CIVIL AVIATION AUTHORITY

CAA PAPER 95012

FEASIBILITY STUDY INTO AN INTELLIGENT FLIGHT PATH MONITOR: FINAL REPORT

CIVIL AVIATION AUTHORITY LONDON PRICE £14.00

CAA PAPER 95012

FEASIBILITY STUDY INTO AN INTELLIGENT FLIGHT PATH MONITOR: FINAL REPORT

Dr Martin Robson
Dr Michael Fairbanks
Dr Michael Shorthose
Smith System Engineering Ltd

PREPARED BY SMITH SYSTEM ENGINEERING LTD AND PUBLISHED BY
CIVIL AVIATION AUTHORITY LONDON DECEMBER 1995

ISBN 0 86039 641 X

Printed and distributed by Civil Aviation Authority, Greville House, 37 Gratton Road, Cheltenham, England

Executive summary

Controlled Flight Into Terrain (CFIT) accidents sadly still occur with tragic frequency, even involving advanced-technology modern aircraft. The primary cause is lack of crew situational awareness: that is, the crew's mental picture of the aircraft's situation becomes incorrect or incomplete.

Statistics indicate that modern glass-cockpit aircraft are not necessarily safer than older generation aircraft. This appears to be due to a new phenomena, in which crews sometimes lose awareness of what the aircraft's automated systems are doing.

There is therefore a requirement for improving cockpit systems in such a way as to improve crew situational awareness, both in terms of the external aircraft surroundings and in terms of the aircraft systems themselves.

The chances of classic CFIT accidents, in which a perfectly serviceable aircraft is flown into terrain, can be greatly reduced by providing aircraft with improved versions of Ground Proximity Warning Systems (GPWS), such as Enhanced GPWS or Ground Collision Avoidance Systems (GCAS). These systems use digital terrain maps to provide the warning device with a forward-looking and more intelligent capability. This allows the system to:

- Warn of rising terrain ahead of the aircraft, well before radio altimeter generated warnings.
- Warn crews performing non-precision approaches, if an attempt to land where there is no runway is made (the GPWS 'no-warning' situation).
- Increase crew situational awareness by providing vertical navigation information.
- Greatly reduce the false alarm rate which plagued earlier systems and reduces crew confidence in the system, by warning envelope modulation.

The more recent phenomena, in which crews lack awareness of what the aircraft's automated systems are doing, could be tackled in several ways, including:

- Improve the interface on existing systems to increase 'mode awareness', and prevent automated systems from getting any more complex than they are at present. This should obviously be done for existing systems with known problems with the interface design. However, there is still a risk that crews are presented with too high a workload in abnormal situations: the automated systems are not helping the crew when help is needed most. Also, the crews might become used to the automated systems and therefore be less able to cope in abnormal situations.
- Reduce the level of automation. This might solve the new problems encountered, but give rise to older problems that drove towards more automation in the first place.
- Increase the 'intelligence' of the aircraft systems so as to provide crews with a smooth workload under all situations (to prevent underload or overload) and prioritise crew tasking. This is an attractive alternative if it is feasible, since it realises the goal of automation. This amounts to a change in interface design philosophy, to a more 'human-centred' approach.

The last alternative fits the concept of Intelligent Flight Path Monitoring (IFPM), however it constitutes more than just a 'black box' addition. The two-man cockpit would be provided with an artificially intelligent third pilot, that performs an autonomous situation assessment for the aircraft, drawing crew attention to the most relevant information. Such a device would (potentially) be immune to the known human failure modes (information saturation, vigilance, etc).

A group of researchers at the University for the German Armed Forces in Munich, in association with Dornier, have been working on the development of just such a system. This has produced a technology demonstrator version of a Cockpit Assistant System (CASSY). CASSY has been trialled in flight simulators and flown in an experimental aircraft. Its feasibility has been demonstrated, subject to the availability of new technology such as reliable voice recognition technology and Air Traffic Control (ATC) datalink.

This report investigates a functional design of (and requirements for) an IFPM, and two particular architectures: one for an IFPM suitable for retro-fit to existing aircraft and one for future aircraft using advanced technologies. Much can be achieved with a design that uses existing technologies. However, a fully-functional version of the design requires new technology such as ATC datalink and voice recognition capability.

Sophisticated warning functions can be provided without placing any higher specifications on other aircraft systems. Development costs would not be prohibitive, at around £50M. The main risk involved in production of an IFPM would be in the safety certification of the Artificial Intelligence (AI) system components that might be required. No AI system has been certified for a safety-critical application as yet.

