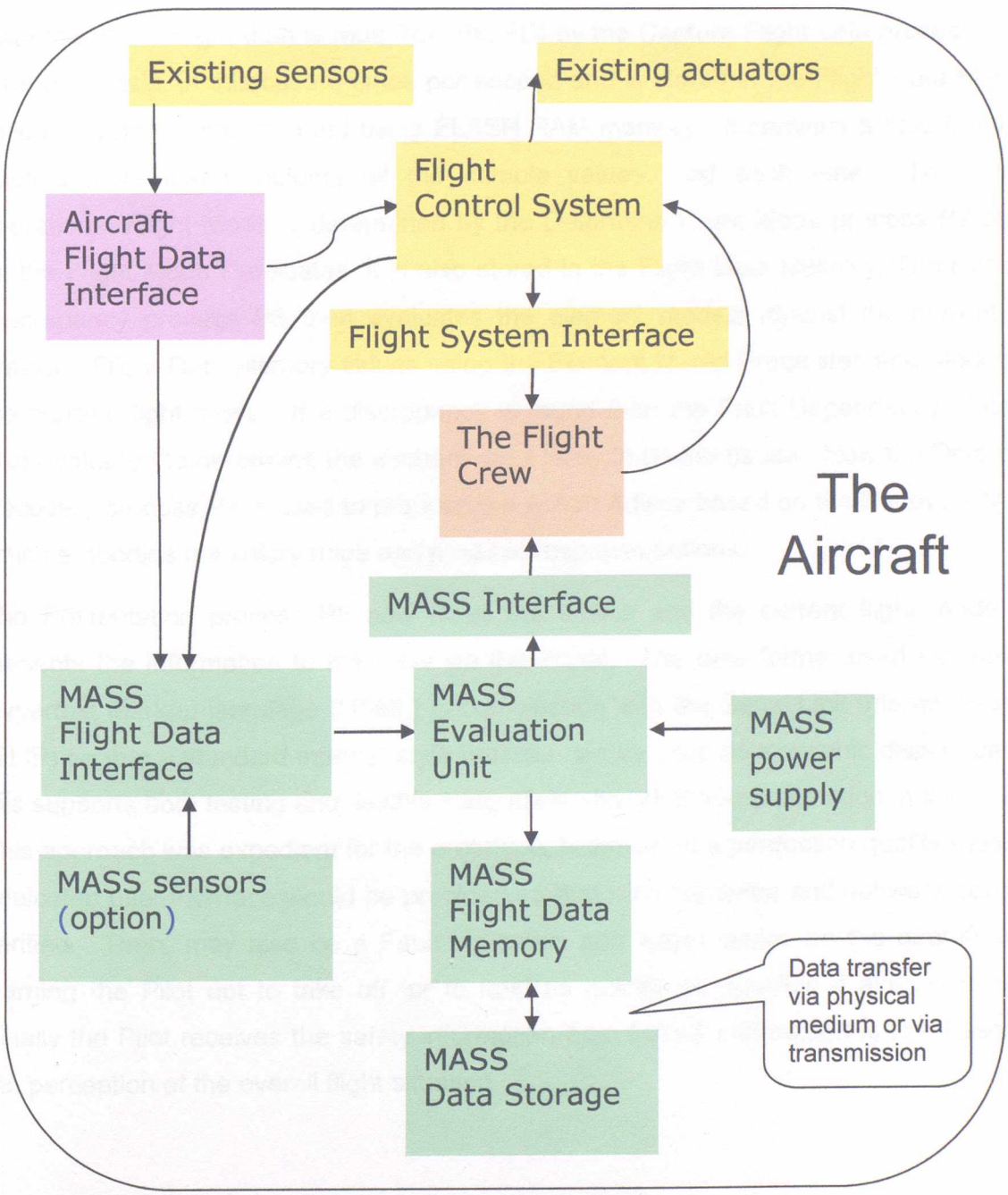


Figure 8.1: Block diagram of an aircraft system with MASS

8.2 Information Processing within MASS

The MASS system is basically a fault management control loop at the level of the aircraft itself. Its purpose is to improve the safety of flight either by advising against starting a new flight or providing salient advice in flight in the event of a fault developing which might compromise operational safety. The information processing involved in the loop is shown in Figure 8.2, and represents an abstract view of the top level implementation of the PASS model within the aircraft during flight, in real time. Note also that the system is active, with the same analysis, before takeoff and so may offer an 'unsafe to fly' indication to the ground and/or flight crew. In this case it would be unsafe to attempt a flight at all.

The data flows and processing are shown in the data flow diagram shown in Figure 8.2, the main processes are labelled P1 to P5 and the main data flows are represented by the arrows. The aircraft contains a number of elements, a Flight Control System and a Flight Data Interface. Flight data is read from the FDI by the Capture Flight data process P1 on a regular basis, in this case 8 times per second and is stored in the Flight Data Memory which is typically implemented using FLASH RAM memory. It contains a data frame for each sample period holding all the sample values read each time. The current operational Flight Mode is determined by the Determine Flight Mode process P2 based on the Flight Mode Predicates, it is also stored in the Flight Data Memory. The Evaluate Discrepancy process P3 then evaluates the element models against the current and previous Flight Data Memory values using the Element Model Predicates and Models for the current flight mode. If a discrepancy is found then the Fault Dependency Matrix is also evaluated to determine the element most likely to be the cause. Now the Determine Recovery process P4 is used to produce the Action Advice based on the Recovery Matrix which embodies the safety rules and possible response actions.

The Presentation process P5 now takes the advice and the current flight mode and presents the information to the crew via the Panel. The data format used internally is Hypertext Markup language (HTML) in combination with the Serial Link Internet Protocol (SLIP) so that a standard internet style browser can be used as a graphic display device; this supports both testing and flexible integration with other instrumentation in the aircraft. This approach was expedient for the prototype, however, in a production quality system a dedicated user interface would be provided so that both hardware and software could be verified. There may also be a Fault Indication and alarm device on the aircraft panel warning the Pilot not to take off, or to land as quickly as possible if already in flight. Finally the Pilot receives the safety information from MASS and responds to it based on the perception of the overall flight situation.

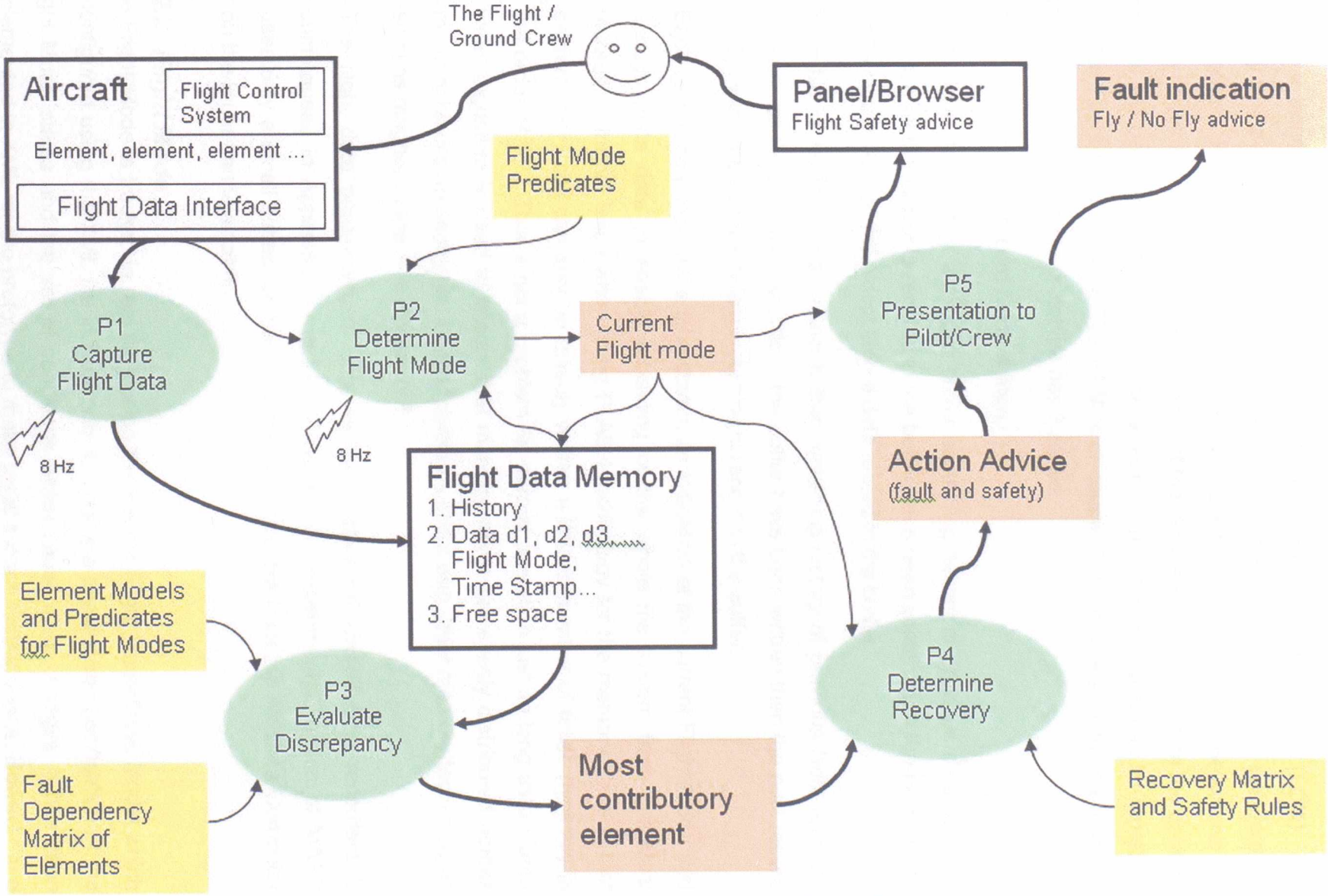


Figure 8.2: Data flow diagram showing the main data flows and processing in a MASS implementation

8.2.1 Flight Data Memory

Data is captured from the aircraft's sensors and avionics, via the Flight Data Interface (FDI) on a periodic basis by P1 and stored in the Flight Data Memory (FDM). The frequency of the data capture will initially be 8Hz, this being an established standard for flight recorders. However, when real data is available it will be analysed to determine the frequency required in order to be able to extract the required information from the data. In this way it will be possible to optimise the amount of relevant data that can be stored in the limited Flight Data Memory. The FDM is of course finite in size and its use must be managed. The design in the prototype has 3 zones:

1. the current data record being written,
2. a file in the form of a circular buffer containing history of previous *data* records; once all the available records in the buffer have been written then the next record is overwritten on the oldest stored data record in the buffer.
3. a file in the form of a circular buffer containing history of previous *flight* records, once all the available records in the buffer have been written then the next record is overwritten on the oldest stored flight record in the buffer.

Each data record includes a time stamp, an indication of the current Flight Mode and enough meta data to enable rebuilding of the whole file system from individual records. A further issue when using FLASH technology for the memory chips is that each memory cell can only be reliably written a limited number of times (typically in the order of 10^9). This is not a problem for normal operation just so long as an 'anti-wear' algorithm is used to ensure that memory writes are evenly distributed across memory blocks on each chip. Similar problems occur with other memory technologies such as magnetic tape, see Appendix 6.

The flight data parameters of data stored in standard aircraft data recorders is summarised in Appendix 3 and [38], however, the experimental version of MASS uses only a small subset of these parameters available from the Air Data Computer on the Piper Lance aircraft.

8.2.2 Flight Mode

The Flight Mode is tracked in real time using the Aircraft Flight Operational Model which is configured using the XML file in Appendix 4. This is a declarative specification of the Flight Mode states and the set of conditions which cause state changes. It has been implemented in XML for the prototype to make initial system testing easier. However in a production system such flexibility of configuration would have to be carefully protected with access controls to prevent malicious tampering with the specification. The flight mode is used by the element models to characterise their parameter limit values and thus improve their discrimination of fault detection.

8.2.3 Real time diagnosis and prognosis

The evaluation of the current (diagnosis) and future (prognosis) faults in the aircraft is performed by P3; this takes data from the FDM and :

1. Evaluates the fault status of each of the aircraft's elements based on a set of predicates, then
2. For any detected fault the fault dependency matrix is evaluated to assess consequential contributions to other fault conditions using
3. A set of rules (packaged experience provided by experts) to guide and characterise the evaluation

The system is configured initially by downloading values into the Dependency and Recovery matrices based on the fault dependencies and recovery strategies needed for the particular aircraft.

8.2.4 Determination of Response

The response to the fault/risk profile is generated by P4 to determine how best to conserve or improve safety by considering the whole fault/risk profile by:

- Mitigation of the effects of a set of current fault
- Avoiding or preventing escalation of current fault from developing into future errors or failures
- Preventing the likelihood of occurrence of the pending fault, or mitigating the severity of its effect
- Addressing fault/risk combinations by priority (i.e., higher risks first).

This involves evaluating the fault/risk profile from P3 based on so-called recovery methods and (possibly in future) a set of rules, the flight mode characterising the overall strategy. The result of this evaluation is an advice profile aimed at conserving or improving the safety of flight i.e., a set of information and recommended actions for the pilot. There are two kinds of information resulting from this analysis:

1. Fault advice e.g. major fault detected, aircraft not airworthy.
2. Consequential safety advice based on a safety analysis of the consequences of faults e.g. fuel leak in left engine, shut down engine if possible (to avert a fire).

The safety advice referred to above is generated from a safety analysis of the consequences of a fault. This will be specific for each type of aircraft, hence the need for customisation.

8.2.5 Presentation of advice to the Flight Crew

The set of fault and safety advice is formatted for presentation by the Human Machine Interface (HMI) to the pilot by P5. The communication has to be clear, concise, precise,

relevant, practical, timely and easy to assimilate. The pilot observes the advice and uses judgement and skill to decide how best to adapt the control of the aircraft given the current perception of the flight context and the safety advice provided. The pilot's reaction to the advice, via the Flight Control System, closes the safety control loop on board the aircraft in real time, depending of course on the response time and appropriateness of reaction of the pilot. There are 2 kinds of indications envisaged:

1. A simple Fly /No-Fly indicator to warn the flight and/or ground crew that the aircraft is not considered airworthy due to a current or impending fault (set) which might render it unsafe.
2. Advice to the Flight crew in the event that a fault is diagnosed during flight which would impact the safety of the aircraft. It is envisaged that this information relates to safety i.e., the avoidance of harm occurring during the rest of the flight.

A browser is used for display to provide flexibility in the choice of display panels e.g. PDAs or Laptops.

8.2.6 Configurability of system

The purpose of system configuration is to make it possible to have a single 'standard' MASS software package which is then characterised for each type of plane (for evaluation algorithms) and particular installation by the configuration meta data. This avoids the possibility that the MASS software itself would need to be adapted and re-verified for each different installation as this would be uneconomic and too time consuming. The configuration data is shown in Figure 8.2 in the borderless boxes that are light yellow.

The configurable data sets are:

1. Flight mode determination rules for P2
2. Predicates for each element model for each flight mode for P3
3. Dependency matrix content for P3
4. Recovery Matrix content and safety actions (rules) for P4

The configuration should be both machine and human readable to support verification so an XML format has been used to make development more flexible. The XML for the prototype is contained in Appendix 4 and defined in [95].

8.3 Software Structure and Performance

The MASS software is written in the Oberon language developed over the past 20 years at ETH [76] . This language features strong data typing and directly supports modular approach to software design [77], [80], [81]. A minimal dialect of the language, called Minos Oberon, was defined by Prof N Wirth and he also produced the compiler and module linker especially for the ONBASS project.

8.3.1 Software Architecture and Partitioning

At the top level the MASS software is partitioned into three closely coupled collections of modules as shown in Figure 8.3:

- Minos runtime core modules
- Framework modules
- Application modules

Each component or module (represented by a box) implements some specific functional domain and exports an abstract interface. Upper level modules may use or import (interfaces of) lower level modules. The runtime core called Minos corresponds to the actual "operating system". It is responsible for the management of resources such as processor, volatile memory, flight data memory and I/O ports. In addition it provides file system functionality, low-level recovery procedures, and system and component initialisation. The runtime core is a set of hierarchically structured: components close to hardware are allocated in lower levels, the lowest level being the Hardware Abstraction Layer (HAL). Its purpose is to improve the system's portability by hiding platform-specific details. Other low-level components are the system boot loader and the floating point emulator.

The device drivers are allocated on top of a hardware abstraction layer (HAL) which serves to hide the idiosyncrasies of a particular hardware platform from the rest of the software. The drivers use the HAL abstraction to communicate with hardware devices. On the next higher level we find the I/O system whose responsibility is standardizing input/output programming. The memory management system manages the system heap. It provides routines to allocate and free memory blocks. However, the runtime core does not implement automatic garbage collection because it is de-facto incompatible with hard real time constraints. Instead a specific programming discipline is used to avoid garbage collection i.e., instantiation of all used objects at initialisation time. Support for several protocols and other services including, for example a ROM file system, a flash RAM based file system and TCP/IP are included. Dynamic loading of software components is supported by a linking module loader. The system scheduler is responsible for distributing the processor resource (time) among the different tasks according to real-time constraints. There is also a liveliness checker ("watchdog") and a logging and tracing facility for debugging purposes. The top level component called Minos basically provides the human machine interface functionality.

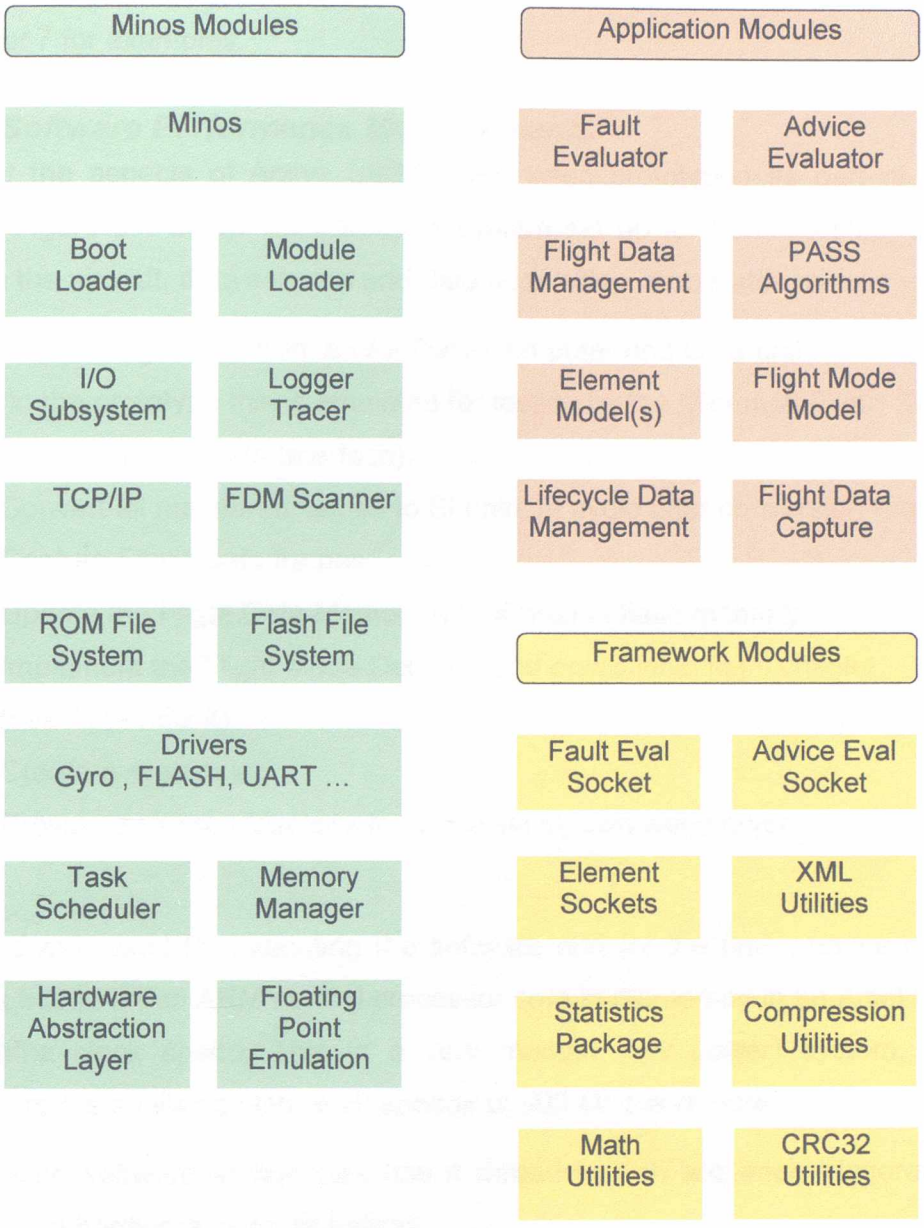


Figure 8.3: Partitioning and Module Structure of MASS

The application framework consists of a plug-in mechanism for flight-data analysis algorithms and a software library provides support modules for mathematics and statistics, string handling and XML document management.

The application itself basically consists of an implementation of the PASS algorithm. It is responsible for analysing the different streams of sensor data and for identifying potentially hazardous situations. Several logical processes (see Figure 8.2) are required for functions such as recording the flight data and giving feedback to the crew via a thin client interface based on HTML, these are implemented as Oberon tasks.

The development system is illustrated in Figure 8.4, it is also used for verifying the application software by using the Microsoft Flight Simulator to emulate the operational environment, the aircraft and its equipment (Air Data Computer and GPS). A series of

flight scenarios was used to check the functioning of the Flight Mode Detector; see Appendix 7 for examples.

8.3.2 Software Performance Measurements

Many of the aspects of Active Safety have been prototyped as part of the ONBASS project. Figure 8.4 below illustrates the system set up for bench testing using a PC to emulate the aircraft, data sensors and data acquisition, it operates as follows:

1. Read in flight data from an Air Data Computer and GPS unit
   (in the prototype this is emulated for testing by the Microsoft Flight Simulator and the ETG Flight Data Interface)
2. Convert all measured values to SI units to avoid later conversion errors.
3. Capture Flight Data frames
4. Update the Flight Data Memory (black box) in flash memory.
5. Implement the Flight Mode Detector and operational flight checks
   (see Appendix 4).
6. Create a system log.
7. Provide a Human Machine Interface via its own web server.

The hardware used for executing the software and for the performance measurements below is based on an ARM central processor core implemented in an Actel FPGA running at 20 Mhz clock speed. This is a very modest (low power) system; current ARM processors are available with clock speeds of 500 Mhz and more.

The runtime software architecture has 4 threads which are each triggered on a timed basis from a hardware clock as follows:

1. Every 5 milli-seconds for handling input and output. This is based on 4 UARTS each with built in FIFO buffers to provide connectivity to the aircraft systems.
2. Every 125 milli-seconds for routing of data already captured or ready to be output
3. Every 1000 milli-seconds for the data frame capture and storage, and the Flight Mode Detection and Operational Safety checks.
4. A background thread which 'soaks up' the residue of processing capacity; it runs both the web server and TCP/IP protocol stack.

Each thread has a list of Oberon commands (actually procedures without parameters) which it executes sequentially every time it is invoked. This simple structure makes it easily possible to apportion processing time and assure determinacy of each separate 'procedure-worth' of execution. In a production version of the system it would be essential that the scheduling and execution of the software could be verified to be deterministic. In the prototype this has been achieved in practice by measuring the execution time of each Oberon procedure used and then ensuring that all such procedures on each thread can

definitely run to completion each second (the period of data collection). This has been verified by observation as indicated below in Figures 8.4 and 8.5. However, for a production version the scheduling design would need to be more formal and rigorous using a technique such as Monotonic Rate Scheduling (RMS) [96],[97]. Fortunately the existing design of the prototype software conforms to the basic RMS assumptions:

1. there is no resource sharing (e.g., semaphore blocking, busy-waits)
2. the deterministic deadlines equate directly to the scheduling periods
3. priorities are static, not dynamic
4. static priorities are rate-monotonic; shorter deadline means higher priority
5. context switch times and thread overheads are insignificant

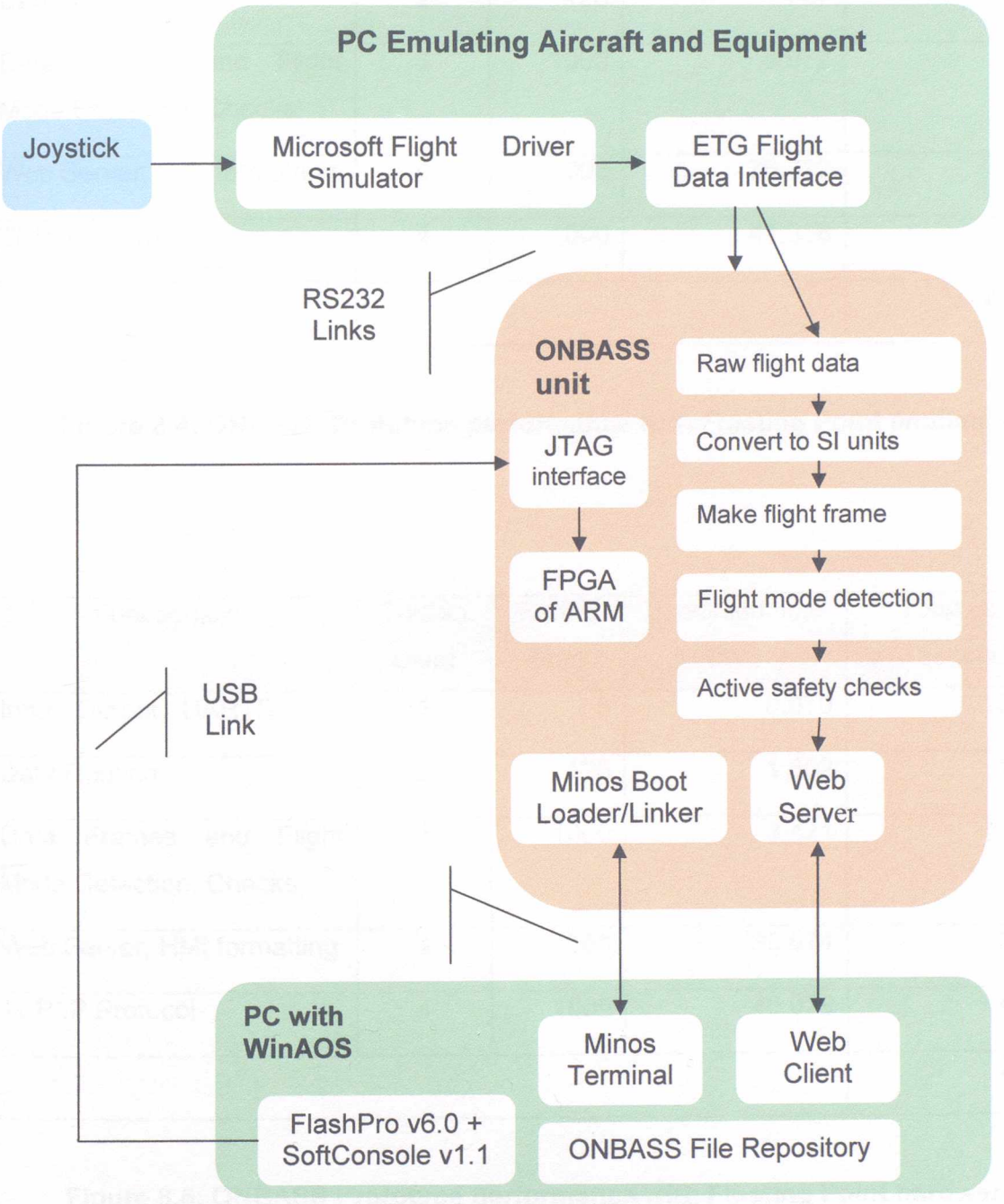


Figure 8.4 ONBASS Development and Simulation Environment

The performance of the system is summarised in the Tables 8.5 and 8.6, with and without floating point hardware. This has been done to assess the impact of floating point on overall performance because Prof Schagaev's fault tolerant processor will not include a floating point unit, it will be emulated.

Functionality	Thread Used	Period (ms)	Execution time (ms)	Total usage per second (ms)
Input- Output, UARTS	1	5	0.651	130.200
Data Routing	2	125	1.707	13.656
Data Frames and Flight Mode Detection, Checks	3	1000	5.972	5.972
Web Server, HMI formatting	4	1000	36.332	36.332
TCP/IP Protocol	4	1000	41.336	41.336
				227.496

Figure 8.4: ONBASS Prototype performance with Floating Point emulation

Functionality	Thread Used	Period (ms)	Execution time (ms)	Total usage per second (ms)
Input- Output, UARTS	1	5	0.670	134.000
Data Routing	2	125	1.302	10.416
Data Frames and Flight Mode Detection, Checks	3	1000	3.421	3.421
Web Server, HMI formatting	4	1000	35.974	35.974
TCP/IP Protocol	4	1000	40.029	40.029
				223.84

Figure 8.5: ONBASS Prototype performance with Floating Point hardware

8.3.3 *Conclusions Regarding Performance*

Some conclusions can be drawn from this analysis:

1. Only about 25% of processing capacity is used to service the whole Active Safety Monitor infrastructure. There is plenty of capacity available for implementing more sophisticated PASS versions of the system.
2. Floating point emulation (on the ARM) reduces calculation intensive performance to about 57% (3.421/5.972). However the software affected is only a small percentage of the whole - there is only a difference of 4 milli-seconds with/without the floating point hardware.
3. As Prof Schagaev's fault tolerant processor runs at 200 Mhz. It has a simpler instruction set than the ARM which may require more instructions for a given level of functionality. Even so it is likely that it will be able to support a full PASS application.
4. It may be feasible to run the whole system at 8 samples per second, however this would only make sense if sampled flight data is available at that rate.

8.4 Achieving Fault Tolerance

The MASS system uses fault tolerance techniques to improve the operational reliability of an aircraft. The first is to improve the safety of operation of the aircraft during each flight and over the life of an aircraft by early detection of operational faults and the use of preventive safety actions to mitigate their effect. The second is to use hardware and software fault tolerance techniques in the implementation of the MASS system to provide a reliable run time platform to ensure the availability of its service. Both of these techniques have the effect of improving the apparent reliability of the aircraft as an operational system.

The MASS system has several key subsystems (see Figure 8.1), each of which has different fault mechanisms, susceptibilities and tolerance design strategies; they are:

1. Aircraft Flight Data Processing Unit
2. MASS Flight Data Interface
3. MASS Flight Data Memory
4. MASS Evaluation Unit
5. MASS Independent Power Supply
6. Connectivity between system components
   via physical connections and data link protocols
7. Connectivity with the aircraft via interfaces to existing onboard equipment such as a Flight Data Computer or GPS receiver

All must operate reliably, and have continuous availability, some at least for the duration of a flight, others such as FDM over the life of the aircraft. The FDM must in addition be able to survive a crash and still be usable for recovery of flight data. On board the aircraft, the FDM, FDI and FDPU must be powered independently. This has now become a mandatory part of the regulations following incidents when power failure of the main aircraft power supply before/during a crash prevented the recording of or corrupted pre-crash data, just at the time when it could be most beneficial.

8.4.1 Reliability of connections

The reliability of connections between separate parts of any system are usually its 'weakest link' because of their physical vulnerability. This is even more evident in systems subjected to vibration, thermal cycling and humidity cycling – the normal environment for GA aircraft. Both electrical and radio based connections also are susceptible to the severe EMI generated on board GA aircraft including actuator motors, starter motors, ignition systems, radar etc. Also the radio frequency environment that CA, BA and GA aircraft fly through can contain intense radio/microwave radiation fields emanating from external sources such as approach radar, telecommunication links, military radar and tracking systems, high voltage pylons and of course electrical storms. It is important to carefully consider every aspect of connectivity in the system accordingly, as it will be a significant determinant of its overall system reliability.

8.4.2 The Importance of Availability

To achieve very high availability of operation over a lifespan of 30 years with absolutely minimal maintenance requires extreme reliability of the system. The traditional approach is to provide fault tolerance within the system by means of redundancy at the system component level. Typically this relies on having triplicated computers combined with an extremely reliable intrinsically fail safe 2 out of 3 voting element (often magnetically based) to isolate a single failing computer. Sometimes a 'hot swap' facility is included whereby the faulty computer can be replaced and then rejoin the system after learning the now current system state [79]. Such systems are very expensive and necessarily complex, this also makes their verification and validation expensive and time consuming (and some would say less than convincing). A further problem is that triplicate computer systems are not as reliable as simpler systems, simply because there is more hardware to go wrong. They only succeed in providing high availability of service by making it possible to 'hot swap' a faulty channel, this in turn infers that maintenance facilities must be available within a short period of time after a fault is detected to achieve an acceptable Mean Time To Repair. In addition some experts propose that each system should be diverse from the other two, i.e., implemented independently using different technologies for hardware and software. Even with this level of redundancy there is still no protection against common mode failures at the system level [82], e.g. a common software error in

the software specification for the triplicate computers or hardware errors simultaneously induced by an alpha particle shower even across diverse hardware designs.

In contrast, the basis for achieving reliability in MASS is to apply:

- Simplicity – using a single very high reliability processing system and avoiding the cost and complexities of a triplicate system.
- Built in hardware redundancy and concurrency to provide fault tolerance to avoid and/or mitigate the effects of random hardware failures and radiation based corruption.
- Software based enhancement of reliability by making software simple enough to be demonstrably correct and by compensating for recoverable errors indicated by the hardware i.e., software assisted repair of the hardware by reconfiguration.

In a practical implementation of MASS it is anticipated that hardware reliability will be optimised by the use of fault tolerant techniques. These provide built in protection from the effects of random failures and also the effects of radiation (i.e., alpha particles inducing electrical charge within semiconductor chips which in turn corrupts memory states and logic states). In addition, hardware and software algorithms can be used for improving the apparent reliability of the memory, e.g. the FDM by means of error detecting and correcting codes, based on Hamming principles. The key idea in all these schemes it to provide redundant memory on physically separate chips in order to support detection of errors, localisation of any corruption and correction of corrupted data.

For the Flight Data Processing Unit its fault tolerant (FT) design needs to be treated *as a whole* including the FT processor, FT RAM (to hold the program state), FT ROM (to hold the program), FT Flash (to hold the FDM) and the FT bus structure (to provide internal connectivity). As the amount of time and effort required to design, produce and properly test the FT FDM and FDPU is considerable and this has not been in the scope of this work, such a system is in the final stages of research by Prof Schagaev and his group.

9 Safety Information and Characterisation

In order to acquire the information to configure the PASS system for a specific aircraft the nature of the aircraft, the elements it is composed from and the parameter (sensor) values available need to be analysed. The process for achieving this is outlined in this Chapter. There are four prime sources of information that can potentially be used to characterise the system for a specific aircraft and so contribute to the improving its safety during operation, the main ones are:

1. The correlation between parameter values (i.e., sensor values or derived values calculated from them), in other words by monitoring whether different parameters retain their expected relations during each flight mode.
2. The transitions between flight modes, in other words how the flight mode is dynamically determined from the parameter values.
3. The dependency between elements, in other words whether the elements models show a discrepancy during each flight mode (indication the manifestation of a fault).
4. The Dictionary of Faults which defines the faults that can be detected by the MASS system and the recommended safety related responses to them, see section 9.4.

9.1 The Aircraft Characterisation Matrix

All of the configuration data can be brought together in the Aircraft Characterisation Matrix, the form of the ACM matrix is shown in Figure 9.1 below:

	Parameter Values	Elements	Flight Modes
Parameter Values	1 Parameter Correlation Matrix	4 Parameters Used by Elements Matrix	5 Parameter Limits per Flight Mode Matrix
Elements	9	2 Element Fault Dependency Matrix	6 Element Characterisation by Flight Mode Matrix
Flight Modes	8	7 Flight Mode Characterised by Elements Matrix	3 Flight Mode Transition Matrix

Figure 9.1: General Form of the Aircraft Characterisation Matrix

The matrix shown in Figure 9.1 is made up of nine sub-matrices, labelled 1 to 9, they are as follows:

1. The *Parameter Correlation Matrix* is a sub-matrix that has a row and column representing each of the parameter (or derived) values measured by the flight data acquisition unit. The content of each cell represent the expected correlation between the sensed values. Each pair of Parameter Values may have a set of correlation tolerance limits. This is described in more detail in section 9.2. This matrix can be used to detect faults during operation using a set of predicates which define the 'normal' relations between them.
2. The *Element Fault Dependency Matrix* defines the probability of propagation of faults between elements, it is defined in section 7.4.1. The content of each cell is the value of the probability between 0.0 and 1.0, in a simple implementation the probability can be considered to be Boolean (either influence or no influence), represented by 0.0 and 1.0. It may also contain a reference to the element predicates used to evaluate the next transition from the current flight mode. The Element Fault Recovery Matrix is effectively a 'shadow' of the Dependency Matrix as it has the same structure (but a different search algorithm). It contains references to the safety recovery actions required when an element is identified as the most likely to be causing a manifested fault.
3. The *Flight Mode Transition Matrix* is a matrix representation of the flight mode model described in section 9.2. It defines the transition also represented in XML in the Flight Mode Model in Appendix 4. Each cell also contains a data record with fields representing the threshold limits to be used in the Flight mode transition predicates.
4. The *Parameters Used by Elements Matrix* defines which parameter values are required by each element model. The way in which the parameter values are used is encapsulated in each element model.
5. The *Parameter Limits per Flight Mode Matrix* defines which parameter values need to have dynamically set limits on their acceptable values for each (or at least some) flight modes. A set of values may be associated with each cell (a data record) which defines the normal, warning, danger and critical values for each parameter (and some sensor's) value.
6. The *Element Characterisation by Flight Mode Matrix* defines which elements need to be characterised dynamically by the current flight mode. The way in which the flight mode is used is encapsulated in each element model. A set of values may be associated with each cell (a data record) defining the normal, warning, danger and critical limit values for evaluating the element's current fault status. These

limits can also be used in the graphic representation of values to the Pilot, some examples are shown in Figure 9.2.

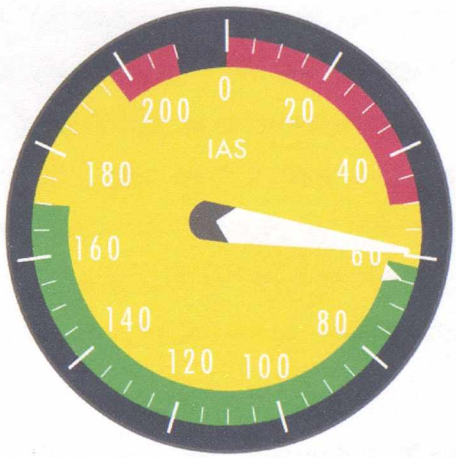
7. The *Flight Mode Characterised by Elements Matrix* defines which elements contribute to the determination of the current flight mode (if any). Note that care is needed to ensure that there are no dynamically 'circular dependencies' between this matrix and matrix 6 above via the element model; such a dependence could cause the flight mode to oscillate (dither) between its values.
8. This sub-matrix is VOID as parameter values are not affected by flight modes.
9. This sub-matrix is VOID because parameter values are not affected by elements.

Danger of Stall to Uncontrolled Descent !

Cruising in Normal Flight

Cruising in Normal Flight

(alternative design)



Warning – about to Stall!

Figure 9.2: Representation of threshold limits for pilot warnings

9.2 The Parameter Correlation Matrix

The parameters available for the Piper Lance aircraft are listed below:

1. GPS Time
2. Pressure altitude
3. Indicated air speed
4. Heading
5. Outside air temperature
6. Ground Speed
7. Drift angle
8. Wind speed
9. Wind direction
10. Latitude/Longitude
11. Right engine fuel flow (twin only) (redundant, single engined)
12. Left (or single) engine fuel flow
13. Barometric pressure setting
14. True air speed
15. Mach speed
16. Density altitude
17. True air temperature
18. Rate of turn
19. Vertical speed
20. Fuel remaining
21. Track
22. Distance to next waypoint
23. Magnetic variation
24. Baro-corrected altitude

This section gives an example of the process behind analysis of the Parameter Correlation matrix for the Piper Lance aircraft based on these parameters; it is illustrated in Figure 9.3. In this matrix an '*' signifies that the parameter in the row has a correlation (in some 'direct' sense) with the parameter of respective column. A blank cell value correspondingly signifies no relation. The link between parameters can be either unidirectional, or bidirectional. For example, in the above matrix, the ground speed of an aircraft is the vector sum of the aircraft's True Air Speed (TAS) and the wind speed. Thus, the Ground Speed depends on the True Air Speed, the wind speed and the wind direction. In contrast it is clear that the wind speed and wind direction do not depend on the True Air Speed or Ground Speed of the aircraft, this is illustrated in Figure 9.4. In general the correlation between parameters will be modelled by equations (e.g. polynomial, best fit) or tables.

There are data and/or parameters that are not directly available in real time in the aircraft that will have to be pre-configured in the software so as to support the determination of the specific dependency between parameters. For example, on the one hand it is demonstrated that all speeds defined in relation to the aircraft are interrelated as illustrated in the matrix, but on the other hand, these speeds also depend on a series of parameters which are not available in real time to the system and hence need to be pre-configured and loaded along with the software core.