Contents

List of figures

List of tables

List of acronyms

4-D	4-Dimensional
AI	Artificial Intelligence
ARCHIE	A Reliable Computer-Human Interface Environment
ARINC	Aeronautical Radio, Incorporated
ASPIO	Assistant for single pilot IFR operation
ATC	Air Traffic Control
ATN	Aeronautical Telecommunications Network
CASSY	Cockpit Assistant System
CFIT	Controlled Flight Into Terrain
CRI	Computer Resources International
DARPA	Defense Advanced Research Projects Agency
DASA	Daimler Benz Aerospace
DLR	Deutsche Forschungsanstalt fur Luft- und Raumfahrt
DME	Distance Measuring Equipment
DPAC	Direction des Programmes de l'Aeronautique Civile
DTED	Digital Terrain Elevation Database
EC	European Commission
ECAM	Electronic Centralised Aircraft Monitor
EEPROM	Electrically Erasable/Programmable Read Only Memory
EFIS	Electronic Flight Instrument System
EGPWS	Enhanced Ground Proximity Warning System
EICAS	Engine Indication and Crew Alerting System
ELS	Electronic Library System
ESAS	Enhanced Situational Awareness Systems
EVS	Enhanced Vision System
FAA	Federal Aviation Administration
FINDER	Flight-plan interactive negotiation/decision aiding system for en-route re-routing
FMS	Flight Management System
GCAS	Ground Collision Avoidance System
GLONASS	Global Navigation Satellite System
GMAv	GEC Marconi Avionics
GNE	Gross Navigational Error
GOCAT	Ground Obstacle Collision Avoidance Technique

GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HUD	Head Up Display
HSI	Horizontal Situation Indicator
ICAO	International Civil Aviation Organisation
IFPM	Intelligent Flight Path Monitor
IFR	Instrument Flight Rules
ILS	Instrument Landing System
INS	Inertial Navigation System
KBS	Knowledge Based System
KF	Kalman Filter
MSA	Minimum Safe Altitude
NASA	National Aeronautics and Space Administration
NN	Neural Network
QA	Quality Assurance
SA	Situational Awareness
SSR	Secondary Surveillance Radar
TCAS	Traffic Alert and Collision Avoidance System
TCM	Terrain Characteristics Matching
TMA	Terminal Manoeuvring Area
TRN	Terrain Referenced Navigation
VASI	Visual Approach Slope Indicator
VOR	Very High Frequency Omni-Directional Radio Range

1 INTRODUCTION

1.1 General

This document concerns a feasibility study of an intelligent flight path monitor (IFPM). It constitutes the final report of the study carried out by Smith System Engineering Ltd for and on behalf of the Civil Aviation Authority's Safety Regulation Group [1].

1.2 Context

The rate of controlled flight into terrain (CFIT) accidents has been reduced by the implementation of ground proximity warning systems (GPWS), which were developed in the 1970s. However, CFIT is still responsible for approximately half of the fatalities arising from aviation accidents. It is, therefore, desirable to reduce further the rate of CFIT accidents.

CFIT is usually associated with a loss of situational awareness, perhaps coupled with spatial disorientation of the crew. Problems can be compounded when there are also substantial communications difficulties in an emergency situation, for example between air crew and air traffic control (ATC). These factors were both found to be important by the investigations into Air Inter accident at Strasbourg and Pakistan International Airways and Thai Airways International crashes in Kathmandu in 1992.

Loss of situational awareness by the air crew can have consequences other than CFIT: for example, in oceanic airspace a loss of situational awareness, coupled with flight management system (FMS) data entry errors, can lead to gross navigational errors (GNEs).

Situation information also reports the status of the aircraft systems to the pilot, for example through the electronic flight instrument systems (EFIS). However, there may be no indication as to whether the status is desirable and such data can be misrepresented or misinterpreted.

It may be feasible to synthesise information available from aircraft systems to provide an alert to the pilot of deviations from the expected flight profile or from the expected aircraft status and hence overcome some of the problems described above. Such a system might be termed an intelligent flight path monitor (IFPM). However, there is no documented operational requirement for such a system and many performance and functional issues need clarification.

This report investigates the operational requirements and feasibility of providing transport aircraft with an Intelligent Flight Path Monitor (IFPM). It looks at the shortcomings of current aircraft systems and how these are being addressed by other research groups. It considers the human factors involved with aircraft accidents and how the IFPM concept might be used in prevention. It looks at the requirements that should be placed on an IFPM, and concludes with some baseline designs, including functional design, architectures, development costs and risks.

1.3 Definitions

In this document, the term 'nuisance' refers to alarms which are generated by a system functioning within its technical specification, but whilst the pilot is flying an accepted safe procedure. The term 'false' refers to alarms generated by a failure or fault in the system which causes equipment to provide a warning that is not in accordance with its technical specification.

This is in accordance with CAP 516 ('Ground Proximity Warning System (GPWS): Guidance Material').

1.4 Contents

This document is organised as follows:

- Section 2 outlines the shortcomings that have been identified in current cockpit systems that might be improved upon using some sort of artificially intelligent (AI) cockpit system;
- Section 3 summarises the previous work particularly relevant to using AI for use in cockpits;
- Section 4 discusses the human factors involved and loosely specifies an interface for an IFPM;
- Section 5 describes the requirements that might be placed on an IFPM;
- Section 6 outlines a baseline IFPM design and discusses algorithms and software technology that each might require;
- Section 7 presents two different architectures of this baseline design: one for an IFPM suitable for retro-fit to existing aircraft using current technology, and one for an IFPM suitable for future (yet-to-be-designed) aircraft using future technology;
- Section 8 analyses the costs, risks and timings for the development of an operational IFPM;
- Section 9 summarises the report's conclusions;
- Section 10 lists the report's recommendations;
- Section 11 lists the references cited in the text;
- Appendix A tabulates some relevant accidents cited in the main text;
- Appendix B discusses the operational requirements for an IFPM as determined from discussions with Air 2000;
- Appendix C reports on the views of Virgin Atlantic's flight department on the IFPM concept.

2 SHORTCOMINGS OF CURRENT SYSTEMS

2.1 Introduction

This section outlines the shortcomings that have been identified in current systems flown aboard large commercial transport aircraft. For clarity, the shortcomings have been categorised into a number of factors as follows:

- those which contribute significantly to CFIT accidents, which are described in section 2.2;
- those which may induce gross navigational errors, which are described in section 2.3;
- those which can lead to fuel management problems, described in section 2.4;
- those which contribute to tactical flight planning problems, e.g. re-routing en-route, which are described in section 2.5;
- those which introduce autopilot misunderstandings or overconfidence in the flight management system (FMS), which are described in section 2.6;
- those caused by inappropriate use of automation in the cockpit, described in section 2.7;
- those which lead to inappropriate aircraft configuration, which are discussed in section 2.8.

Examples of accidents/incidents used to illustrate the discussion are contained in Appendix A and referred to in the text.

2.2 CFIT accidents

Research [2] has shown that many factors contribute to the cause of CFIT accidents. These factors, which often occur in combination are:

(1) Altimeter setting or reading errors.

(2) Non-standard weather conditions.

(3) Minimal terrain clearances (distance) used on some aircraft approaches.

(4) Pilot/ATC misunderstandings.

(5) Navigation errors.

(6) Lack of vertical situational awareness.

(7) Over confidence in Flight Management Systems.

Table 2–1 summarises the contribution that an IFPM could make to each of these factors to reduce ultimately the occurrence of CFIT accidents.

Table 2–1 Possible IFPM contributions to preventing CFIT

Cause:	Description:	IFPM contribution:
1	Altimeter setting errors	IFPM could compare and check barometric altimeter readings against GPS altitude and radio altitude (all converted to same frame of reference)
2	Unforecast/adverse weather conditions	Improvements could be obtained if the aircraft were obtaining meteorological information via datalink
3	Minimal terrain clearances on some approaches	IFPM could use aircraft navigation systems and trajectory prediction in conjunction with a terrain database to warn against unacceptable clearances
4	Pilot/ATC misunderstanding	IFPM could act as aircraft's 'negotiation manager' for negotiating the aircraft's 4-D flight plan with future ATC systems via datalink
5	Navigation error	Use an integrated navigation system (including terrain database and TRN) to provide IFPM with reliable aircraft position data
6	Lack of vertical situational awareness	IFPM could have major contribution in monitoring vertical profile, warning pilots and providing a vertical profile or plan display
7	Over confidence in FMS	IFPM could sanity check that current autopilot setting is appropriate for aircraft status

2.3 Gross Navigational Errors

Gross Navigational Errors (GNEs) occur when incorrect data is entered into the FMS, for example if a heading of 270° instead of 27° is entered (accident 'f' in Appendix A). A considerable number of such errors have occurred in the past, particularly for aircraft flying through Oceanic airspace. As air traffic control in these regions is procedural and based on aircraft position reports, considerable time can elapse before the GNE is detected.

These types of errors have detrimental effects:

- delay and inconvenience;
- increased collision risk:
  - in Oceanic airspace, with TCAS equipped aircraft, increased collision risk must be slight;
  - in a TMA, collision risks may be significantly increased either with other aircraft or with terrain (see 2.2).