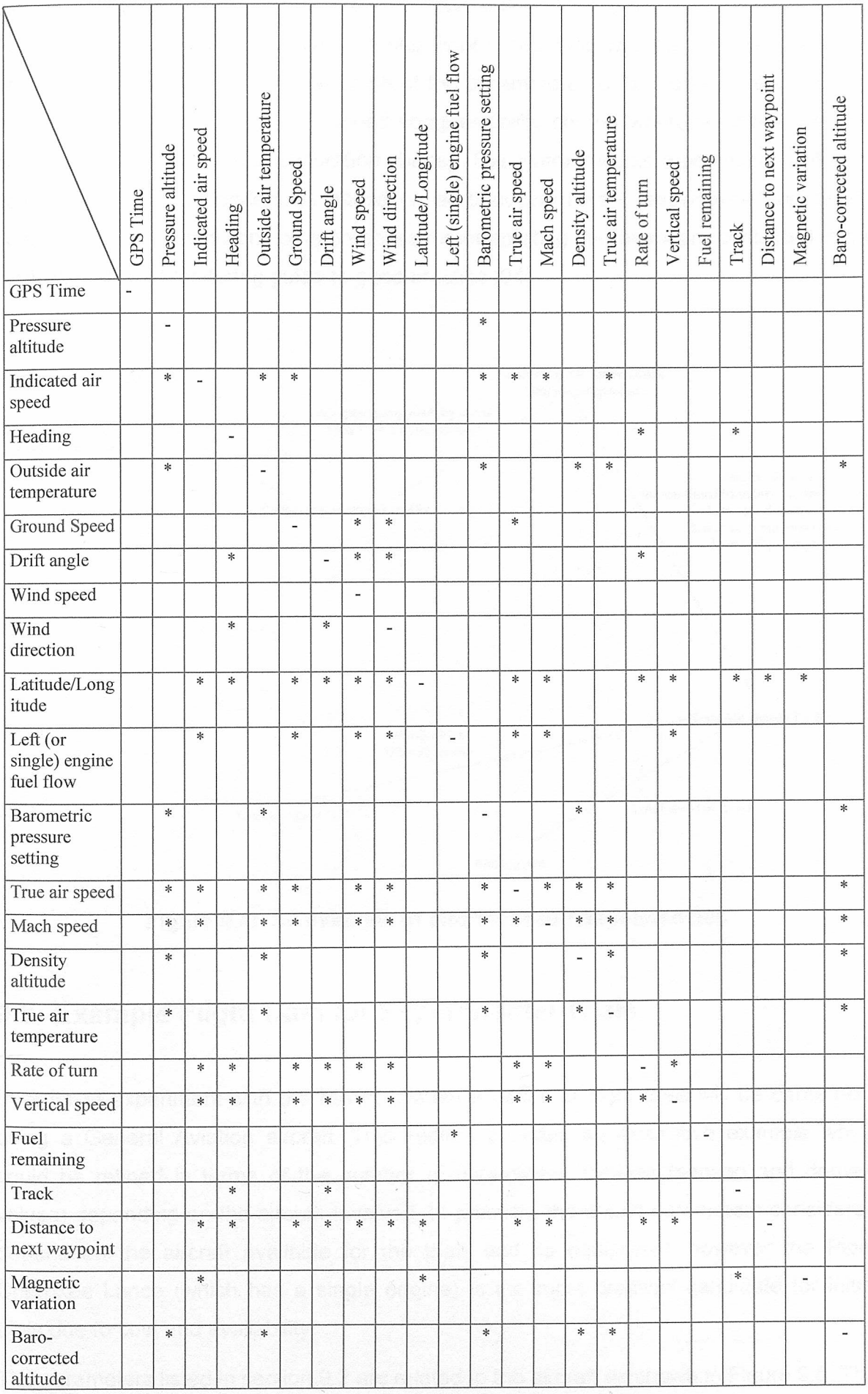


Figure 9.3: Example of a Parameter Value Correlation Matrix

An example is given in Figure 9.4 below where (red-coloured) text in *italics* has been used to distinguish between the parameters available and those not available in real time. Parameters in red text are available during flight in real time whereas all others are not. Another point to note here is that some of the parameters not available in real time are aircraft independent (e.g. the air speed compressibility charts) whereas others are very much so (e.g. the air speed calibration charts). The matrix reflects a preliminary effort to define parameter dependencies based on aeronautical theory, experience and expert opinion. Further discussions of approaches for interpreting the matrix are contained in the CAA Flight Data Monitoring guide to good practice [94]

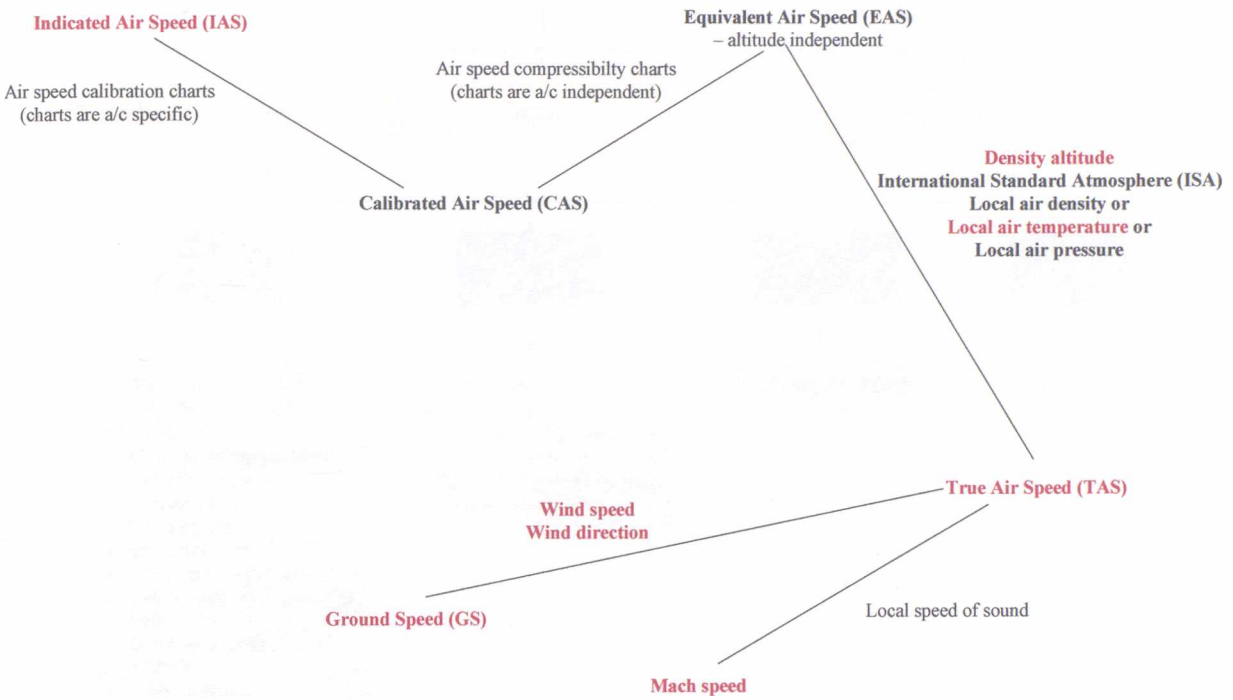


Figure 9.4: An example of aircraft speed dependencies

9.3 Example Flight Data for Experimental Trials

In order to experiment with the MASS system a series of flight trials will be carried-out using a General Aviation aircraft. This section provides an illustrative example which could be refined in terms of the number of parameters involves (sensed and derived values) depending on the aircraft involved. In practice, the actual parameters considered depend on the aircraft available for the trials and its equipment; however the Piper Cherokee Lance (which has a single engine) is the most practical candidate for initial trials due to cost and availability.

The parameters listed in section 9.2 are related to the aircraft as shown in Figure 9.5. The aircraft elements (as discussed previously) are divided into three categories: the

Airframe/Structure, the Engine and Systems. For this example only four elements are identified for which data/parameters are available (and they all belong to the 'Systems' category); these are the Air Data Computer, the GPS Unit, the Altitude Encoder and the Slave Gyro. The parameters acquired from each of these elements are listed and wherever more than one source for a parameter is available the parameter appears in italics. This redundancy also offers the opportunity to cross check the values for consistency in the element models with the potential for identifying and locating additional faults.

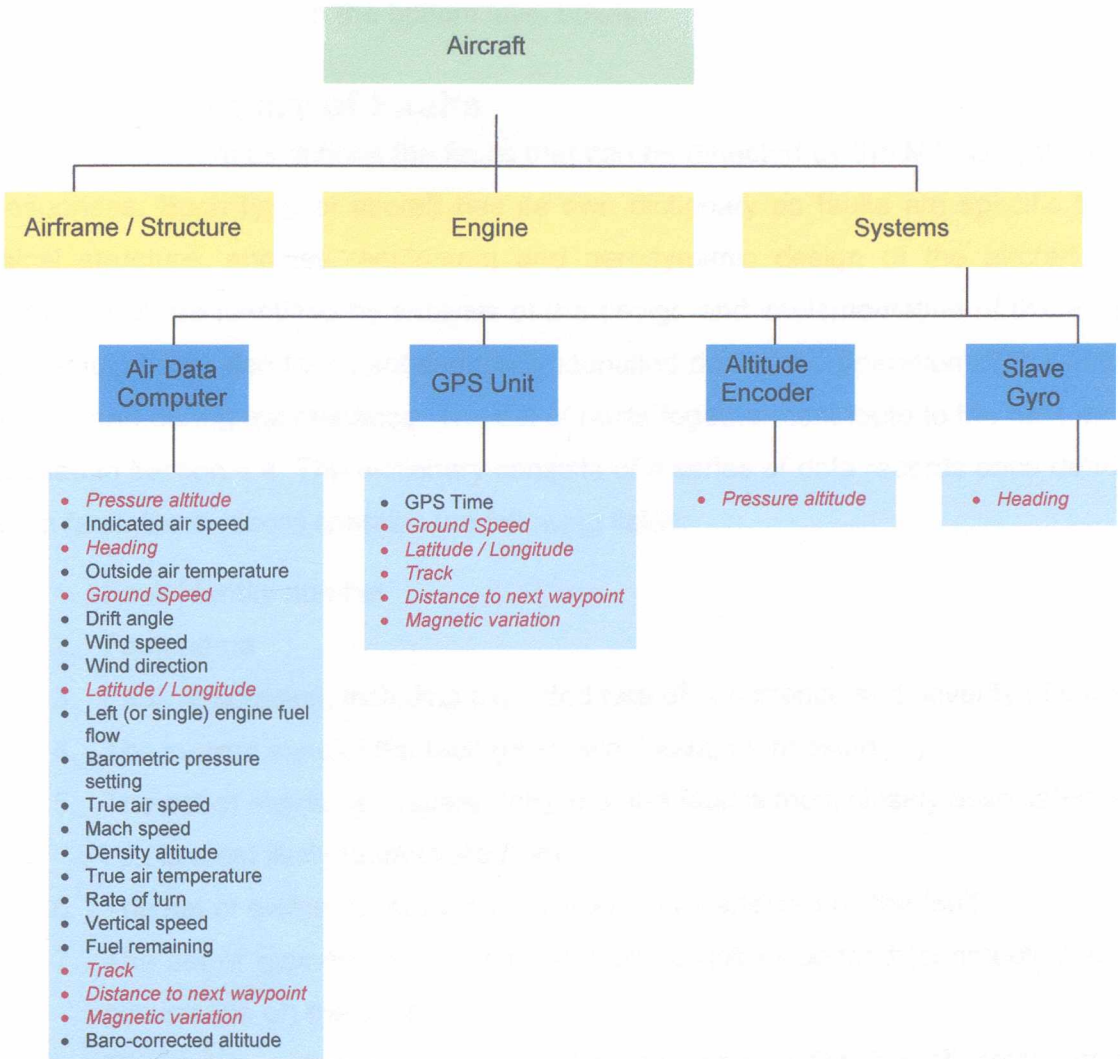


Figure 9.5: How the values relate to the aircraft

Following this categorisation, it is possible to define trends/patterns in data 'evaluation' as elements. For example combinations of parameter values and/or thresholds, can be used to monitor the operation of the four previously mentioned aircraft elements and thus evaluate whether an element has gone 'faulty', or continues to operate in a 'healthy' manner. So these parameters provide data which may be used (as described) to assess the failure status of the Air Data Computer, the GPS Unit, the Altitude Encoder and the Slave Gyro. The parameters also provide some data which can be used to assess the condition/status of further aircraft elements from which there are no direct inputs, e.g. the

aircraft landing gear, engine or aircraft fuselage, wings, rudder etc. Of course, more data relating to the specific aircraft would be required to be built-in to the software core (such as fuel consumption versus range algorithms, yield loading for the fuselage, wing(s), rudder etc) for such assessments to be made.

Given the incorporation of this extra data, an example of the data/parameters that could be used to assess the condition/status of the various aircraft elements is represented in Figure 9.4. Note that the aircraft's elements are signified by the boxes below the 'system' box, the element categories are in boxes below them and finally the relevant (available real-time) parameters are in the bottom level boxes.

9.4 The Dictionary of Faults

The Dictionary of Faults defines the faults that can be detected by the MASS system and its responses. Each type of aircraft has its own dictionary as faults are specific to the physical structure, engines, equipment and aerodynamic design of the aircraft. The potential faults are identified by analysis of the design and implementation of the aircraft and its equipment; also faults subsequently identified during the operation of the aircraft in service and during maintenance. The set of faults together contribute to the fault model discussed in section 4.4. The dictionary consists of a series of data records each defining a single fault. Each record contains the following fields:

1. Fault identity number
2. Fault name
3. Fault description, including expected rate of occurrence and severity of impact
4. The current state of the fault (unknown, latent, manifested ...)
5. The set of elements (usually one) that the fault is most closely associated with i.e., is most likely to emanate from
6. The set of elements that are most likely to be affected by the fault
7. The set of elements that are most likely to has influenced (contributed to the occurrence of) the fault
8. The safety action that is most likely to improve the overall safety of the operation of the aircraft in real time; this may be a set of actions each differing depending on the current flight mode (which may be changing dynamically during operation)
9. The MASS message to be provided to the Pilot and Crew in order to conserve or improve safety, for example 'Danger of stalling – increase airspeed now!'
10. The log message associated with the action for the flight data memory.

9.5 A Process for Active Safety Configuration Analysis

The process for acquiring the values for the Aircraft Characterisation Matrix is iterative and based of an expert's analysis of the aircraft and its operation on the ground and in flight. The process has the following steps:

1. Obtain the Design, Flight Operation and Maintenance Manuals for the aircraft being considered and details of modifications and enhancements made to it.
2. Produce the Dictionary of Faults for the specific aircraft based on an analysis of the structure of the aircraft, its functional subsystems, it main elements and its operational flight cycle and whole lifecycle.
3. Decide on the operational Flight Mode model that will be used, including the set of parameters that are required to model it in real time, the actual flight mode states and the transition predicates between states. Complete the Flight Mode Transition Matrix.
4. Create the Parameter Correlation Matrix by identifying all the parameters available to the MASS system from the flight Data Interface and other devices on board (e.g. GPS). Consider each parameter pairing in the matrix and mark the matrix to indicate and expected correlation. For each expected correlation characterise the nature of the correlation and the limits of any calculated values which represent the correlation.
5. Now consider the Parameter Limits per Flight Mode Matrix and decide whether the correlation needs to be characterised for each flight mode and if so refine the nature of the correlation and the limits of any calculated values for each flight mode. Decide the normal, warning, danger and critical thresholds.
6. Refine the choice of elements that will be used to provide the reference model the aircraft in flight for 'expected' behaviour (to judge actual faulty behaviour against). Define each element model in terms of the parameters available and complete the Parameters Used by Elements Matrix. Then define the algorithmic aspects of each model and its fault detection predicates.
7. Now consider for each element whether it is characterised by the flight mode and fill in the Element Characterised by Flight Mode matrix. For each element with flight mode dependency then define the nature of it and the additional fault detection predicates required for the relevant flight modes.
8. Also consider whether the flight mode is partially determined by each element and fill in the Flight Mode Characterised by Element Matrix. Check that there are no circular dependencies between this step and the previous step which would lead to the flight mode oscillating (some hysteresis may need to be built in)

9. Define the Element Fault Dependency Matrix based on the information already discovered and expert opinion of the relations that exist between the elements and the influence of fault propagation between them.

10. Define the Element Fault Recovery Matrix, this has the same structure as the Dependency Matrix and can be considered to be another layer of information of it. The content of each cell is a reference to the safety recovery action to be taken if the particular cell is found to be the prime cause any faulty behaviour. The safety actions are defined by experts on the aircraft and on its operation. Different search algorithms are used for tracing fault consequences (dependency matrix) and fault influences (recovery matrix).

11. Finally review the current elements identified and then consider *all the parameters not used in other element models* to all be a new element model. This 'default' element model is just used to check for parameter limit violations. This includes, for example, parameter values with multiple sources, the redundancy of which can be used to check for likely faults in the equipment providing the values i.e., consistency checking.

The whole process is then reviewed from step 2 onwards until elements have been encapsulated, all the matrices have been completed and all safety action defined for all faults in the Dictionary of Faults

10 State of the Art and Further Research

Active Safety is a new field of research and so there is relatively little material available describing the state of the art, a review is included in section 10.1 below. Even so there are example of early use of systems to improve operational safety, for instance the 'self righting' lifeboat, throwing sandbags out of a crashing air balloon and more recently Instrument Landing systems which improve the safety of the landing phase of the flight lifecycle. As with any emerging field it is difficult to 'get a handle' on how to frame the problem and until this is done it is impossible to develop systematic engineering solutions. Of course this situation has been encountered before and it well described in Vincenti's book 'What engineers know and how they know it' [1]. This book surveys the period of aircraft research and development when the basic problems were intangible issues like:

- Which phenomena and parameters affect flight and how can they be measured?
- What control surfaces are needed, how big should they be and what gearing should be used between the foot pedals and the control linkages ?
- What should the interface be between the Pilot and the Aircraft to achieve the best flight control with least mental and physical effort?
- What is the best shape of propeller and how fast should it be turning for best effect?

In some sense Active Safety is in the same sort of research phase, part theory and part exploration with progress being made by experimentation. In such a situation it is useful to learn from past failures; a (slightly cynical) review of design mistakes and operational safety mishaps is contained in John Gall's book Systemantics 'How systems work and how they fail' [1].

The field of Active Safety is ripe for research and whilst writing this thesis the author had a feeling of the field continually broadening as the research progressed; accordingly some ideas for future directions of the research are contained in section 10.2.

Finally it is now clear that the Principle of Active Safety and MASS could be applied in other application areas, not just in Aviation. A brief review is included in section 10.3.

10.1 The State of the Art in Active Safety

A search of the literature has revealed several approaches to safety and to active safety. The conventional approaches have been focused on improving reliability and availability of systems when they are designed, so called RAMS based approaches and these have been absorbed into the International Standards and have become 'conventional wisdom'. The Active Safety approach does not render any of these techniques obsolete; it should be viewed as a complementary technique which extends safety analysis and

improvement to the real time operation of the system. More recently the emphasis has been on 'integrated vehicle health' systems, basically another term for conditional maintenance; a useful review paper is [43].

10.1.1 The RAMS based approach to Safety

RAMS stands for Reliability, Availability, Maintainability and Safety. It is a design process which seeks to maximise all four components, although in practice it is only possible to optimise each at the expense of the others. An excellent review of the current standards is contained in [83] and a tutorial in [50]. The definitive standard for using RAMS is ISO 50126 'The Specification and Demonstration of RAMS' [84]. The techniques used are based around fault tree analysis, FMEA and hazard analysis. These are combined with standard statistical analysis reliability calculation as defined in Birolini's book [48] and the reliability handbook by O'Connor, Newton and Bromley [49]; common mode failures have also been investigated [82] and should be taken into account. The system architecture of RAMS based systems usually focuses on the use of multiple redundant implementations of system functions and some ultra reliable means of arbitration to decide which implementation to trust in the event of failures occurring. A major problem of this approach is its size, cost, weight and energy use and its ultimately self defeating nature: as the redundant systems become more and more complex the overall system reliability begins to decrease rather than improve. The main idea behind PASS *in the small* is to provide a means of implementation of safety related and safety critical systems which is inherently simpler, more reliable and more efficient than traditional RAMS based implementation. As mentioned before PASS *in the small* is the subject of a separate research project within Prof Schagaev's group.

10.1.2 Safety Standards

There are many standards for safety in general and systems safety in particular from ISO, EASA (Europe) and NTSB (USA); for the most part they concentrate on using the traditional techniques of fault tree analysis and reliability engineering over the lifecycle of the system or equipment concerned. None of the mainstream standards are concerned with the design of systems for operational safety improvement, the Shuttle disaster reviewed in section 4.2 demonstrated some limitations of 'conventional wisdom' and that approaches based on the conservation of operational safety and active use of redundancy are needed. The philosophy at the foundation of safety standards is reviewed in [85] , that analysis uses the CENELEC standards as a model. The basic approach, now also absorbed into the ISO standards (e.g. ISO 61598), is to classify faults and their effects according to the harm done (to life or to property) and the probability of fault occurrence. This leads to the concept of Safety Levels from SL0 to SL4, SL4 being the most stringent, demanding negligible harm and minimal probability of occurrence. The

USA Patent discussed in section 10.1.4 uses this concept as the basis for ranking faults in automotive applications..

In future the emphasis for standardization is likely to focus on process reliability enhancement based on the operation cycle and whole lifecycle of systems, as outlined in this thesis; the PASS concept can make a significant contribution in this area.

10.1.3 Russian Patent

During the search for 'prior art' when drafting the UK MASS Patent, see section 10.1.5, the Russian patent 'Active On-board Flight Safety System' [73] came to light. This patent deals with a specific aspect of Active Safety rather than a generalised concept and method. Its scope is concerned with fire safety on board the aircraft and the risks of burning fuel or running out of fuel before landing. It proposes transmission of safety data to a ground station. It also proposes choosing a landing site as local as possible, presumably so as much fuel as possible can be ditched. It contains an outline description of a safety device for monitoring the systems on board the aircraft, particularly in relation to the wellbeing of the crew, and reporting faults to the crew and ground.

10.1.4 USA/ German Patent

During the search for 'prior art' when drafting the UK MASS Patent, see section 10.1.5, the only 'prior art' cited by the UK Patent Examiner was USA patent US 2005/0223263 A1 [74]. The scope and claims of this patent are not considered by the UK Patent Agent to invalidate the claims of the UK MASS Patent which is based on material in this thesis. However the approach it takes is interesting, a summary is as follows:

The application domain of the patent is automotive control systems

The patent is concerned with the overall safety analysis i.e., it is about ensuring the safety of a system during the design process - it is a design methodology.

The system architecture is for a set of 'functions' which are encapsulated in the nodes of a communications network, messages pass through the network enabling the functions to collaborate as a system [78], [79].

The concept is about design time analysis of the intercommunication between functions to ensure that the locus of faults can be determined. In this respect it also uses the concept of dependency to trace paths through the communication network to search for the origin of fault manifestation in a particular function.

The safety evaluation method used is fault tree analysis and Failure Modes and Effects Criticality Analysis overlaid with the idea of assigning each fault (based on its effect on the system) into a classification based on the ISO safety levels (SL0 to SL4). Each safety level is associated with a probability of occurrence and a severity of harm (benign to lethal)

The design time safety analysis follows the conventional safety development 'V' model for verification and validation, verification down and up from layer to layer of the V and validation across each layer [85], [86].

In summary the contribution of this patent is to introduce the concept of searching paths in a communication network based on dependency and to introduce the standard ISO safety levels for ranking fault effects in terms of harm (safety impact).

10.1.5 UK MASS Patent

Some of the material in this thesis has been partially covered by the UK Patent Filing 0707057.6, 2007 'Method and Apparatus for Active Safety System'.

The patent describes and discloses the concept of the dependency and recovery matrices and the methods used for forward and backward searching and as such covers only PASS *in the medium.* The patent claims are listed in Appendix 5.