Clearly an IFPM could play a significant role in preventing GNEs. The database the system uses could also contain global details of the airspace structure, and sanity-check entered flight plans. It could also, in principle, check the tactical flight plan against the filed flight plan and airline approved routes.

2.4 Fuel Management

In the context of the IFPM, fuel management has two potential areas of interest:

- increasing the safety of flight by using the IFPM as a sophisticated fuel manager;
- increasing the fuel efficiency of flights.

There have been a limited number of accidents involving fuel starvation due to crew fuel mismanagement, including incidents after ATC tactical intervention, for example accident 'h' in Appendix A. The IFPM could clearly provide input to prevent this type of accident, since it potentially has available to it enough information (without additional crew input) to assess and monitor the fuel situation, e.g. using the:

- current flight plan;
- current fuel status;
- current gross weight;
- meteorological conditions ahead (either from the flight plan or, preferably, up-to-date information available via datalink);
- aircraft engine performance.

2.5 Flight planning

Related to the fuel management issue is flight planning, particularly if aircraft are tactically re-routed by ATC once airborne. As with fuel management, there are both safety and efficiency issues to be considered.

On the safety side, CFIT accidents have been caused by erroneous crew actions when flight plans have been changed, particularly if those changes have occurred during the final phase of a flight, when work load on crews might be quite high (this has been a contributory factor in many CFIT accidents, including accidents 'n' and 'o' in Appendix A). These types of errors have caused both accidents in which aircraft fly into precipitous terrain and accidents in which aircraft have tried to land where no runway exists. If an IFPM is monitoring or advising on the entered flight plan, the chain of events that causes these accidents might be broken at an early stage.

In terms of efficiency, there is much to be gained in providing a system that is capable of calculating optimal re-routing if tactical ATC changes to the flight plan are required. There is a debate whether optimal routing should be determined by the airborne systems or by the ground based systems. In either case, the IFPM could comprise an important element of the airborne part of a 4-D flight plan negotiation system. Negotiations could be undertaken between future ATC systems and the aircraft utilising a datalink, such as VHF, Mode S radar or satellite. This is clearly a major goal of Sextant Avionique's FINDER system (see section 3).

2.6 Autopilot/pilot misunderstandings, EFIS/FMS overconfidence

Accident/incident statistics show that the introduction of new technology to commercial transport aircraft has improved flight safety (e.g. the introduction of electronic flight instrument systems, EFIS). However, it has also given rise to a new phenomenon: pilot overconfidence in these systems [3]. There have been at least 14 occasions in the past ten years in which pilots have misunderstood or misinterpreted what the EFIS is displaying or what mode the autopilot is in, resulting in serious accidents (for example accidents 'c', 'd', 'i', 'k', 'l', 'm' and 'p' in Appendix A).

The problem seems to arise from the multitude of different modes that the autopilot could be in, which are not always transparent to pilots, and autopilots automatically changing between one mode and another.

These problems could be resolved by the avionics manufacturers being forced to change EFIS/autopilot operation and display (this is occurring to a certain extent). Alternatively, an IFPM could be used to monitor the current autopilot settings and compare this against aircraft status.

2.7 Other aircraft automation incidents

There have been other accidents that have been caused by advanced aircraft automation that was intended to increase safety (for example accidents 'b' and 'e' in Appendix A). Whilst these accidents/incidents are few in number, they constitute an important class of potentially preventable mishaps.

In some cases, accidents have been caused by the failure or inoperation of configuration warning devices. In other cases (e.g. accident 'g' in Appendix A) the automation operated in accordance with its design but in a mode incompatible with safe flight under those circumstances.

Some of the problems seem to be caused by the warning devices having become primary alerting devices, even though they were originally intended as a 'second line of defence'.

The human factor aspects of using advanced automation in cockpits is discussed in section 4.

2.8 Aircraft configuration

There have been many accidents in the past involving aircraft landing or taking off in incorrect aircraft configuration (e.g. accidents 'a' or 'j' in Appendix A). It is already mandatory for aircraft systems to provide certain configuration warnings, and systems such as GPWS take as inputs landing gear and flaps configuration.

However, more sophisticated configuration warnings (such as flap settings during take-off) could be implemented on an IFPM.

2.9 Summary

The limitations and shortcomings of current cockpit systems have been investigated in this section. The main conclusions are:

- A trend identified is that modern, advanced-technology aircraft are not necessarily much safer than older generation aircraft, mainly due to poor man-machine interface design. At present, the different aircraft systems operate more or less independently from each other. There is no 'integrating' device taking an overview of the aircraft's situation.