Further patents are envisaged to cover intellectual property involved in PASS *in the small* and PASS *in the large.*

10.2 Further Research and Refinements

During the research several topics have arisen which are either new or outside the scope of the work. This section reviews these areas and outlines some topics which could be the subject of future research in Active Safety.

10.2.1 Refine the MASS Concept

The scope of the MASS concept so far results in only safety advice being generated to conserve or improve safety during flight operations. The MASS concept itself could be refined and developed to:

1. Improve the discrimination of faults, their most likely causes and their impact. Presently only the most likely element is identified during the PASS analysis. In future the contribution of elements in the path of the cause (the influence) and the impact (the consequence) might be taken into account by developing algorithm(s) which take account of multiple contributions, inferences and effects.
2. Introduce automatic monitoring of actual dependencies between parameters and between elements during flight. This could be run as a background task during system operation. The concept here is to monitor actual operation to check that it is consistent with the way in which the system has been configured and also to seek dependencies that have not been anticipated. Such dependencies could then be used to refine the parameter and element model thresholds and thus improve the scope, sensitivity and effectiveness of MASS.

3. Introduce the concept of an Aircraft Safety Control Loop by coupling the output of MASS to the aircrafts Flight Control System. This would be the safety equivalent of an Autopilot, once engaged the Active Safety Management System would automatically modify the piloting of the aircraft to conserve and/ or improve safety.
4. Dynamically improve the apparent reliability of hardware systems.

10.2.2 Refine the Scope of Application

The MASS concept is not limited just to the scope of a single aircraft, it might be used at a larger of smaller scope. At a larger scope a system can be conceived which monitors the safety of, say, all aircraft in European airspace. Each aircraft might continually update a Safety Control Centre with its current safety status derived from its MASS system. At the control centre this information could be analysed and displayed, providing the safety equivalent of 'air traffic control'. Then if the MASS system on a particular aircraft indicates it is becoming marginally safe or unsafe preventive and corrective actions can be taken.

At a smaller scope within the implementation of the MASS, or other hardware, the PASS *in the small* concept could be used to dynamically improve the apparent reliability of hardware systems. Research in this area is already progressing based on the ERRIC ultra reliable reduced instruction set computer within Prof Schagaev's group. The concept here is to use dynamic fault detection to reconfigure redundant hardware, or repeat operations (time redundancy) in order to improve reliability (and hence system availability)

10.2.3 Refine Dependency Modelling

The dependency between elements in the Dependency and Recovery matrices is represented by a numeric probability in this thesis. Further research by Prof Schagaev has since yielded the concept of Graph Logic Language and modelling. The concept here is that the dependencies between nodes of the dependency graph can have logic relations associated with them i.e., AND, OR and XOR. This makes it possible to express graphs with Markovian and non-Markovian properties. I also make possible the definition of a richer and more accurate model to represent the physical and logical relations between the nodes (elements). Graph Logic is in the early stages of development. Future research is planned to introduce a computer language in which Graph Logic based solutions can be programmed, this could then possibly provide a more runtime efficient means to express and evaluate the graph equivalent of the Dependency and Recovery matrices.

10.2.4 Reliability and Maintenance

The actual practical rate of reliability degradation is a topic for further research. There seems to be little information in the literature on this topic however if methods can be

developed to measure or estimate the rate of degradation accurately then it will become possible to make major savings in routine maintenance of aircraft (and other complex multi-element systems). The lifecycle reliability calculations in this thesis are based on an assumption of a negligible period of maintenance; however a more accurate model could include a non-negligible period of maintenance. In the same line there are other factors that influence reliability and which should be included such as repair time, incomplete coverage of testing and quality of maintenance. It might also be interesting to investigate more advanced MASS properties and assumptions such as sensitivity to coverage of testing, reduction of maintenance time due to real time processing of flight data and whether maintenance quality is sustained when MASS is in use.

A better policy of preventive maintenance could be developed if the fundamental model includes some other factors such as *unavoidability* of preventive maintenance procedures and cost of maintenance. Both scenarios should be applied for preventive maintenance with and without MASS implementation. Such research would be required to convince insurance companies to join the GA market of general aviation.

10.2.5 Data Modelling

Some promising research topics in active safety Data Modelling are:

- How data from individual flights can be compressed in such a way as to conserve the information needed for aircraft lifecycle analysis (distillation of aircraft and operational trends)
- Efficient methods for data processing involving large volumes of aircraft lifecycle data
- Methods of expressing tangible common mode but non functional dependencies in the data, e.g. hydraulic and fuel pipes and electrical cables sharing the same conduit
- How to use the accumulated Flight Data Memory content to tune the parameter and element models in the long term, for example to correct for gradual drift in parameter checking limits and changes in element predicate limits.
- Whether regular automatic statistical analysis of the accumulated Flight Data can be used to tune a model of element dependencies by updating it with newly discovered dependencies and possibly excluding existing ones that are obsolete i.e., no longer significant. For an aircraft, this means that statistical analysis processing after each flight could provide automatic self-tuning of the MASS to take into account the changes in the condition of its elements.

10.2.6 Integrating PASS in Aircraft Design Tools

In order to define the Aircraft Characterisation Matrix described in section 9.1 special expertise is required from aviation specialists, manufacturers and maintenance engineers

for the chosen type of aircraft. In order to guide and standardise the approach a fruitful line of research would be to create design tools to ease this task. The objectives of the tools might be to:

- estimate and improve lifecycle reliability
- find problems early (e.g. safety inconsistencies)
- reduce fault dependencies that endanger safety
- promote efficiency of construction without compromising safety
- separation of concerns
- basis for insurance
- lower cost of ownership of the operational aircraft e.g. less maintenance

Such tools should be viewed as having two complementary purposes, firstly to provide a means of reliably configuring the system in a well structured and documented way and secondly to contribute to the simplification of the design and manufacture of the aircraft by anticipating the dependency between faults and seeking to minimise its overall effect during operational use.

The definition and creation of such tools would require a new research project.

10.2.7 Performance Optimisation for MASS

The experimental implementation of MASS used an ARM processor running at 200Mhz clock speed and this proved adequate for a parameter matrix of 24 parameters and an element dependency matrix of 4 elements. However in the Commercial Aviation domain these figures would rise to 1000 parameters and 50 elements and the real time processing requirements would rise accordingly (and unfortunately not always linearly). So in future it may become necessary to seek optimisation in order to minimise the computing resources needed during operation on the ground and in flight. A possible method for doing this would be to pre-compute the search paths through the element matrix by hypothesising a fault at each element node, before flight, and the calculating and storing the resulting 'most probable' path. Then at run time the search operation reduces solely to comparisons, the multiplication of cumulative probabilities having been completed during the configuration phase of the system operation. Alternatively these searches could be made when the system is initially turned on before a flight. Note that many redundant calculations would be made initially, however the real time analysis during operation would be much faster.

10.2.8 Devise a Verifiable Implementation

The prototype system would not be suitable for practical use in its present form as it would require certification before being put into service. One aspect of certification is the

need to verify the software of the system and this would not be possible given the ad-hoc nature of the user interface (HMI) implementation. As a minimum the internal webserver and TCP/IP stack software would need to be verified and also the browser used externally to render the user interface. It is likely, given market pressures, that such software components will be come available in the near future (by 2010). An alternative approach would be to implement the user interface in a more traditional manner, for example, using a dedicated Liquid crystal display and membrane keyboard. This would be a simpler and much more easily verifiable solution, but would lack flexibility for integration with other instrumentation and into other HMI schemes.

10.3 Further Applications of Active Safety

This thesis has focused on Active Safety in Aviation however the concepts and techniques could be used to bring the benefits of active safety to other application domains. The automotive market has always emphasised safety and most modern cars, trucks and buses contain a host of independent specific safety sub-systems. The General Aviation market is similar to automotive one in many ways (driver is responsible for operational safety, driver often is also responsible for maintenance ...) and it is conceivable that Active Safety will find automotive applications by integrating the localised safety sub-systems into a 'unified operational safety system'. The US Patent demonstrates the industry thinking of a few years ago and already it is clear that the data and communication infrastructure required to implement Active Safety exists within the in-car system.

Another possible application domain in the automotive domain is traffic flow control. In this case the PASS algorithm could be used to evaluate the consequence of faulty nodes (e.g. accident spots or road works) and the influence paths causing possible congestion. The safety actions could in this case be to dynamically re-route traffic away from the road network constriction. A similar concept could be used in the Rail domain to manage flow control on the rail network when faults occur (e.g. point, signal or engine failures). Mass could also be used on-board trains to monitor and manage their active safety and to reduce maintenance costs.

11 Summary and Conclusions

This chapter reviews the work on which this thesis is based including theoretical results and the experience of contributing to a practical implementation. It also considers the potential beneficiaries of the work and the benefits that can be accrued from it. This is followed by a set of conclusions summarising what has been learned and achieved, the contribution of the work to the field of Active Safety, the limits of what has been possible and the opportunities for further progress and improvement.

11.1 Summary

The thesis is in three parts. The first part is a survey of the domain of application (aviation) and its current state. The second part introduces the field of Active Safety and the Principle of Active System Safety (PASS) and then a practical implementation framework – the Method of Active System Safety. The third part contains supportive information for the first and second parts.

11.1.1 Active Safety in Aviation : The Context

Aviation is a huge and expanding application domain and in order to understand how Active Safety can make a contribution it is necessary to succinctly define 'the territory'. In chapter 2 this has been achieved by classification of the aviation and aircraft by mission (purpose), type of operation, technical characteristics and state of development. This, along with an analysis of the market for aircraft and its future trends has helpful to focus the research to ensure that the resulting Method of Active System Safety will have well defined, relevant and practical applications.

In order to understand the main safety issues in Aviation a study of operation safety related to risk of flight has been made in chapter 3 covering Commercial and General Aviation in detail. This has been achieved by analysing published incident and accident statistics and flight risks profiles to clarify the causes and impacts of incidents and accidents.

At a higher level flight safety is regulated and managed by safety management schemes; the current approach is reviewed and analysed. The conclusion from this is that there is much room for improvement and that real time monitoring and analysis of operational flight safety provides a basis for offering practical solutions to improve safety.

The technologies currently in use for flight data recording and safety monitoring are reviewed in Appendix 6 including its evolution, existing devices and opportunities for improved schemes and systems.

11.1.2 The Principle of Active Systems Safety (PASS)

Part 2 of the thesis starts in chapter 4 with a description of PASS and a refinement of the original work done by Prof Schagaev [3], [4], [5], [6]. It relates dynamic fault detection to

flight safety management and develops a generalised model. This is then related to the field of aviation in chapter 5 by creating a reliability model for aircraft operation and exploring relevant measures of system reliability i.e., point and mission availability. Active Safety is then analysed at 3 levels of abstraction: PASS *in the large* for the aircraft's reliability over its whole lifecycle of use, PASS *in the medium* for the reliability of each operational flight and PASS *in the small* for the reliability of the equipment used to support the implementation of PASS itself (i.e., MASS). PASS *in the small* is not analysed in detail as it is the subject of a separate, but related, research programme.

PASS *in the large* is analysed in chapter 6 in terms of conditional and preventive maintenance in order to derive a theoretical model for improving the reliability of the aircraft during its life. The key result is that using a PASS system continuously during flight operations can provide a significant improvement in overall operational reliability of the order of 20% over the aircrafts lifecycle. PASS *in the medium* is analysed in Chapter 7 in terms of an aircraft. The concept of viewing the aircraft as being composed of a set of interdependent elements is introduced along with a review of techniques for detection of anomalies in operational behaviour (symptoms of faults). The sensitivity of fault detection (and a refinement of its contextual relevance) is improved by relating the criteria for fault detection to the current flight mode of the aircraft's operation (e.g. during take-off or cruising)

The PASS algorithm for analysing the consequences of a fault manifested in one element on the other elements, based on a matrix defining inter-element dependencies, is described in detail and illustrated. A complementary algorithm for exploring the element most likely to be influencing the apparently faulty element is also described. Its operation is based on the same dependency matrix structure augmented with actions designed to improve the safety of the system.

11.1.3 Active Safety: From Theory to Practice

Theory by itself will bring no practical benefits, an implementation is needed to reap them; the converse is also true. Chapter 8 describes a design for a prototype of a system for implementation of PASS, this is called the Method of Active System Safety (MASS). It proposes a functional block diagram (see Figure 8.1) and an information processing model (see Figure 8.2) for its realisation. The structure of the software has been designed in a modular form and is being written in the Oberon language [77]. A prototype hardware and software system has been built by ETHZ Zurich, London Metropolitan University and Iroctech Grenoble. This system has been verified 'in the laboratory' using the Microsoft Flight Simulator to model the flight behaviour of a Piper Cherokee Lance aircraft. There are future plans to verify the prototype implementation in flight trials in a real aircraft once it has been equipped; this is part of the ONBASS project [75].

In order for MASS to be relevant for a particular aircraft the aircraft must be carefully characterised and then the MASS system configured accordingly. Chapter 9 describes the overall process needed to achieve this and gives an overview of the data structures required and their purpose. Finally the current state of the art in Active Safety is reviewed in Chapter 10 and different approaches are considered. The MASS Patent, which captures the essence of the originality of this thesis is briefly described and the 'Patent Claims' are provided verbatim in Appendix 5. A review of patents covering similar Intellectual Property makes it evident that the thesis is original and that Active Safety is of practical interest.

11.2 Conclusions

The main conclusions drawn from the research are as follows:

1. There is an opportunity to improve safety management in aviation by introducing the Method of Active System Safety. This would improve the reliability of flight operations and safety.

2. From a theoretical point of view the operational reliability of a typical aircraft can be improved by the order of 20% over its lifecycle. This would result in a significant reduction in the cost of maintenance, higher availability for operational use and a reduction in the likelihood of incidents and accidents in the most risk prone phases of flight.

3. The classification developed for aircraft indicates that MASS could be widely applicable in Commercial, Business and General Aviation.

4. The real time analysis of operational reliability during flight can be used to significantly improve safety management schemes. It provides the opportunity for unavoidable monitoring of the fault condition of an aircraft and a strong contribution to the crucial 'fly-no fly' decision made before every flight.

5. The prototype MASS implementation confirms that a highly reliable product could be developed at a feasible cost for widespread application in Aviation.

6. There are opportunities for further research to improve the theory and application of Active Safety (section 10.2) both in the scope of its application and in the refinement of its theory, techniques and implementation.

7. The Principle of Active System Safety could be used as a process in the design of aircraft to improve operational reliability 'by design'. In other words by continuously analysing the emerging design for fault dependence with a view to improving operational safety the design itself will become more safety resilient. This 'intrinsic' safety management could be just as important as the 'additive' safety management achieved by incorporating MASS based safety monitoring.

8. Other application domains could benefit from the incorporation of PASS theoretical modelling and MASS implementation (section 10.3).

9. The availability of a MASS safety device in aircraft opens the way for tighter regulation of their operation and safety. Its effect might be similar to safety improvements achieved by the mandatory use of Tachometers in road transport.

10. The patenting of MASS (originally invented by Prof Schagaev) secures the intellectual property that has been further developed in this thesis; the detailed claims are contained in Appendix 5. The next stage of research is for the timely, practical and expedient promotion of its use.

12 References

[1] Bukov V., Kirk B. and Schagaev I.,
Applying the Principle of Active Safety to Aviation
EUCASS 2nd European Conference for Aerospace Sciences, Brussels, Belgium, 2007.
http://www.vki.ac.be/eucass2007/index.html, accessed 29th January 2008.

[2] Bukov V., Kirk B., and Schagaev I.,
Analytical Synthesis of Aircraft Control Laws
EUCASS 2nd European Conference for Aerospace Sciences, Brussels, Belgium, 2007.
http://www.vki.ac.be/eucass2007/index.html, accessed 29th January 2008.

[3] Schagaev I.,
Concept of Dynamic Safety for Aeroplanes,
Air Fleet Herald, Issue 7, 1996

[4] Schagaev I.,
CoDySa – Concept of Dynamic Safety,
Proceedings of International System Safety Society, Seattle, 1998

[5] Schagaev I, Overtoon L.,
Active Safety System for General Aviation
Proceedings of 17th International System Safety Conference, Orlando, Florida, USA, 1999
http://www.system-safety.org/Conference99/Orlando99.htm, accessed 29th January 2008.

[6] Schagaev I.,
CASSA - Concept of Active System Safety for Aviation
Proceedings of 15th IFAC Symposium on Automatic Control in Aerospace,
Bologna/Forli, Italy, 2001.
http://www.bentham.com/publications/?id=392&PHPSESSID=1d9f09bf6b766a54595ded3b04442fd3, accessed 29th January 2008.

[7] Michie D., Spiegelhalter D. and Taylor C. (eds),
Machine Learning, Neural and Statistical Classification
Ellis Horwood, UK, 1994.
Book is available online at http://www.amsta.leeds.ac.uk/~charles/statlog/, accessed 29th January 2008.

[8] Gosling G. and Speyer J.,
Role of Analytical Tools in Safety Management Systems
Presentation: Seventh GAIN World Conference Montreal, Canada, September, 2004.
http://www.tc.gc.ca/tdc/events/2004/gain.htm , accessed 29th January 2008.

[9] US Air Force Auxilliary Civil Air Patrol (CAP)
Civil Air Patrol Guide to Operational Risk Management, USA.
http://level2.cap.gov/documents/Guide_to_ORM.pdf, accessed Oct 2007.

[10] International Council of Aircraft Owner and Pilot Associations (IAOPA)
Statistical Report World Assembly, April 2004.
http://www.iaopa.org/info/assembly22/stat22.html , accessed Oct 2007

[11] General Aviation Manufacturers Association
General Aviation Statistical Handbook, 2006, USA
http://www.gama.aero/dloads/2006GAMAStatisticalDatabook.pdf , accessed Jan 2008

[12] United States GAO (General Accounting Office)
General Aviation Status of the Industry, Related Infrastructure, and Safety Issues
Report to Congressional Requesters GAO-01-916 , August 2001, USA.

[13] http://www.aeroflight.co.uk/types/international/aerospat-bac/concorde/concorde.htm

[14] Weener E.,
Commercial Aviation Safety for 21st Century,
ISSSC, September 1998, Seattle, USA.

[15] National Transportation Safety Board
Annual Review of Aircraft Accident Data U.S. General Aviation Calendar Year 2001
http://www.ntsb.gov/publictn/2006/ARG0601.pdf , accessed Oct 2007

[16] NTSB (National Transportation Safety Board)
Annual Review of Aircraft Accident Data - U.S. General Aviation, Calendar Year 1998
http://www.ntsb.gov/publictn/2003/ARG0301.pdf , accessed Oct 2007

[17] National Transportation Safety Board
Annual Review of Aircraft Accident Data - U.S. General Aviation, Calendar Year 1999
http://www.ntsb.gov/publictn/2003/ARG0302.pdf , accessed Oct 2007

[18] National Transportation Safety Board
Annual Review of Aircraft Accident Data - U.S. General Aviation, Calendar Year 2000, NTSB/ARG-04/01, June 2004
http://www.ntsb.gov/publictn/2004/ARG0401.pdf, accessed Oct 2007

[19] AOPA Air Safety Foundation
Nall Report 2001 - General Aviation Accident Trends and Factors for 2000
http://www.aopa.org/asf/publications/01nall.pdf , accessed Oct 2007.

[20] AOPA Air Safety Foundation
Nall Report 2003 - General Aviation Accident Trends and Factors for 2002
http://www.aopa.org/asf/publications/03nall.pdf , accessed Oct 2007

[21] Federal Office for Accident Investigation, Germany,
"Bundesamt für Unfalluntersuchung"
http://www.bfu-web.de, accessed Oct 2007.

[22] Australian Transport Safety Bureau, 2005
http://www.atsb.gov.au/, accessed January 2008

[23] Civil Aviation Authority Safety Regulation Group
CAP 673 - Aviation Safety Review
CAA, UK, May 1997, www.caa.co.uk, accessed Oct 2007.

[24] Civil Aviation Authority Safety Regulation Group
CAP 667 - Review of General Aviation Fatal Accidents 1985- 1994,
CAA, UK, March 1997, www.caa.co.uk, accessed Oct 2007.

[25] Boeing Corporation, Summary of Airplane Accident Statistics 1959 to 2006
http://www.boeing.com/news/techissues/pdf/statsum.pdf , accessed Oct 2007

[26] National Transportation Safety Board: Safety Statistics Home Page
Summary of Accident Statistics, USA
http://www.ntsb.gov/aviation/Stats.htm, accessed Oct 2007

[27] Faraci V.,
Calculating Probability of Failure (Markov vs FTA)
Journal of the Reliability Analysis Centre, Third Quarter, 2001
http://src.alionscience.com/pdf/1Q2006.pdf, accessed 29th January 2008.

[28] Aviziensis A., Laprie J-C.and Randell B.,
Fundamental Concepts of Computer System Dependability
IARP/IEEE-RAS Workshop on Robot Dependability, May 21-22, Seoul, Korea, 2001

[29] International Symposium on Transportation Recorders
May 3 - 5, 1999, Arlington, Virginia, USA.

[30] FAA Statistics Home Page
http://www.faa.gov/data_statistics/ , accessed 29th January 2008.

[31] Warren D.,
"Father of the Black Box" http://news.bbc.co.uk/1/hi/sci/tech/2640793.stm
Introduction about Dr Dave Warren http://www.dsto.defence.gov.au/page/3383/
History of the Black Box http://www.dsto.defence.gov.au/page/3384/
Biography of Dr Dave Warren http://www.dsto.defence.gov.au/page/3246/
All accessed 29th January 2008.

[32] Brooks J.,
Flight Data/Cockpit Voice Recorders,
Smiths Industries, USA
http://www.ntsb.gov/Events/symp_rec/proceedings/authors/brooks.htm , accessed 29th January 2008.

[33] EUROCAE Working Group 50
Minimum Operational Performance Specification For Airborne Recorders For Accident Investigation, Nov 2004 and
Environmental Specifications for Avionics, EUROCAE ED-14 / RTCA DO-160D.
See also: accessed January 29th 2008.
http://www.ntsb.gov/Events/symp_vr_toptec/Presentations/Panel_1/aviation_elliott.pdf

[34] Horne M.,
Image Recording on Commercial Aircraft
NTSB Symposium on Transportation Recorders, Arlington, 2003.
http://www.ntsb.gov/Events/symp_vr_toptec/Presentations/Panel_3/aviation_horne.pdf
accessed 29th January 2008.

[35] EUROCAE WG50, Subgroup 3
Fundamental Needs For On-Board Image Recording
Agreed Final Draft, 27th Sept., 2001.

http://www.airmanshiponline.com/30sept2003/22b-Cockpit%20Video%20Recorder.pdf accessed 29th January 2008.

[36] Ferrie J.,
Airbourne Electronics – Evolution and Future Trends
Royal Aeronautical Society invited lecture, 28th November, 2006.

[37] International Standards Organisation
Space systems: Safety requirements Part 3: Flight safety systems.
ISO/WD 14620-3, 2001.

[38] Federal Aviation Regulations (FAR) 121.343, Flight Parameter Specifications,
http://www.risingup.com/fars/info/121-index.shtml

[39] Schagaev I., Schagaev A., Kirk B.,
Method and Apparatus for Active Safety System
GB Patent Filing 0707057.6, UK, 2007.

[40] Pakstas A., Schagaev I. and Zalewski J.,
Redundancy Classification For Fault Tolerant Computer Design
IEEE TESADI-01, Tucson, Arizona, October 2001, USA.
http://de.scientificcommons.org/589752, accessed Oct 2007.

[41] Nelson V., Carroll B.,
Tutorial: Fault Tolerant Computing,
Washington D C, IEEE Computer Society Press, Los Angeles, CA, USA, 1987

[42] Schneider W.,
Active Safety Systems
Radar Conference, Proceedings of EURAD 2005 6-7 Oct. 2005 pp:169-172.

[43] Fudge M., Stagliano T. and Tsiao S.,
Non-Traditional Flight Safety Systems & Integrated Vehicle Health Management Systems,
ITT Industries for FAA Section AST-300, August 2003
www.faa.gov/about/office_org/headquarters_offices/ast/media/DO3_Report_final.pdf
accessed 29th January 2008.

[44] NASA
Report of the Presidential Commission on the Space Shuttle Challenger Accident,
USA, 1986.
http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html, accessed Oct 2007

[45] Shuttle Orbital Management System – Propulsion
Queens University, Califirnia, 2001.
http://me.queensu.ca/courses/MECH497/Queens/2001/3/report/2-4.htm, accessed Oct 2007

[46] NASA Ames Research Centre
Shuttle Black Box announcement, USA, 2005
http://www.nasa.gov/centers/ames/multimedia/images/2005/blackbox.html

[47] Feynman R.,
Challenger Report: Appendix F - Personal observations on the reliability of the Shuttle,
http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt
accessed 29th January 2008.

[48] Birolini A.,
Reliability Engineering: Theory and Practice, 4th Edition
Springer Verlag, ISBN 354040287X, 2004.

[49] O'Connor P., Newton I. and Bromley R.
Practical Reliability Engineering
Wiley, ISBN 0-470-84463-9, UK.

[50] Rausand M, Failure Modes, Effects, and Criticality Analysis
http://www.ntnu.no/ross/srt/slides/fmeca.pdf , October, 2005.

[51] Dijkstra E. W.,
A Discipline of Programming
Prentice Hall, ISBN:013215871X,USA, 2007.

[52] Avizienis A., Ying W. N.,
A Unified Reliability Model for Fault Tolerant Computers
IEEE Trans. Computers, C-29, Vol.1, No.11, pp 1002-1011, Nov.1980.

[53] Stone R.,
REE Fault Tolerance Strategy (based on COTS),
Jet Propulsion Laboratory, Pasadena , USA

[54] Shannon C.,
A mathematical theory of communication

ACM SIGMOBILE Mobile Computing and Communications Review
SPECIAL ISSUE: Special issue dedicated to Claude E. Shannon
ISSN:1559-1662, pp 3-55, USA, 2001.

[55] Science Museum, London, UK.
Williams Tube and Mercury Delay Line Computer Storage
http://www.sciencemuseum.org.uk/images/I040/10307897.aspx,
accessed 28th January 2008.

[56] Schagaev I.,
Document D1.3: PASS in the Small,
London Metropoloitan University. Confidential to the ONBASS project, UK, 2006.

[57] Ruegger, B.,
Human error in the cockpit.
Swiss Reinsurance Company, Aviation Department, Zurich, Switzerland, 1990.

[58] Human Factors Design Guide (HFDG),
U.S. Department of Transportation, DOT/FAA/CT-96/0, USA, 1996
www.hf.faa.gov/docs/508/docs/**hfdg**_ch_5_update.pdf , accessed 29th January 2008.

[59] Chervonenkis A. and Vapnik V.,
On the Uniform Convergence of Relative Frequencies of Events to their Probabilities
Theory of Probability Applications Vol. 16, No. 2, pp261-280, 1971.

[60] Haussler D.,
Quantifying Inductive Bias, AI Learning Algorithms and Valiant's Learning Framework
Artificial Intelligence, Vol 36 pp177-221, 1988

[61] MacClure C.,
Industrial Mathematics, Prentice Hall, USA, 1999,
ISBN13: 9780139491993 or ISBN10: 0139491996

[62] Hall, J., Chairman of NTSB USA, Testimony to House of Representatives, USA
http://www.ntsb.gov/speeches/former/hall/jh971113.htm , accessed Oct 2007

[63] Reliability Analysis Centre
Applicability of Markov Analysis Techniques to Reliability , Maintainability and Safety
START, Volume 10, Number 2, Department of Defence, USA, 2002.
http://src.alionscience.com/pdf/1q2002.pdf , accessed 29th January 2008.
http://quanterion.com/RIAC/Publications/STARTSheets/PDFFiles/MARKOV.pdf

[64] Rausand M.,
Markov Processes and Kolmogorov Differential Equations in
Systems Reliability Theory,
Wiley Interscience, New York, USA
http://www.ntnu.no/ross/srt/slides/chapt8-1.pdf, accessed Oct 2007

[65] Criscimagna N.,
Meaningful Measures,
Journal of the Reliability Analysis Centre, 3rd Quarter, 2001, pp 22
US Department of Defence,

[66] Vincenti W.,
What Engineers Know and How they Know it
Johns Hopkins University Press, ISBN 0-8018-4588-2, USA, 1990.

[67] Gall J.,
Systemantics: How systems work and especially how they fail
General Systemantics Press, USA, 1970.
http://www.generalsystemantics.com/Systemantics.htm, accessed 29th January 2008.

[68] Turnbull A.,
The Typical General Aviation Aircraft
NASA, CR-1999-209550, USA, September 1999

[69] BBC News, Easy Jet Cutting Corners
http://news.bbc.co.uk/1/hi/business/2217280.stm, accessed on 29th January 2008, UK

[70] US General Accounting Office
Aviation Safety - Efforts to Implement Flight Operational Quality Assurance Programs
Report GAO/RCED-98-10, USA, Dec 1997
http://ntl.bts.gov/lib/000/700/762/rc98010.pdf , accessed 29th January 2008

[71] ARINC 700 Standard, www.arinc.com , accessed Oct 2007

[72] Simon H. A.,
The Structure of Ill Structured Problems
Artificial Intelligence, Vol. 4, No. 3, pp.181-201, 1975, USA.
http://citeseer.ist.psu.edu/simon73structure.html, accessed 29th January 2008.

[73] Russian Active Safety Patent
http://v3.espacenet.com/origdoc?DB=EPODOC&IDX=RU2223542&F=0&QPN=RU2223542
accessed 29th January 2008.

[74] Flores P. T., Lapp A. and Laengst W.,
Device and Method for Assessing the Safety of Systems and for Obtaining Safety in a System, and a Corresponding Computer Program
US Patent 2005/0223263 A1, October 6th, 2005

[75] European Commission: Contract of the 6th European Framework Program
Integrating and strengthening the European Research Area
Annex 1 - "Description of Work", Version 1.1, dd. 12/11/2004, for ONBASS.
Thematic Priority: Aeronautics and Space Contract: AST4-CT-2004-516045.

[76] Wirth N. and Gutknecht J.,
Project Oberon - The Design of an Operating System and Compiler
Addison Wesley, Wokingham, USA.

[77] Wirth N. and Reiser M.,
Programming in Oberon – Steps Beyond Pascal and Modula
Addison Wesley, Wokingham, USA.

[78] Kirk B., Harris T., Doyle S., Priestley T.,
Systems = Components + Languages : Building Flexible Real-Time Simulation and Test Environments
Joint Modular Languages Conference, 2003
Springer Verlag, Lecture Notes in Computer Science 2789
ISBN 0302-9743 and also in ISBN 3-540-40796-0

[79] Kirk B.,
System Architecture and Design using Cooperating Groups of Real and Abstract Components (to support redundancy in fault tolerant high availability safety systems)
Joint Modular Languages Conference, 2000
Springer Verlag, Lecture Notes in Computer Science 1897, ISBN 0302-9743

[80] Kirk B.,
Designing Systems with Objects, Processes and Modules
Proceedings of BCS Conference on Software Engineering 90
Brighton, UK, July 1990
also reprinted in
Microprocessors and Microsystems, Vol. 18, No. 3, April, 1994.

[81] Kirk B., Nigro L. and Pupo F.,
Using Real Time Constraints for Modularisation
Joint Modular Languages Conference 1997
Springer Verlag Lecture Notes in Computer Science 1204, ISBN 0302-9743

[82] Mauri G.,
PhD Thesis: Integrating Safety Analysis Techniques, Supporting Identification of Common Cause Failures,
Dept. Computer Science, University of York, UK, 2000.

[83] Rausand M.,
RAMS Standards and Guidelines
Norwegian University of Science and Technology (NTNU) Trondheim, Norway
http://www.ntnu.no/ross/info/standards.php, accessed 28th January 2008.

[84] International Standards Organisation
The specification and demonstration of reliability, availability, maintainability and safety
ISO EN 50126:1999, ISBN 058035694 9 .

[85] Schäbe H.,
The Safety Philosophy behind the CENELEC Safety Standards
TUV: ERSEL, Lyon, 2002

[86] International Standards Organisation
Functional safety of electrical/electronic/programmable electronic safety-related systems
ISO EN 61508-7:2003
See also http://www.iec.ch/zone/fsafety/fsafety_entry.htm, accessed 28th January 2008.

[87] International Standards Organisation
Communication, signalling and processing systems,
Safety related electronic systems for signalling.
See sections on: Safety Related communication in Open (part 1) and Closed (part2) transmission systems.
ISO EN 50129-1 and -2:2003 (previously CENELEC HD 485 S1:1987 and HD 617 S1:1992)

[88] The European Association of Aerospace Industries,
AECMA Specification 1000D
http://www.edocmagazine.com/vault_articles.asp?ID=29076

[89] US Department of Defence
Human Engineering
Standard MIL-STD-1472, (version F of August 1999 and version E of March 1998).
http://www.nssn.org , accessed 28th January 2008.

[90] http://en.wikipedia.org/wiki/Flash_memory#Flash_file_systems , accessed Oct 2007

[91] http://en.wikipedia.org/wiki/Piper_Cherokee_Six , accessed Oct 2007

[92] Piper Aircraft Corporation
Piper Cherokee Lance PA-32R-300 Information Manual,
Part Number 761-633, Vero Beach, Florida, USA, 2004.

[93] Bukov V. N., Chernyshov V.A., Kirk B., Schagaev I.,
Principle of Active System Safety for Aviation:
Challenges, Supportive Theory, Implementation, Application and Future
ASTEC'07 "New Challenges in Aeronautics", August 19–23, Moscow, 2007.

[94] CAA Safety Regulation Group
CAP 739 – Flight Data Monitoring: A Guide to Good Practice,
Civil Aviation Authority, UK, August 2003
www.caa.co.uk , accessed Oct 2007

[95] Extensible Markup Language (XML) 1.0 Specification (Fourth Edition)
http://www.w3.org/TR/xml , accessed on 23 October 2007

[96] Liu C.L. and Layland J. W.,
Scheduling Algorithms for Multiprogramming in a Hard Real Time Environment.
Journal of the ACM, 20(1):46-61, January 1973.

[97] Obenza R.and Mendal G.,
Guaranteeing Real Time Performance Using RMA,
The Embedded Systems Conference, San Hose, California, 1998.

[98] Williams F. C., and Kilburn T.,
A Storage System for use with Binary Digital Computing Machines,
Journal of the Institute of Electrical Engineers, 96(III):81-89, UK, March1949.

[99] Harvison R. E.,
M Sc Thesis: Current Input Negative Feedback Amplifier,
The Victoria University of Manchester, Manchester, UK, 1949.

Part 3: Supportive Information

13 Appendix 1: Abbreviations

a/c	Aircraft
A&P	Airframe & Power plant
ACARS	Aircraft Communications, Addressing and Reporting System
ACAS	Airborne Collision Avoidance Systems
AD	Airworthiness Directives
ADC	Air Data Computer
ADS	Automatic Dependent Surveillance
ADS-B	ADS – Broadcast
AEEC	Airline Electronic Engineering Committee
AERO	Aerobatics
AFTN	Aeronautic Fixed Telecommunication Network
AHRS	Attitude Heading Reference System
ANO	Air Navigation Order
AOPA	Aircraft Owners and Pilots Association
APALS	Autonomous Precision Approach Landing System
APASS	Algorithm of PASS
APU	Auxiliary Power Unit
AR	Advanced Recorders
ARINC	Aeronautical Radio Inc (now a USA Standards Provider)
AS	Active Safety
ASM	Air Space Management
ASR	Air Safety Reporting (BASIS module)
ATC	Air Traffic Control
ATD	Aircraft Training Devices
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
ATP	Airline Transport Pilot
ATS	Air Traffic Service
ATSB	Australian Transport Safety Bureau
AW	Aerial Work
BA	Business Aviation
BASIS	British Airways Safety Information System
CA	Civil Aviation
CAA	Civil Aviation Authority
CAD	Computer Aided Design
CAN	Controller Area Network
CDTI	Cockpit Display of Traffic Information
CENELEC	European Committee For Electro-technical Standardisation
CFIT	Controlled Flight Into Terrain
CFR	Code of Federal Regulations
CG	Centre of Gravity
CiA	CAN in Automation (organisation)
CIS	Cockpit Instrumentation System
CIU	Configuration and Interface Unit
CNI	Communication, Navigation, Information
CNS	Communications, Navigation and Surveillance
CPDLC	Controller Pilot Data Link Communication
CPU	Central Processing Unit
CRM	Cockpit Resource Management
CSR	Cabin Safety Reporting (BASIS module)
CVR	Cockpit Voice Recorder
DARP	Dynamic Aircraft Route Planning
DAU	Data Acquisition Unit
DFDAU	Digital Flight Data Acquisition Unit
DFDR	Digital Flight Data Recorder
DG	Director General
DGPS	Differential GPS
DME	Distance Measuring Equipment

DP	Departure Procedure
DU	Data Processing and Recording Unit
EASA	European Aviation Safety Agency
EFIS	Electronic Flight Instrument System
EGNOS	European Geostationary Navigation Overlay Service
EGPWS	Enhanced Ground Proximity Warning System
EICAS	Engine Indicating and Crew Alert System
ELT	Emergency Locator Transmitter
EN	European Norm (standard)
ERTMS	European Rail Transport Management System
ETH	Eidgenössische Technische Hochschule in Zurich, Switzerland
EU	European Union
EUROCAE	EUROpean organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FANS	Future Air Navigation Systems
FCS	Flight Control System
FDAU	Flight Data Acquisition Unit
FDE	Flight Data Exceedences (BASIS module)
FDM	Flight Data Measurements (BASIS module)
FDR	Flight Data Recorder
FDS	Flight Data Simulation (BASIS module)
FDT	Flight Data Traces (BASIS module)
FIS	Flight Information System
FIS-B	Flight Information Service – Broadcast
FLASH	Floating Gate Semiconductor Memory
FMC	Flight Management Computer
FMECA	Failure Mode Effects Criticality Analysis
FMEA	Failure Mode Effects Analysis
FSS	Flight Safety System
FTA	Fault Tree Analysis
FTS	Flight Termination System
GA	General Aviation
GAMA	General Aviation Manufacturers Association
GHR	Ground Handling Reporting (BASIS module)
GLL	Graph Logic Language
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GOR	Ground found Occurrence Reporting (BASIS module)
GPH	Gallons Per Hour
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HF	High Frequency (radio signal)
HFDL	High Frequency Data Link
HFR	Human Factor Reporting (BASIS module)
HIS	Horizontal Situation Indicator
HIS	Heading Station Indicator or Horizontal Situation Indicator
HMI	Human Machine Interface
HUD	Head-Up Display
IAOPA	International Council of Aircraft Owner and Pilot Associations
ICAO	International Civil Aviation Organisation
ICT	Information and Communications Technology
IEC	International Electro-technical Commission
ISO	International Standards Organization
IT	Information Technology
IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
INS	Inertial Navigation Systems
IrDA	Infra-red Data Association
IRS	Inertial Reference Systems
ISSSC	International System Safety Conference
IVHM	Integrated Vehicle Health Management
IVS	Instantaneous Vertical Speed

JAA	Joint Aviation Authorities
JAR	Joint Aviation Requirements or Joint Airworthiness Requirements
LAAS	Local Area Augmentation System
LOC	Loss Of Control
LOW	Low flying
LRU	Line Replaceable Unit
MA	Military Aviation
MASS	Method of Active System Safety
MEI	Maintenance Error Reporting (BASIS module)
MFD	Multi Functional Display
MLS	Microwave Landing System
MMR	Multi-Mode Receiver
MOPS	Minimum Operational Performance Specifications
MS	Microsoft Corporation
MSAS	Multi-transport Satellite-based Augmentation System
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
NASA	National Aeronautics and Space Administration
ND	Navigation Display
NDM	Non-Directional Beacons
NEXCOM	Next Generation Air Ground Communications
NM	Nautical Miles
NMEA	National Marine Electronics Association
NOTAM	Notices to Airmen
NTSB	National Transportation Safety Board (US)
OAT	Outside Air Temperature
OD	Objects of Danger
ODE	Ordinary Differential Equation
OMS	Orbital Manoeuvring System (Space shuttle)
ONBASS	Onboard Active Safety System
OS	Objects of Safety
PASS	Principle of Active Safety System
PCMCIA	Personal Computer Memory Card International Association
PDE	Partial Differential Equation
PFD	Primary Flight Display
PL	Project Lead
PM	Project Manager
QAR	Quick Access Recorder
RAM	Random Access Memory
RAMS	Reliability, Availability, Maintainability and Safety
RHSM	Reduced Horizontal Separation Minima
RLV	Reusable Launch Vehicle
RNAV.	Area Navigation
RNP	Required Navigation Performance
RT	Real Time
RTCA	Radio Technical Commission for Aeronautics (USA Federal Advisory Committee)
RTS	Range Tracking System
RVSM	Reduced Vertical Separation Minima
SIE	Safety Information Exchange (BASIS module)
SM	Safety Monitor
SMS	Short Message Service
SOC	System Of Checking
SSUFDR	Solid State Universal Flight Data Recorder
TREN	Transport Regulation European Norms (standards)
TSO	Technical Service Order or The Stationary Office
UK	United Kingdom
US	United States
USA	United States of America
USAF	United States Air Force
VMC	Visual Meteorological Conditions

14 Appendix 2: Glossary

Based on USA Federal Aviation Regulations

Air commerce means interstate, overseas, or foreign air commerce or the transportation of mail by aircraft or any operation or navigation of aircraft within the limits of any Federal airway or any operation or navigation of aircraft which directly affects, or which may endanger safety in, interstate, overseas, or foreign air commerce.

Aircraft means a device that is used or intended to be used for flight in the air.

Aircraft engine means an engine that is used or intended to be used for propelling aircraft. It includes turbo superchargers, appurtenances, and accessories necessary for its functioning, but does not include propellers.

Airframe means the fuselage, booms, nacelles, cowlings, fairings, airfoil surfaces (including rotors but excluding propellers and rotating airfoils of engines), and landing gear of an aircraft and their accessories and controls.

Aircraft means an engine-driven fixed-wing aircraft heavier than air that is supported in flight by the dynamic reaction of the air against its wings.

Airship means an engine-driven lighter-than-air aircraft that can be steered.

Air transportation means interstate, overseas, or foreign air transportation or the transportation of mail by aircraft.

Balloon means a lighter-than-air aircraft that is not engine driven, and that sustains flight through the use of either gas buoyancy or an airborne heater.

Canard means the forward wing of a canard configuration and may be a fixed, movable, or variable geometry surface, with or without control surfaces.

Canard configuration means a configuration in which the span of the forward wing is substantially less than that of the main wing.

Category:

(1) As used with respect to the certification, ratings, privileges, and limitations of airmen, means a broad classification of aircraft. Examples include: aircraft; rotorcraft; glider; and lighter-than-air; and

(2) As used with respect to the certification of aircraft, means a grouping of aircraft based upon intended use or operating limitations. Examples include: transport, normal, utility, acrobatic, limited, restricted, and provisional.

Category A, with respect to transport category rotorcraft, means multiengine rotorcraft designed with engine and system isolation features specified in Part 29 and utilizing scheduled takeoff and landing operations under a critical engine failure concept which assures adequate designated surface area and adequate performance capability for continued safe flight in the event of engine failure.

Category B, with respect to transport category rotorcraft, means single-engine or multiengine rotorcraft which do not fully meet all Category A standards. Category B rotorcraft have no guaranteed stay-up ability in the event of engine failure and unscheduled landing is assumed.

Civil aircraft means aircraft other than public aircraft.

Class:

(1) As used with respect to the certification, ratings, privileges, and limitations of airmen, means a classification of aircraft within a category having similar operating characteristics. Examples include: single engine; multiengine; land; water; gyroplane; helicopter; airship; and free balloon; and

(2) As used with respect to the certification of aircraft, means a broad grouping of aircraft having similar characteristics of propulsion, flight, or landing. Examples include: aircraft; rotorcraft; glider; balloon; landplane; and seaplane.

Forward wing means a forward lifting surface of a canard configuration or tandem-wing configuration aircraft. The surface may be a fixed, movable, or variable geometry surface, with or without control surfaces.

Glider means a heavier-than-air aircraft, that is supported in flight by the dynamic reaction of the air against its lifting surfaces and whose free flight does not depend principally on an engine.

Gyrodyne means a rotorcraft whose rotors are normally engine-driven for takeoff, hovering, and landing, and for forward flight through part of its speed range, and whose means of propulsion, consisting usually of conventional propellers, is independent of the rotor system.

Gyroplane means a rotorcraft whose rotors are not engine-driven, except for initial starting, but are made to rotate by action of the air when the rotorcraft is moving; and whose means of propulsion, consisting usually of conventional propellers, is independent of the rotor system.

Helicopter means a rotorcraft that, for its horizontal motion, depends principally on its engine-driven rotors.

Kite means a framework, covered with paper, cloth, metal, or other material, intended to be flown at the end of a rope or cable, and having as its only support the force of the wind moving past its surfaces.

Large aircraft means aircraft of more than 12,500 pounds, maximum certificated takeoff weight.

Lighter-than-air aircraft means aircraft that can rise and remain suspended by using contained gas weighing less than the air that is displaced by the gas.

Light-sport aircraft means an aircraft, other than a helicopter or powered-lift that, since its original certification, has continued to meet the following:

(1) A maximum takeoff weight of not more than--

(i) 660 pounds (300 kilograms) for lighter-than-air aircraft;

(ii) 1,320 pounds (600 kilograms) for aircraft not intended for operation on water; or

(iii) 1,430 pounds (650 kilograms) for an aircraft intended for operation on water.

(2) A maximum airspeed in level flight with maximum continuous power (VH) of not more than 120 knots CAS under standard atmospheric conditions at sea level.

(3) A maximum never-exceed speed (VNE) of not more than 120 knots CAS for a glider.

(4) A maximum stalling speed or minimum steady flight speed without the use of lift-enhancing devices (VS1) of not more than 45 knots CAS at the aircraft's maximum certificated takeoff weight and most critical centre of gravity.

(5) A maximum seating capacity of no more than two persons, including the pilot.

(6) A single, reciprocating engine, if powered.

(7) A fixed or ground-adjustable propeller if a powered aircraft other than a powered glider.

(8) A fixed or auto-feathering propeller system if a powered glider.

(9) A fixed-pitch, semi-rigid, teetering, two-blade rotor system, if a gyroplane.

(10) A non-pressurized cabin, if equipped with a cabin.

(11) Fixed landing gear, except for an aircraft intended for operation on water or a glider.

(12) Fixed or repositionable landing gear, or a hull, for an aircraft intended for operation on water.

(13) Fixed or retractable landing gear for a glider.

Main rotor means the rotor that supplies the principal lift to a rotorcraft.

Parachute means a device used or intended to be used to retard the fall of a body or object through the air.

Powered-lift means a heavier-than-air aircraft capable of vertical takeoff, vertical landing, and low speed flight that depends principally on engine-driven lift devices or engine thrust for lift during these flight regimes and on non-rotating airfoil(s) for lift during horizontal flight.

Powered parachute means a powered aircraft comprised of a flexible or semi-rigid wing connected to a fuselage so that the wing is not in position for flight until the aircraft is in motion. The fuselage of a powered parachute contains the aircraft engine, a seat for each occupant and is attached to the aircraft's landing gear.

Propeller means a device for propelling an aircraft that has blades on an engine-driven shaft and that, when rotated, produces by its action on the air, a thrust approximately perpendicular to its

plane of rotation. It includes control components normally supplied by its manufacturer, but does not include main and auxiliary rotors or rotating airfoils of engines.

Public aircraft means any of the following aircraft when not being used for a commercial purpose or to carry an individual other than a crewmember or qualified non-crewmember:

(1) An aircraft used only for the United States Government; an aircraft owned by the Government and operated by any person for purposes related to crew training, equipment development, or demonstration; an aircraft owned and operated by the government of a State, the District of Columbia, or a territory or possession of the United States or a political subdivision of one of these governments; or an aircraft exclusively leased for at least 90 continuous days by the government of a State, the District of Columbia, or a territory or possession of the United States or a political subdivision of one of these governments.

(i) For the sole purpose of determining public aircraft status, commercial purposes means the transportation of persons or property for compensation or hire, but does not include the operation of an aircraft by the armed forces for reimbursement when that reimbursement is required by any Federal statute, regulation, or directive, in effect on November 1, 1999, or by one government on behalf of another government under a cost reimbursement agreement if the government on whose behalf the operation is conducted certifies to the Administrator of the Federal Aviation Administration that the operation is necessary to respond to a significant and imminent threat to life or property (including natural resources) and that no service by a private operator is reasonably available to meet the threat.

(ii) For the sole purpose of determining public aircraft status, governmental function means an activity undertaken by a government, such as national defence, intelligence missions, fire fighting, search and rescue, law enforcement (including transport of prisoners, detainees, and illegal aliens), aeronautical research, or biological or geological resource management.

(iii) For the sole purpose of determining public aircraft status, qualified non-crewmember means an individual, other than a member of the crew, aboard an aircraft operated by the armed forces or an intelligence agency of the United States Government, or whose presence is required to perform, or is associated with the performance of, a governmental function.

(2) An aircraft owned or operated by the armed forces or chartered to provide transportation to the armed forces if--

(i) The aircraft is operated in accordance with title 10 of the United States Code;

(ii) The aircraft is operated in the performance of a governmental function under title 14, 31, 32, or 50 of the United States Code and the aircraft is not used for commercial purposes; or

(iii) The aircraft is chartered to provide transportation to the armed forces and the Secretary of Defence (or the Secretary of the department in which the Coast Guard is operating) designates the operation of the aircraft as being required in the national interest.

(3) An aircraft owned or operated by the National Guard of a State, the District of Columbia, or any territory or possession of the United States, and that meets the criteria of paragraph (2) of this definition, qualifies as a public aircraft only to the extent that it is operated under the direct control of the Department of Defence.

Rocket means an aircraft propelled by ejected expanding gases generated in the engine from self-contained propellants and not dependent on the intake of outside substances. It includes any part which becomes separated during the operation.

Rotorcraft means a heavier-than-air aircraft that depends principally for its support in flight on the lift generated by one or more rotors.

Rotorcraft-load combination means the combination of a rotorcraft and an external-load, including the external-load attaching means. Rotorcraft-load combinations are designated as Class A, Class B, Class C, and Class D, as follows:

(1) *Class A rotorcraft-load combination* means one in which the external load cannot move freely, cannot be jettisoned, and does not extend below the landing gear.

(2) *Class B rotorcraft-load combination* means one in which the external load is jettison-able and is lifted free of land or water during the rotorcraft operation.

(3) *Class C rotorcraft-load combination* means one in which the external load is jettison-able and remains in contact with land or water during the rotorcraft operation.

(4) *Class D rotorcraft-load combination* means one in which the external-load is other than a Class A, B, or C and has been specifically approved by the Administrator for that operation.

Small aircraft means aircraft of 12,500 pounds or less, maximum certificated takeoff weight.

Tandem wing configuration means a configuration having two wings of similar span, mounted in tandem.

Type:

(1) ...

(2) As used with respect to the certification of aircraft, means those aircraft which are similar in design. Examples include: DC-7 and DC-7C; 1049G and 1049H; and F-27 and F-27F.

(3) As used with respect to the certification of aircraft engines means those engines which are similar in design. For example, JT8D and JT8D-7 are engines of the same type, and JT9D-3A and JT9D-7 are engines of the same type.

Weight-shift-control aircraft means a powered aircraft with a framed pivoting wing and a fuselage controllable only in pitch and roll by the pilot's ability to change the aircraft's centre of gravity with respect to the wing. Flight control of the aircraft depends on the wing's ability to flexibly deform rather than the use of control surfaces.

Winglet or tip fin means an out-of-plane surface extending from a lifting surface. The surface may or may not

15 Appendix 3: Flight Data Parameter Sets

15.1 List of Flight Data Parameters in GA

There are 3 basic sets of parameters referenced in standard 14CFR12I343:

Minimal set of 6: (1) Time, (2) Altitude, (3) Airspeed, (4) Vertical acceleration, (5) Heading, (6) Time of each radio transmission either to or from air traffic control.

Enhanced set of 11: (1) Time, (2) Altitude, (3) Airspeed, (4) Vertical acceleration, (5) Heading, (6) Time of each radio transmission either to or from air traffic control, (7) Pitch attitude, (8) Roll attitude, (9) Longitudinal acceleration, (10) Control column or pitch control surface position, (11) Thrust of each engine.

Full set of 17: (1) Time, (2) Altitude, (3) Airspeed, (4) Vertical acceleration, (5) Heading, (6) Time of each radio transmission either to or from air traffic control, (7) Pitch attitude, (8) Roll attitude, (9) Longitudinal acceleration, (10) Pitch trim position, (11) Control column or pitch control surface position, (12) Control wheel or lateral control surface position, (13) Rudder pedal or yaw control surface position, (14) Thrust of each engine, (15) Position of each thrust reverser, (16) Trailing edge flap or cockpit flap control position, (17) Leading edge flap or cockpit flap control position.

15.2 Projected future flight parameters recorded in GA aircraft

(1) Time;
(2) Pressure altitude;
(3) Indicated airspeed;
(4) Heading-primary flight crew reference (if selectable, record discrete, true or magnetic);
(5) Normal acceleration (Vertical);
(6) Pitch attitude;
(7) Roll attitude;
(8) Manual radio transmitter keying, or CVR/DFDR synchronization reference;
(9) Thrust/power of each engine-primary flight crew reference;
(10) Autopilot engagement status;
(11) Longitudinal acceleration;
(12) Pitch control input;
(13) Lateral control input;
(14) Rudder pedal input;
(15) Primary pitch control surface position;
(16) Primary lateral control surface position;
(17) Primary yaw control surface position;
(18) Lateral acceleration;
(19) Pitch trim surface position or the parameters of paragraph
(20) Trailing edge flap or cockpit flap control selection
(21) Leading edge flap or cockpit flap control selection
(22) Each Thrust reverser position (or equivalent for propeller aircraft);
(23) Ground spoiler position or speed brake selection
(24) Outside or total air temperature;
(25) Automatic Flight Control System (AFCS) modes and usage status, including auto-throttle;
(26) Radio altitude (when an information source is installed);
(27) Localizer deviation, MLS Azimuth;
(28) Glide-slope deviation, MLS Elevation;
(29) Marker beacon passage;
(30) Master warning;
(31) Air/ground sensor (primary aircraft system reference nose or main gear);
(32) Angle of attack (when information source is installed);
(33) Hydraulic pressure low (each system);
(34) Ground speed (when an information source is installed);
(35) Ground proximity warning system;
(36) Landing gear position or landing gear cockpit control selection;

(37) Drift angle (when an information source is installed);
(38) Wind speed and direction (when an information source is installed);
(39) Latitude and longitude (when an information source is installed);
(40) Stick shaker/pusher (when an information source is installed);
(41) Wind shear (when an information source is installed);
(42) Throttle/power lever position;
(43) Additional engine parameters;
(44) Traffic alert and collision avoidance system;
(45) DME 1 and 2 distances;
(46) Nav 1 and 2 selected frequency;
(47) Selected barometric setting (when an information source is installed);
(48) Selected altitude (when an information source is installed);
(49) Selected speed (when an information source is installed);
(50) Selected mach (when an information source is installed);
(51) Selected vertical speed (when an information source is installed);
(52) Selected heading (when an information source is installed);
(53) Selected flight path (when an information source is installed);
(54) Selected decision height (when an information source is installed);
(55) EFIS display format;
(56) Multi-function/engine/alerts display format;
(57) Thrust command (when an information source is installed);
(58) Thrust target (when an information source is installed);
(59) Fuel quantity in CG trim tank (when an information source is installed);
(60) Primary Navigation System Reference;
(61) Icing (when an information source is installed);
(62) Engine warning each engine vibration (when an information source is installed);
(63) Engine warning each engine over temp (when an information source is installed);
(64) Engine warning each engine oil pressure low (when an information source is installed);
(65) Engine warning each engine over speed (when an information source is installed);
(66) Yaw trim surface position;
(67) Roll trim surface position;
(68) Brake pressure (selected system);
(69) Brake pedal application (left and right);
(70) Yaw or sideslip angle (when an information source is installed);
(71) Engine bleed value position (when an information source is installed);
(72) De-icing or anti-icing system selected (when an information source is installed);
(73) Computed center of gravity (when an information source is installed);
(74) AC electrical bus status;
(75) DC electrical bus status;
(76) APU bleed valve position (when an information source is installed);
(77) Hydraulic pressure (each system);
(78) Loss of cabin pressure;
(79) Computer failure;
(80) Heads-up display (when an information source is installed);
(81) Para-visual display (when an information source is installed);
(82) Cockpit trim control input position--pitch;
(83) Cockpit trim control input position--roll;
(84) Cockpit trim control input position--yaw;

16 Appendix 4: Configuration of Flight Mode Detection

This section contains the Flight Mode Transition Graph used for flight simulations and the equivalent declarative specification of the aircraft element flight mode detector expressed in XML [95].

16.1 Flight Mode Transition Graph

The graph is shown again here in Figure 16.1 for convenience of reference. The conventions used are as follows:

- Normal transitions between flight modes are shown in the thicker grey lines
- Dotted lines denote unusual sequences of transitions, such as a 'touch down landing followed immediately by a take off.
- Thinner (red) lines represent emergency and emergency recovery situations.

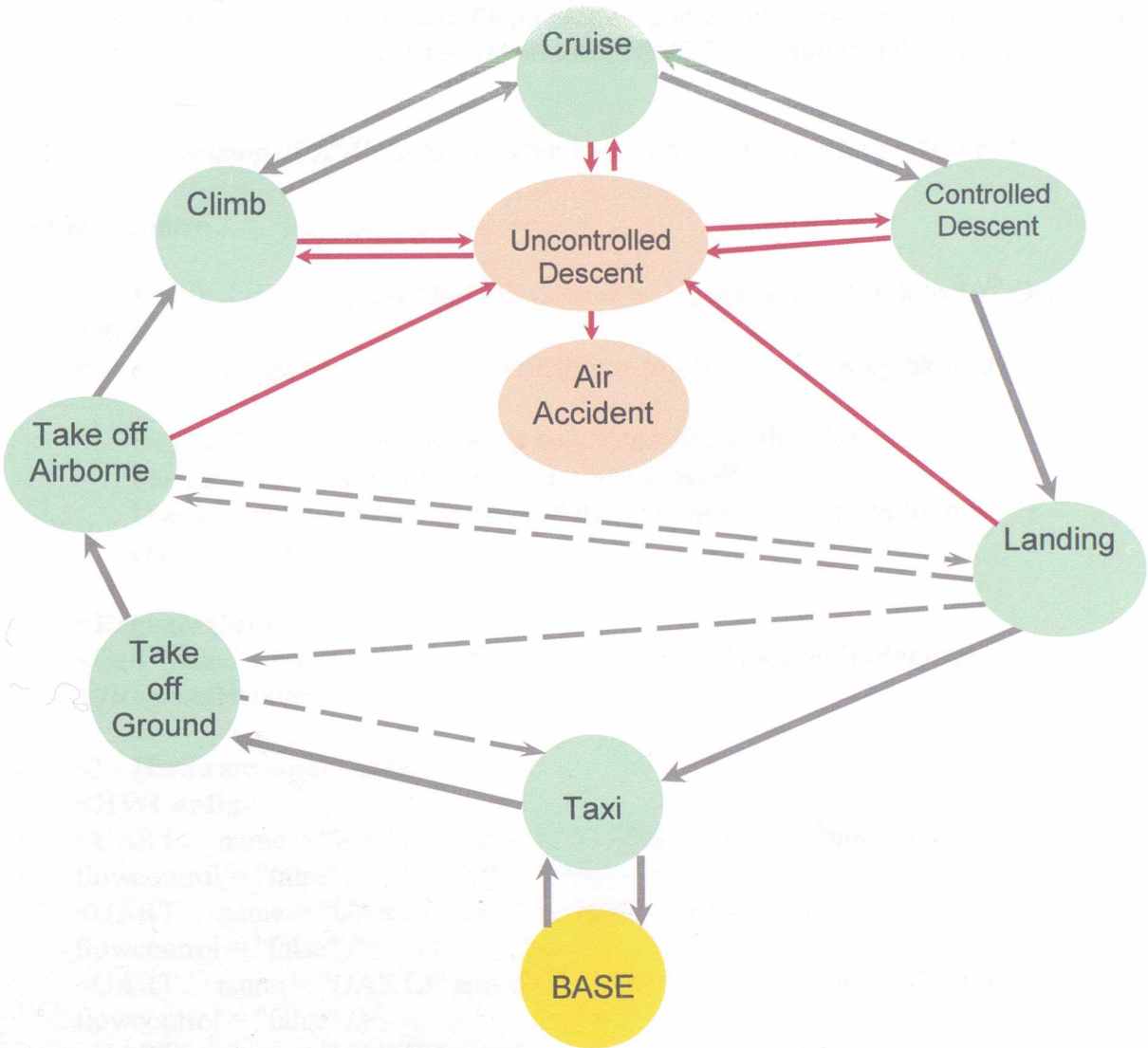


Figure 16.1: Flight Mode Transitions

16.2 Declarative Flight Mode and Safety Specification in XML

In order to support the development of the Flight Mode Detector software and ease of configuration of the system the ETH ONBASS team decided to use a dialect of the generic XML language [95]. This made it possible to create a very high level language which is application specific. The XML text takes the form of a declarative specification with separate sections of the text defining the Configuration, Flight Mode Detector, Operational Safety Checks

below includes a 'proof of concept' implement the 'corridors' suggested by Prof Igor Schagaev, with limits suggested by the Pilot. For example in the Climb flight mode the pilot suggested that the rate of climb limits could define a corridor with 'white/amber/red' indications on the display with corridors limits of 2500 for white, 2600 for amber and 2700 for red. During the verification activity further comments have been inserted into the XML to provide clarification of its structure and content.

Note that V&V experiments have shown that there is only a minimal overhead for using XML as a declarative specification i.e., an application specific high level language for defining the Equipment configuration, Flight Modes and Safety Checks. This is due to its compilation (to a binary tree structure) within the ONBASS unit during initialisation.

```
<!-- -->
<!-- This is the version of XML used --> <?xml version="1.0" encoding = "UTF-8" ?>

<Configuration>

    <!-- Verified on Microsoft Flight Simulator by bk and tk at ETH  8 to 10th Oct
    2007 -->
    <!-- Based on the input of Mark Griffith (the pilot) and review by bk,fof,tk -->

    <!-- RegisterHandlers section (must be located first in the file)
        The order of initializations must not be changed!
        Use this section to register all modules that must have access to this
        configuration file -->

    <RegisterHandlers log = "true">
    <Call   name = "Hardware Configuration" value = "HWConfig.Register" />
     </RegisterHandlers>

    <!-- Hardware configuration -->
    <HWConfig>
    <UART    name = "UART0" speed = "115200"    parity = "none" databits = "8"
    flowcontrol = "false" /> <!-- USB to Serial -->
    <UART    name = "UART1" speed = "9600"    parity = "none" databits = "8"
    flowcontrol = "false" />
    <UART    name = "UART2" speed = "115200"    parity = "none" databits = "8"
    flowcontrol = "false" />
    <UART    name = "UART3" speed = "4800"    parity = "none" databits = "8"
    flowcontrol = "false" />
    <UART    name = "UART4" speed = "115200"    parity = "none" databits = "8"
    flowcontrol = "false" />
```

```
<RAMDisk     base = "500000H" size = "512" blockSize = "4096" />
<!-- 2 Mbytes RAMDisk -->
<IRoCMMCDriver/>
<MMCDisk prefix = "MMC1" partition = "1" cache = "0" format = "true" />
<MMCDisk prefix = "MMC2" partition = "1" cache = "0" format = "true" />
</HWConfig>

<Autostart log = "true">
<!-- Ordering is immutable in this section, do not change!! -->

<!--                Text for the system log      Module.Procedure called -->
<Call   name = "Uart Polling Task"   value = "IRoCUartTask.Install" />

<!-- Remove these comment brackets whenever debug logging is required
<Call   name = "Test Support"   value = "TestSupport.Install" />
-->
<Call   name = "BlackBox" value = "BlackBox.Install" />
<Call   name = "Flight Mode Detector" value = "FlightModeDetector.Register" />
<Call   name = "Check Safety" value = "CheckSafety.Register" />
<Call   name = "TCP/IP"     value = "Net.Install"       />
<Call   name = "Echo server"     value = "EchoServer.Install"       />
 <Call   name = "UIS" value= "UIS.Install" />

<Call   name = "FrameCapture"   value = "FrameCapture.Install" />

<Call   name = "ADCParser"  value = "ADCParser.Register" />
<Call   name = "GPSParser"  value = "GPSParser.Register" />
<Call   name = "AEParser"   value = "AEParser.Register" />
<Call   name = "Check Safety" value = "CheckSafety.Register" />

<!-- Remove these comment brackets whenever logging of the web I/O is required
<Call   name = "WebLog" value = "WebLog.Install" />
-->
</Autostart>

<!-- Application & service configurations -->
<!-- Ordering is immutable in this section, do not change! -->

<BBReplication mmc1 = "MMC1" partition1 = "2"
                    mmc2 = "MMC2" partition2 = "2" /> <!-- FLASH -->
<BlackBox format = "true" />
<TestSupport device = "UART0"   timeout = "10" />
<Net device = "UART4"   localhost = "192.168.1.210"  />
<UIS port = "5061" />
<EchoServer port="1234" />
<GPSParser   device = "UART3"/>
<ADCParser  device = "UART1"/>

<FlightModeDetector>

<!-- This section defines the set of transitions between Flight Modes and the sets of
conditions that cause the transitions. It is a declarative specification that
characterizes the behaviour of the Flight Mode Detector software module-->
```

<!-- Initialization for 3 second flight record filter buffering, assuming 1 sample per second. Note that this reduces jitter between Flight Modes at the expense of a slight delay in response time-->
<speed is 3 seconds filtered GroundSpeed>
<height is 3 seconds filtered GPSHeight>
<RateOfClimb is 3 seconds slope of height>
<acceleration is 3 seconds slope of speed>

<!-- This transition must always true to force the first cycle for initialisation -->
<state from = "Invalid" to = "Base" condition = "height > -10000" />

<!--Base State-->
<state from = "Base" to = "Taxi" condition = "speed > 0
& speed < 10 knots" />

<!--Taxi State--> <!-- now covers both taxi out and taxi in -->
<!-- Note that this has been simplified so that the transition indicates that the aircraft has exceeded the stall speed (assumed to be 55 knots). The Rate of Climb assumes a horizontal runway-->
<state from = "Taxi" to="TakeOffGround" condition = "speed > 25 & speed < 55 knots & RateOfClimb = 0 feetperminute" />

<state from = "Taxi" to = "Base" condition = "speed = 0 knots" />

<!-- TakeOffGround State-->
<!-- Stall speed changed to 55 knots and rate of climb changed from 1 to 25 feetperminute, Pilot suggested that rate of climb may need filtering for short term smoothing (e.g. gusting wind) -->
<state from = "TakeOffGround" to = "TakeOffAirbourne"
condition = "IndicatedAirSpeed > 55 knots & RateOfClimb > 25 feetperminute" />

<!-- Removed rate of climb condition -->
<state from = "TakeOffGround" to = "Taxi" condition = "speed < 25 knots" />

<!-- TakeOffAirbourne State-->
<!-- Pilot recommended filtering Rateofclimb (smoothed),
stall speed changed to 55 KIAS for trials-->
<state from = "TakeOffAirbourne" to = "Climb" condition = "IndicatedAirSpeed > 55 knots & RateOfClimb > 0.1 feetperminute & height > 1000 feet" />

<!-- Pilot recommended this be adapted in future to match the glide slope of the landing (normally about 3 degrees off horizontal), the plane should be within a corridor of the slope -->
<state from = "TakeOffAirbourne" to = "Landing" condition = "RateOfClimb < -10 feetperminute & height < 1000 feet" />

<!-- Note: the best that can be done here for proof of concept is to detect a Stall in reality the major cause of accidents in the context is hitting and obstacle e.g. building near the runway due to lack of vertical acceleration, Pilots advice is that this cannot be predicted-->

< state from = "TakeOffAirbourne" to = "UncontrolledDescent" condition = "IndicatedAirSpeed < 55 knots" />

<!--Climb State-->
<!-- Note here the original +500 and -500 figures are just a delta to provide some tolerance. The pilot suggests corridor limits of
2500 for white (OK) , 2600 for amber (Warning) and 2700 for red (Danger) -->
<state from = "Climb" to = "Cruise" condition = "RateOfClimb < 500 feetperminute & RateOfClimb >-500 feetperminute" />

<state from = "Climb" to = "UncontrolledDescent"
condition = "IndicatedAirSpeed < 55 knots" />

<!--Cruise State-->
<!-- Note that both threshold values have been changed below, also the Pilot recommended filtering the RateOfClimb calculation to avoid jittering between Flight Modes -->

<state from = "Cruise" to = "ControlledDescent" condition = "RateOfClimb < -500 feetperminute" />

<state from = "Cruise" to = "Climb" condition = "RateOfClimb > 500 feetperminute" />

<state from = "Cruise" to = "UncontrolledDescent"
condition = "IndicatedAirSpeed < 55 knots" />

<!--ControlledDescent State-->
<!-- Pilot commented that a better condition would be 'greater than stall speed and less then the aircrafts "never exceed" speed limit, he also suggested that the corridor concept could be investigated here -->

<state from = "ControlledDescent" to = "Landing" condition = "RateOfClimb < -0.1 feetperminute & IndicatedAirSpeed < 55 knots" />

<state from = "ControlledDescent" to = "Cruise" condition = " RateOfClimb < 490 feetperminute & RateOfClimb >-490 feetperminute & height > 1000 feet" />

<state from = "ControlledDescent" to = "UncontrolledDescent"
condition = "IndicatedAirSpeed < 55 knots" />

<!--Landing State-->

<!-- Pilot recommended this be adapted in future to match the glide slope of the landing (normally about 3 degrees off horizontal), the plane should be within a corridor of the slope -->

<state from = "Landing" to = "Taxi"
condition = "IndicatedAirSpeed < 25 knots & RateOfClimb = 0" />

<state from = "Landing" to = "TakeOffGround" condition = "GroundSpeed > 25 knots & GroundSpeed < 52 knots & RateOfClimb > 0 feetperminute & acceleration > 0.1" />

<!-- Pilot suggested 200 rather than 1000 for height limit and smoothing of RateOf Climb -->
<state from = "Landing" to = "TakeOffAirbourne" condition = "IndicatedAirSpeed > 52 knots & RateOfClimb > 1 feetperminute & height > 200 feet " />

<!--UncontrolledDescent State-->
<!-- Pilot suggests recovery from stall enters the Controlled Descent state and then goes through other states from there -->
<state from = "UnControlledDescent" to = "ControlledDescent"
condition = "IndicatedAirSpeed > 55 knots" />

<!--state from = "UnControlledDescent" to = "AirAccident" condition = False! Not yet defined -->

<!--AirAccident State-->
<!-- Not yet defined -->

</FlightModeDetector>

<CheckSafety>
<-- This section contains a declarative specification of the safety checks (conditions) and responses (description of event, advice and significance) within each Flight Mode, it is used to characterise the continuous evaluation of the safety of the aircraft as an element, and to propose safety advice for the Pilot given the current operational context (Flight Mode)
Note that this is the direct equivalent of the dependency and recovery matrix of the aircraft as an element, but the paths have been pre-searched and the recovery actions combined for each Flight Mode-->

<state name="Any">
<-- Continually checked in all Flight Modes -->
<error
name="flying above the certified ceiling"
advice="structural integrity is being compromised"
level="red"
condition="DensityAltitude>14600 feet OR PressureAltitude > 14600 feet"/>
<error
name="approaching ground rapidly"
advice="reduce the rate of descent"
level="red"
condition="RateOfClimb < -2400 feetperminute & height < 2000 feet"/>
<error
name="the aircraft is undergoing dangerous manoeuvres"
advice="level out aircraft"
level="red"
condition="RateOfTurn > 10 & RateOfClimb < 0 & PressureAltitude < 400 feet"

```
        />
<error
        name="structural integrity is being compromised"
        advice="reduce the aircraft speed immediately"
        level="red"
        condition="TrueAirSpeed > 191 knots"
        />
<error
        name="air data computer or GPS error"
        advice="land aircraft and maintain the ADC (or GPS)"
        level="yellow"
        condition="RateOfClimb > 0 & (Groundspeed > 338 knots
        OR GroundSpeed < 0)"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="WindSpeed < -1 OR WindSpeed > 150 knots"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="RateOfClimb > 0 & (TrueAirSpeed > 188 knots
        OR TrueAirSpeed < 0 knots)"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="RateOfClimb > 0 & (MachSpeed > 300 OR MachSpeed
        < 0 )"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="RateOfTurn < -20 feet OR RateOfTurn > 20"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="RateOfClimb < -6000 feetperminute
        OR RateOfClimb > 6000 feetperminute"
        />
<error
        name="air data computer error"
        advice="land aircraft and maintain the adc"
        level="yellow"
        condition="IndicatedAirSpeed <0 OR IndicatedAirSpeed > 385
        knots"
```

```
                />
        <error
                name="air data computer error"
                advice="land aircraft and maintain the adc"
                level="yellow"
                condition="PressureAltitude <-1000 feet OR PressureAltitude >
                14600 feet"
                />
</state>
        <!-- Note that ideally there would be three checks for the next statement –
        corridor ranges
        0 to 10 knots WHITE indication
        10+ to 20 knots AMBER indication
        20+ knots RED -->
<state name="Taxi">
<!-- covers both TaxiIn and TaxiOut by bk/tk y071009 -->

                <error
                name="Taxi Speed High"
                advice="decrease taxiing speed now ?"
                level="yellow"
                condition = "IndicatedAirSpeed > 10 knots & IndicatedAirSpeed  <
20 knots"
                />
                <error
                name="Taxi speed dangerous!"
                advice="Nearing flight speed !"
                level="red"
                condition = "IndicatedAirSpeed >= 20 knots"
                />
</state>

<state name="Cruise">
        <error
                name="aircraft about to stall"
                advice="increase aircraft speed now"
                level="red"
                condition = "IndicatedAirSpeed  <55 knots"
                />
        <error
                name="cruise speed to high"
                advice="decrease cruise speed"
                level = "yellow"
                condition="IndicatedAirSpeed  > 109 knots"
                />
        <error
                name = "No acrobatic manoeuvres are approved by the
                manufacturer"
                advice = "Discontinue the manoeuvre immediately!"
                level="yellow"
                condition = "( RateOfTurn > 1 OR RateOfTurn < 1)
                & ( RateOfClimb > 1 feetperminute OR RateOfClimb < -1
                feetperminute )"
```

```
                />
        </state>
        <state name="TakeOffAirBourne">
                <error
                        name="Takeoff speed to high"
                        advice="decrease takeoff speed"
                        level = "yellow"
                        condition="IndicatedAirSpeed  > 109 knots"
                        />
                <error
                        name="aircraft about to stall"
                        advice="increase aircraft speed now"
                        level = "red"
                        condition="IndicatedAirSpeed < 55 knots"
                        />
        </state>
        <state name="Climb">
                <error
                        name="climb speed to high"
                        advice="decrease climb speed"
                        level = "yellow"
                        condition="IndicatedAirSpeed  > 109 knots"
                        />
                <error
                        name="aircraft about to stall"
                        advice="increase aircraft speed now"
                        level = "red"
                        condition="IndicatedAirSpeed < 55 knots"
                        />
        </state>
        <state name="ControlledDescent">
                <error
                        name="aircraft about to stall"
                        advice="increase aircraft speed now"
                        level = "red"
                        condition="IndicatedAirSpeed<55 knots"
                        />
                <error
                        name="descent speed too high"
                        advice="decrease descent speed"
                        level = "yellow"
                        condition="IndicatedAirSpeed  > 129 knots"
                        />
        </state>
        </CheckSafety>

</Configuration>
```

17 Appendix 5: UK MASS Patent Claims

The MASS concept has been patented in the UK Patent GB 0707057.6, 2007 'Method and Apparatus for Active Safety System'

1. The list below contains the Claims made in the draft Patent:
2. A method of providing active system safety for a system comprising a plurality of elements, the method comprising:
   detecting an element that is exhibiting anomalous behaviour;
   determining at least one element likely to be causally linked to the anomalous behaviour by using a set of dependency values associated with respective pairs of the elements, each dependency value representing a level of behavioural dependence between the elements of the pair; and
   performing a safety-related action in dependence on the determination.
3. A method as claimed in any preceding claim, comprising determining the element most likely to be causally linked to the anomalous behaviour.
4. A method as claimed in claim 2 or 3, wherein the determining step comprises, for each of a plurality of test elements, determining an overall dependency value, representing a level of behavioural dependence between the test element and the detected anomalous element, with reference to at least one path between the test element and the detected anomalous element, each path comprising a sequence of two or more elements including the detected anomalous element at one end and the test element at the other end.
5. A method as claimed in claim 4, wherein the overall dependency value for a test element is determined from the or each dependency value along the at least one path between the test element and the detected anomalous element.
6. A method as claimed in claim 5, wherein the overall dependency value is determined from an accumulation of the or each dependency value along the at least one path between the test element and the detected anomalous element.
7. A method as claimed in claim 4, 5 or 6, when dependent on claim 3, comprising determining the most likely element as the test element having the highest overall dependency value.
8. A method as claimed in any one of claims 4 to 7, wherein a test element is considered likely to be causally linked to the anomalous behaviour if it is determined to have an overall dependency value greater than a predetermined threshold.

9. A method as claimed in any one of claims 4 to 8, comprising propagating the or each path outwardly from the detected anomalous element.

10. A method as claimed in claim 9, when dependent on claim 6, comprising halting propagation of a path when the accumulation for that path becomes less than a predetermined value.

11. A method as claimed in any one of claims 4 to 10, wherein the set of test elements considered is determined as part of the method and represents a subset of the plurality of elements, the other elements being assumed to have a lower likelihood of being causally linked to the anomalous behaviour.

12. A method as claimed in any preceding claim, wherein each dependency value is expressed as a likelihood.

13. A method as claimed in claim 12, wherein the likelihood is expressed as a probability.

14. A method as claimed in any preceding claim, wherein the determining step comprises determining at least one element likely to be causing or at least contributing to the anomalous behaviour, such that the at least one element is causally linked to the anomalous behaviour by causing or at least contributing to the anomalous behaviour.

15. A method as claimed in claim 14, wherein the safety-related action is performed on at least one of the at least one element determined to be likely to be causing or at least contributing to the anomalous behaviour.

16. A method as claimed in any preceding claim, wherein an element is considered likely to be causally linked to the anomalous behaviour if there is determined to be a level of behavioural dependence between the element and the detected anomalous element greater than a predetermined level.

17. A method as claimed in any preceding claim, wherein the determining step comprises determining at least one element likely to be affected by the anomalous behaviour, such that the at least one element is causally linked to the anomalous behaviour by being affected by the anomalous behaviour.

18. A method as claimed in claim 17, wherein the at least one element likely to be affected by the anomalous behaviour is the at least one element likely to suffer harm or risk as a result of the anomalous behaviour.

19. A method as claimed in claim 17 or 18, wherein the safety-related action is performed so as to mitigate any consequences for at least one of the at least one element determined to be likely to be affected by the anomalous behaviour.

20. A method as claimed in any preceding claim, wherein the safety-related action defines the advice and/or feedback which is to be applied to improve the current and/or future operational reliability of the element and/or the system and thereby its safety.

21. A method as claimed in any preceding claim, wherein at least one of the dependency values comprises two different values, one representing a level of behavioural dependence of a first element on the second element, and the other representing a level of behavioural dependence of the second element on the first element, and comprising using the value appropriate to the determination being made.

22. A method as claimed in any preceding claim, comprising detecting anomalous behaviour of an element by reference to a behavioural model for the element.

23. A method as claimed in claim 22, comprising updating the behavioural models during use of the method, particularly to improve their capability for identifying anomalies in parts of the system that affect safety and/or to improve the current and future safety of the system.

24. A method as claimed in any preceding claim, comprising transmitting information produced by the method to a separate location where the informed can be securely monitored and/or stored and/or analysed.

25. A method as claimed in any preceding claim, comprising combining information produced by the method in the form of a display so as to highlight current and/or future safety issues and priorities, the information relating to at least one entity or element or group of elements such as an aircraft, train or automobile.

26. A method as claimed in any preceding claim, comprising monitoring at least one physical characteristic of each element for use in detecting the anomalous behaviour.

27. A method as claimed in any preceding claim, comprising adapting the monitoring of elements for anomalous behaviour based on a history of immediate past behaviour so as to improve the sensitivity of detection.

28. A method as claimed in any preceding claim, comprising adapting the monitoring of elements for anomalous behaviour over a prolonged period so as to enable detection of factors affecting safety that only become apparent over a prolonged period of time.

29. A method as claimed in any preceding claim, comprising detecting anomalous behaviour that might affect the safety of the element and/or the system.

30. A method as claimed in any preceding claim, comprising performing at least the determining step in relation to each of a plurality of sets of dependency values.

31. A method as claimed in claim 30, comprising performing the safety-related action in dependence on the determinations relating to the plurality of sets of dependency values.

32. A method as claimed in any preceding claim, comprising detecting a plurality of elements that are exhibiting anomalous behaviour, and performing the determining step in relation to each of the plurality of detected anomalous elements.

33. A method as claimed in claim 32, comprising determining at least one element likely to be causally linked to the anomalous behaviour of each of the detected anomalous elements.

34. A method as claimed in claim 32 or 33, comprising performing the safety-related action in dependence on the determinations relating to the plurality of detected anomalous elements

35. A method as claimed in any preceding claim, wherein a behavioural dependence between two elements exists when the behaviour of one element has an influence on the behaviour of the other element, the level of behavioural dependence being dependent on the extent of that influence.

36. A method as claimed in any preceding claim, implemented by mechanical, electro-mechanical, electrical, electronic means including Field Programmable Gate Arrays, Custom Designed Integrated Circuits ASICs or Microprocessors, employing analogue and or digital techniques.

37. A method as claimed in any preceding claim, comprising using fault tolerant techniques, for example making use of redundancy, so as to improve overall operational reliability of the system.

38. A method of providing active system safety substantially as hereinbefore described with reference to the accompanying drawings.

39. An apparatus for providing active system safety for a system comprising a plurality of elements, the apparatus comprising:

means for detecting an element that is exhibiting anomalous behaviour;

means for determining at least one element likely to be causally linked to the anomalous behaviour by using a set of dependency values associated with respective pairs of the elements, each dependency value representing a level of behavioural dependence between the elements of the pair; and

means for performing a safety-related action in dependence on the determination.

40. An apparatus for providing active system safety substantially as hereinbefore described with reference to the accompanying drawings.

<< Comment: the following Claims are allowed in Europe and USA, but not UK >>

41. A program for controlling an apparatus to perform a method as claimed in any one of claims 1 to 38.

42. A program which, when loaded into an apparatus, causes the apparatus to become an apparatus as claimed in claim 39 or 40.

43. A program as claimed in claim 41 or 42, carried on a carrier medium.

44. A program as claimed in claim 43, wherein the carrier medium is a storage medium.

45. A program as claimed in claim 43, wherein the carrier medium is a transmission medium.

46. An apparatus programmed by a program as claimed in any one of claims 41 to 45.

47. A storage medium containing a program as claimed in any one of claims 41 to 44.

18 Appendix 6: Technologies for Flight Recording

18.1 Flight Recording: History and Evolution

This section reviews the evolution of current flight data recording devices and the technological trends. The history of flight data recording started in Australia in 1948 [31] when Dr Dave Warren introduced his first flight data recorder Fig 18.1, he was the pioneer of flight data recording and the inventor of first flight data recorders, so called 'black' boxes.

Figure 18.1: Dr Dave Warren "Father of Accident Flight Recorders"

The original recorder used analogue recording onto 0.25" inch wide magnetic tape as the storage medium; newer ones of course use digital technology and memory chips. A typical such system permits a 25-hour continuous recording of the parameters monitored. The tape is in the form of an endless loop and is simply overwritten on a continuous basis. This means that unless the data is regularly off loaded to a repository the aircrafts lifecycle data is simply lost. There is normally no interaction of the recorder with other on-board devices.

The next significant development of flight data recording system was Concorde in the 1960s, see Figure 18.2. The most significant aspect of Concord's development, apart from supersonic passenger travel, was that the flight data were heavily used for safety management during flight in conjunction with a supportive flight simulator on ground, staffed with a team of the best existing experts in the field. Though this approach is not practical for regular CA and GA purposes the precedent was set for the concept of flight data analysis being performed in real time of flight.

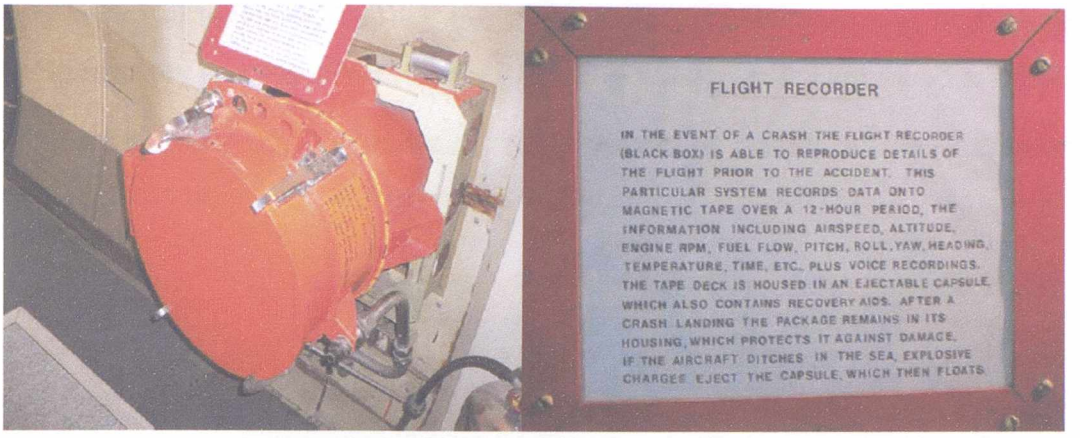


Figure 18.2: Concorde Flight Data Recorder (courtesy of Duxford Aviation Museum)

Digital avionic systems were introduced into Civil Aviation in the early '80s and now provide a greater volume of flight information on-board; at the same time the industry introduced the DFDR (Digital Flight Data Recorders) and QARs (Quick Access Recorders), these are illustrated in Figure 18.3 below:

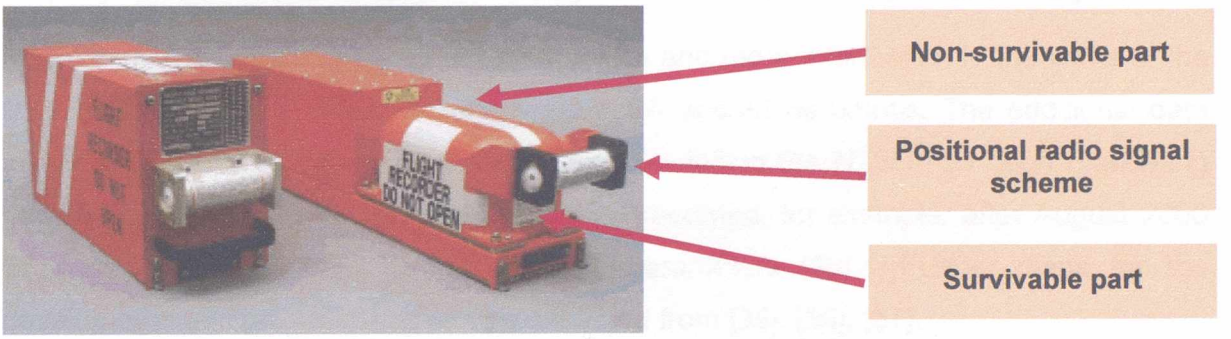


Figure 18.3: Typical digital flight data recorders

These devices have a processor and solid state memory, they also have an ability to compress and efficiently organise the storing of in-flight data. Improvements in data handling and compression technologies indicate that compression of data parameters by a factor of between 9 and 12 can be achieved without information loss. The ARINC 700 and EUROCAE standards [33] [71] provide a standard basis for the design of these systems. With an on board processing capability it now becomes possible to record and analyse data simultaneously.

In modern systems the analogue transducer signals are converted into digital format and recorded by the FDAU (Flight Data Acquisition Unit). A DFDAU (Digital Flight Data Acquisition Unit) can also accept digital inputs from sensors and other avionics equipment. Recent developments such as MP3 and MP4 audio and video compression have now made it possible to store many hours of cockpit voice and video data at

relatively low bit rates. The absence of moving parts in RAM and FLASH based solid-state memory recorders have made it possible to have much improved reliability.

According to Horne [34] accident recording should include all three different types of recorders as presented in Figure 18.4 below:

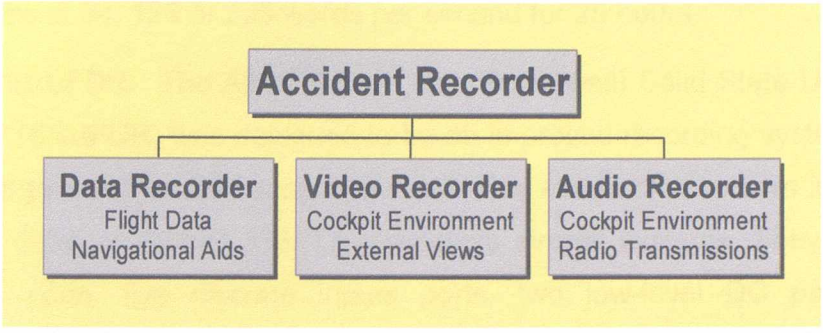


Figure 18.4: Horne's classification of Accident Recorders

Many flight safety systems now are able to print events on the cockpit printer immediately as they occur. However this does not make any sense in safety improvement terms as pilots today are overloaded with existing information, and therefore are unable to react properly on the new flow of data. What they need is safety *information* and *timely advice*.

There is a strong trend towards recording more and more information in the wake of the 9/11 terrorist attacks, which effectively used CA aircraft as bombs. The additional data includes cockpit and cabin video and audio. In addition the NTSB has been mandating that more aircraft sensor parameters must be recorded, for example: after August 2000 57 parameters and after August 2002 88-parameters [38] . Further plans for the development of flight recording can be extracted from [35], [36], [37].

18.2 Existing Flight Data Recording Devices

Some military and testing flight data recording systems are briefly described to give some general idea of their capabilities and the design approaches used. A functional block diagram that is typical for these flight data recorders is presented in Figure 18.6:

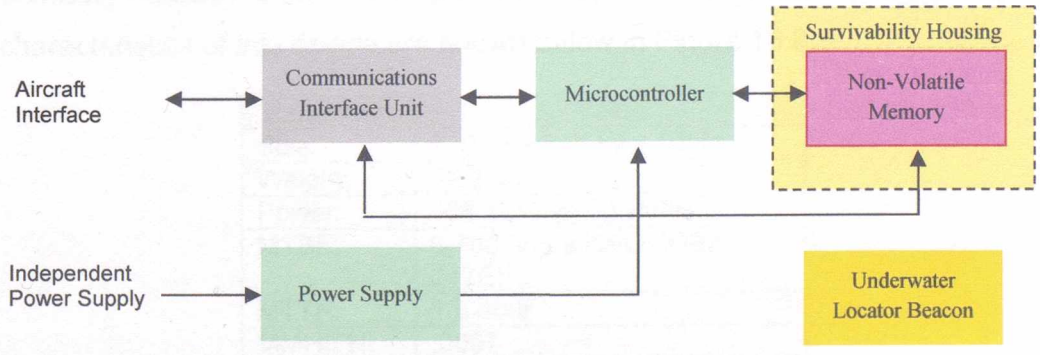


Figure 18.6: Functional Blocks of a Typical Military Data Recorder

Some typical commercial examples of recorders are:

Honeywell AR series. This series of Advanced Recorders (AR) target at recording needs aircraft in Business/General Aviation and Helicopters where space and weight are of major concern. The recorders are designed to minimize weight, reduce installation costs and minimise maintenance, even so the sales price is about $30,000 US. They meet or exceed TSO C-123a/C124a and EUROCAE ED-56/55A specifications. The recorder can record data rates of 64, 128 or 256 words per second for 25 hours.

Allied Signal SSUFDR. The Allied Signal (now Honeywell) Solid State Universal Flight Data Recorder (SSUFDR) was designed to be an improved recording system for general aviation and large commercial transport aircraft. This series of recorders is designed for use in ARINC 542A or ARINC 573//17 compatible aircraft systems. They have thirteen programmable ports, five discrete inputs ports, two low-level DC ports to record acceleration, and one temperature port. The system complies with TSO-C124 and respective environmental conditions according to RTCA-DO 160D.

L3 Military Aviation Recorder. A typical example of a modern military aviation data-recording device is presented in Figure 18.7; it is manufactured by L3 in the US and has the following specifications:

- Size: 3.0" H X 4.5" W x 6.5" L
- Weight: 6.5 lbs. (< 5 lbs. in Titanium)
- Power: +9 to +15 VDC @ 150mA, or 28VDC
- Operating Temperature Range: -40° C to +71° C
- Shock: 5100g/5-8 ms, six axis
- Penetration: 10-foot drop of 500-lb weight, six-axis, 0.05"
- Crush: 20,000 lbs. all orthogonal and major diagonal axes
- Fire: 1100°C for 60 minutes
- Seawater immersion: 20,000 ft, 30 days
- Fluids: Fuel, glycol, hydraulic, fire extinguishing, for 48 hours
- MTBF: 30,000 hours (MIL-HDBK-217E)
- Life: 17,000 hours operating, 30 years useful.

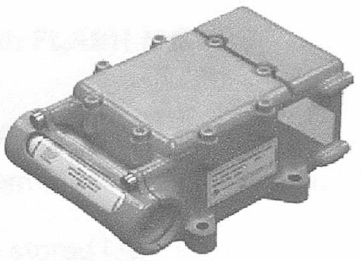


Figure 18.7: Typical Military Aviation Data Recorder and Specifications

The mean time between failures (MTBF) for micro controller parts and other hardware that are not included in crash-survivable housing of the device is much lower than for the data-recording module, for the L3 Flight Data Recorder the MTBF is 6,700 hours. Some other characteristics of this device are shown below in Figure 18.8:

Parameter	Value
Size:	7. 0" H x 6.2" W x 10" D
Weight:	16.2 lbs.
Power:	+28 VDC @ 60 watts
MTBF:	6,700 hours (MIL-HDBK-217E)
MTTR:	1.0 hour
MMH/FH:	.0007
Life:	15,000 hours operating, 20 years serviceability

Figure 18.8: L3 Flight Recorder Specifications

A more recent solution for flight data recording in military aircraft is produced by:

PLR Information Systems Ltd (www.plr.com). This device is designed to be mounted in the cockpit, where it stores data on standard PCMCIA Flash Memory cards capable of recording over 3 Giga Bytes. It is compatible with several standard data interfaces such as 1553 Mix Bus, ARINC-429, and RS-232/422/485, see Figure 18.9 below

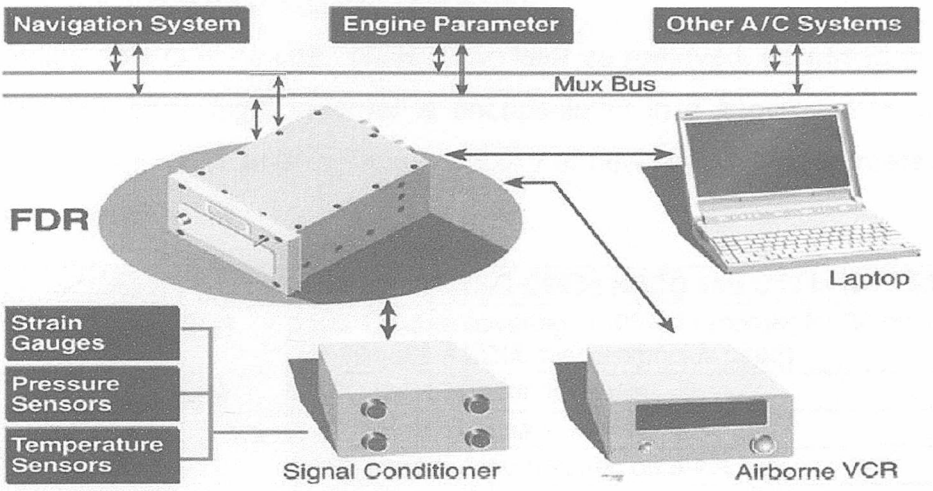


Figure 18.9: Military Flight Data Recorder with FLASH Memory

18.3 Requirements for New Flight Data Recording

As technology has become available there has been a stream of recommendations:

FAA updates the FAR Flight Data Parameters that must be stored [38].

The FAA Safety Board has recommended that two recorders should be located in two physically separated areas of aircraft, such as the nose and tail. Autonomous power supplies should be used for each device as past experience has shown that the last few minutes of flight were very often not recorded due to the loss of aircraft power.

The NTSB/AAR-90/04 meeting recommended the use of video recorders:
"The amount of information that could be provided by a cockpit video recorder is considerable ...the application of current long duration video technology in the cockpits of air transport aircraft could prove to be a valuable addition to aircraft accident investigation."

In 2004, the FAA requested recording of Controller Pilot Data Link Communication (CPDLC) messages.

In addition to voice and flight data recording, ICAO, EUROCAE and ARINC are considering video recorder standards and recommended practices.

The NTSB and FAA have proposed tightening cockpit voice recorder requirements by the end of 2006. Both bodies have requested video recorders in the cockpit, especially for small turboprops currently without them.

The market for these new devices for GA is estimated 9,600 aircraft (with 10 or more seats) with a cost for the aviation industry about $256 million.

18.4 Survivability Requirements

Recording data is of no use unless it can later be retrieved, accessed and processed. To achieve this each flight recorder is encapsulated in a shock, water, oil and fire proof packaging, the requirements for survivability of new flight data recorders are summarised in Figure 18.10 below:

Aspect	TSO C123a (CVR) and C124a (DFDR)
Fire (High Intensity)	1100°C flame covering, 100% of recorder for 30 minutes. (60 minutes if ED56 test protocol is used).
Fire (Low Intensity)	260°C Oven test for 10 hours
Impact Shock	3,400 Gs for 6.5 ms
Static Crush	5,000 pounds for 5 minutes on each axis
Fluid Immersion	Immersion in aircraft fluids (fuel, oil etc.) for 24 hours
Water Immersion	Immersion in sea water for 30 days
Penetration Resistance	500 lb. Dropped from 10 ft. with a ¼-inch-diameter contact point.
Hydrostatic Pressure	Pressure equivalent to depth of 20,000 ft.

Figure 18.10: Current flight recorder crash/fire survivability requirements

18.5 Flight Data Processing Systems

Recorded flight data is useless unless there is a complementary data processing system which can be used to reveal the likely causes of accidents and thereby be used to improve aviation safety. One of the most advanced and widely used software packages for post-flight data processing is called BASIS, originally developed by British Airways. The whole system consists of flight data processing modules and reporting modules. Flight data processing modules are targeted to work with raw flight data and where necessary normalise and filter information to be distributed to the various kinds of users (such as maintenance engineers, pilots, aviation experts and others).

There are several kinds of modules, for example the Flight data group includes the:

1. Flight Data Exceedences module (FDE).
2. Flight Data Simulation module (FDS).
3. Flight Data Traces (FDT) module.
4. Flight Data Measurements (FDM) module.

The Incident reporting modules include the:

1. ASR (Air Safety Reporting)
2. CSR (Cabin Safety Reporting)
3. GOR (Ground-found Occurrence Reporting)
4. GHR (Ground Handling Reporting)
5. HFR (Human Factor Reporting).

Other modules are the MEI (Maintenance Error Investigation), and SIE (Safety Information Exchange), a summary of their function is shown in Figure 18.11.

Flight Data Module	Function
FDE	FDE measures and monitors flight data from aircraft, analyses events by aircraft type, event type, airfield, date, keyword etc. FDE presents the results in graphical formats selected as most appropriate for that particular analysis.
FDS	FDS recreates the flight as the pilot saw it and represents the actual flight instrument display for each aircraft type. FDS can reproduce flight data in various speeds.
FDT	FDT reads in the raw flight data from an aircraft's onboard flight data recorders; automatically detects exceeding, e.g. deep landing, high roll rate on landing etc.; stores traces; displays selected flight data and detected exceeding/events as a trace on screen.
FDM	FDM analyses the maximum value of many flight parameters on each and every flight e.g. maximum 'g' force on landing, maximum rate of descent, maximum pitch on landing etc.
Reporting Modules	**Function**
ASR	This module is used to process flight crew generated reports of any safety-related incident.
AUD	Stores and analyses details of JAR Ops (Flight Operations, Engineering, Ground Operations) and Health and Safety audits.
CSR	Analyses safety incidents in the cabin.
GOR	Collects and analyses maintenance incident reports.
GHR	Collects and analyses ground handling incident reports.
HFR	It displays the causal factors behind an incident.
MEI	Investigation of maintenance errors. It detects what were the contributory factors.
SIE	This contains Air Safety Reports from over 40 contributing airlines. The merged SIE database is sent out every quarter and contains incidents occurring during the preceding 12 months.

Table 18.11: BASIS Modules & Functions

The classifications of CA and GA often overlap and so given that CA has by far the best safety record in aviation, it is only logical to assume that the GA flight data recording and processing and safety management will follow the direction of CA in the future.

19 Appendix 7: Flight Mode Test Scenarios

This appendix contains some examples of test scenarios used to exercise the operation of the Flight Mode Detector using the XML specification in Appendix 2 running on the development and simulation system illustrated in Figure 19.4. The flight scenarios are intended for use in creating Flight Plans with the Test Pilot, they were specified by the author, Angus Kintis of Spirit SA and Mark Griffiths (pilot).

Each flight always starts with Scenario 1 and ends with Scenario 2 these are defined separately to avoid repetition of details in other scenarios. The other scenarios are intended to be self contained and can be combined together within flight plans.

19.1 Scenario #1 Pre-flight ONBASS Equipment Preparation

Objective: Verify ONBASS unit is functioning and capable of recording the flight data
Steps:

1. Ensure ONBASS operator has a paper note pad and pen for taking notes during the flight, any notes should contain at least the Flight Plan reference, date, time and name of operator.
2. Check all cables plugged in securely (Power, ADC, GPS (if fitted), Terminal Cable, HMI Cable)
3. Check Power is on
4. Check that two MMC memory cards are fitted and have sufficient capacity for the flight data expected for the next flight
5. Check data is being received from ADC and GPS using Minos.Terminal on the laptop connected to the ONBASS unit
6. Enable flight data recording and logging on the ONBASS unit

Results to be saved: Record the flight details in the Flight Test logbook
Post Flight Analysis required: None

19.2 Scenario #2 Post-flight ONBASS Equipment Preparation

Objective: Verify and store flight data from ONBASS unit
Steps:

1. Stop operation of the ONBASS unit via Minos.Terminal
2. Remove the two MMC memory cards and back up their data to the laptop (a memory card adapter may be needed on the laptop to read the cards) Store the data image with a filename indicating the Flight Plan, date, time
3. Copy any handwritten notes made by ONBASS operator during the Flight, scan and store then in a folder with the Flight Data

Results to be saved: Record the flight details in the Flight Test logbook
Post Flight Analysis required: Record total amount of flight data collected and where it is stored, both in Flight Test logbook

19.3 Scenario #3 Initial ONBASS Functionality Check

Objective: Verify ONBASS unit is initially functioning in flight
Steps:

1. Make a flight from the Base consisting of a single circuit of the airfield and land, going back to base. Ensure that a height of at least 1200 feet is attained during the flight.
2. Remove the two MMC memory cards and back up their data to the laptop (a memory card adapter may be needed on the laptop to read the cards) Store the data image with a filename indicating the Flight Plan, date, time

3. Copy any handwritten notes made by ONBASS operator during the Flight, scan and store then in a folder with the Flight Data

Results to be saved: Record the flight details in the Flight Test logbook
Post Flight Analysis required: Record total amount of flight data collected and where it is stored, both in Flight Test logbook

19.4 Scenario #4 Check Basic Flight Mode Detection

Objective: Verify that flight modes on a simple basic flight are detected as expected
Steps:

1. Start with aircraft at Base
2. Do pre-flight checks on aircraft
3. Taxi out to take off point
4. Take off and climb continually and slowly to 2000 feet with KIAS of at least 70 knots
5. Gradually level out and stay as level as possible for several minutes at about 80 knots
6. Complete a circuit and prepare to land
7. Start descending with a rate of descent of 600 feet per second
8. Land the aircraft
9. Taxi back to base
10. Shut down the aircraft

Results to be saved: Record the flight details in the Flight Test logbook, record the approximate times that each step was started
Post Flight Analysis required:

1. Record total amount of flight data collected and where it is stored, both in Flight Test logbook
2. Check the Flight Mode sequence detected was
   Base, Taxi, TakeOffAirborne, Climb, Cruise, ControlledDescent, Landing, Taxi, Base

19.5 Scenario #5 Transitions: Climb, Cruise, Controlled Decent

Objective: Verify that it is possible to detect transitions between flight modes Climb, Cruise and Controlled Descent
Steps:

1. Assume steps 1 to 4 of Scenario 4 have been done
2. Continue flying between 70 and 90 knots throughout the following steps
3. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
4. Establish rate of fall of 600 feet per minute for 30 seconds (Controlled Descent)
5. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
6. Establish rate of climb of 600 feet per minute for 30 seconds (Climb)
7. Establish rate of fall of 600 feet per minute for 30 seconds
   (transient Cruise, Controlled Descent)
8. Level out and stay as level as possible for one minute at about 80 knots (Cruise)

Results to be saved: Record the flight details in the Flight Test logbook, record the approximate times that each step was started
Post Flight Analysis required:

1. Record total amount of flight data collected and where it is stored, both in Flight Test logbook
2. Check the Flight Mode sequence detected was
   Cruise, ControlledDescent, Cruise, Climb, (transient)Cruise, ControlledDescent, Cruise

19.6 Scenario #6 Check Safe Transitions to Uncontrolled Descent

Objective: Verify that it is possible to detect transitions between flight modes leading to Uncontrolled Descent. Note that the Pilot has discretion as to which tests to perform as stalling the aircraft may be unsafe e.g. TakeoffAirborne and Landing. The height assumed for this set of maneuvers is 3000 feet, subject to Pilot opinion.

Steps:

1. Assume steps 1 to 4 of Scenario 4 have been done
2. Climb to test altitude, 3000 feet at 600 feet per minute (Climb)
3. Stall the plane by increasing the rate of climb (and reduce throttle if necessary) (UncontrolledDescent)
4. Allow loss of height to 2000 feet (if safe)
5. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
6. Climb to test altitude, 3000 feet at 600 feet per minute (Climb)
7. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
8. Stall the plane by increasing the rate of climb (and reduce throttle if necessary) (UncontrolledDescent)
9. Allow loss of height to 2000 feet (if safe)
10. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
11. Climb to test altitude, 3000 feet at 600 feet per minute (Climb)
12. Level out and stay as level as possible for one minute at about 80 knots (Cruise)
13. Establish rate of fall of 600 feet per minute for 30 seconds (Controlled Descent)
14. Stall the plane whilst still descending at more than 500 feet per minute (UncontrolledDescent)
15. Allow loss of height to 2000 feet (if safe)
16. Level out and stay as level as possible for one minute at about 80 knots (Cruise)

Results to be saved: Record the flight details in the Flight Test logbook, record the approximate times that each step was started

Post Flight Analysis required:

1. Record total amount of flight data collected and where it is stored, both in Flight Test logbook
2. Check the Flight Mode sequence detected was
   Cruise, Climb, UncontrolledDescent, Cruise
   Cruise, Climb, Cruise, UncontrolledDescent,
   Cruise, Climb, Cruise, ControlledDescent, Uncontrolled Descent, Cruise

The end of the Thesis.