- CFIT accidents are caused by a number of circumstances. The likelihood is that nearly all these types of accident might be reduced by either retrofitting new technology (e.g. terrain database) or including new technologies in future aircraft designs.
- Gross navigational errors are caused by incorrect flight plan data being entered into a FMS. An IFPM could sanity check flight plans against a database of terrain, ATC structure, airport locations (for existing aircraft) and (in addition) ATC clearance (for future aircraft with ATC datalink).
- Accidents can occur when aircraft flight plans are changed at the last minute. An IFPM could play an important role in future aircraft which employ 4-D flight plan negotiation with future ATC systems. An IFPM retrofitted to current aircraft could reduce air crew workload during stressful periods, whilst at the same time improving the quality of the decisions made by providing considered advice.
- Fuel management errors result both in increased fuel starvation risk and reduced operating efficiency. An IFPM retrofitted to existing aircraft could help reduce these risks, since it would have easy access to all the necessary data.
- Finally, accidents still occur due to incorrect aircraft configuration. An IFPM could monitor aircraft configuration against current situation and provide warnings accordingly.

3 PREVIOUS RELEVANT WORK

3.1 Introduction

Much work has been done and is still underway to produce new technology that should help to prevent CFIT accidents. The International Civil Aviation Organisation (ICAO) has developed a programme to reduce CFIT by 50% over a five year period: a steering team was formed in 1992 to implement this goal, with representatives from the major aviation players such as British Airways, Boeing and NASA. The steering team has considered operational issues such as crew training and guidance, but is also concerned with the development of intelligent warning systems that will incorporate knowledge of particular terrain to enable flight path monitoring and terrain threat evaluation. One such system is AlliedSignal's Enhanced Ground Proximity Warning System [4] which is described in section 3.2.

A similar device, the Ground Collision Avoidance System (GCAS) is being produced by Dassault Electronique [5]. This is described in section 3.3.

A significant factor in the majority of CFIT accidents is the loss of an air crew's situational awareness. In such a scenario, the crew's mental model of the position of the aircraft in relation to the ground, terrain features or other aircraft becomes distorted. To improve situational awareness, research is currently being performed on a so-called Enhanced Situational Awareness System [6] (ESAS), led by Honeywell and Westinghouse aided by GEC Marconi Avionics (GMAv). This is described in section 3.4.

A considerable amount of research and development effort has been directed at using artificial intelligence (AI) as an aid to the pilots of single seat military aircraft: the Defense Advanced Research Projects Agency (DARPA) initiated two parallel projects to develop a 'Pilot's Associate' [7], aimed at increasing the effectiveness of fast jet pilots, especially in conditions of extreme stress. This is described in section 3.5.

Similar research is also being carried out in the civil sector. The Cockpit Assistant System (CASSY) [8] is being developed by the University of the German Armed Forces, Munich in association with Dornier GmbH. CASSY is intended as an AI aid for two-pilot cockpits, and is discussed in section 3.6. It was developed from an earlier project, the assistant for single pilot IFR operation (ASPIO).

Two other current research projects have been identified as having particular relevance to the IFPM: Sextant Avionique in France is developing an AI cockpit assistant called FINDER [9], described in section 3.7. GMAv is also part of a consortium addressing various AI issues with funding from the European Commission's ESPRIT programme. One particular problem involves the specification and development of A Reliable Computer-Human Interface Environment [9] (ARCHIE), see section 3.8.

Considerable effort has been placed (particularly in the military) in integrating together navigational data from various navigation aids (including Terrain Referenced Navigation [10]). This is often called 'Data Fusion'. Methods for doing this are discussed in section 3.9.

Finally, section 3.10 considers the current AI 'state-of-the-art', with particular consideration to the certification of AI systems [11].

3.2 Enhanced Ground Proximity Warning System

Ground Proximity Warning Systems (GPWS) have been developed in a series of marks since their conception at Scandinavian Airlines (SAS) in 1969. The concept of a basic GPWS is to alert pilots to abnormal aircraft flight path and abnormal terrain clearances with respect to the ground or water, using a radio altimeter as the prime sensor. The system also uses signals from other existing aircraft sensors, such as descent rate and glideslope deviation. Warnings occur (typically) 10 to 20 seconds before the potential impact.

Mark I of GPWS issues simple verbal warnings, e.g. '*Pull up!*' (for most alerts) and is prone to nuisance alarms. This significantly degrades crew confidence in the system. Many CFIT accidents have occurred on aircraft fitted with Mark I GPWS because the cause of the alert was not given to the crew, because crew confidence in the system was so low that the unit was disconnected or because the alert was ignored.

The nuisance alarm problem was partially improved on later marks (II onwards), with the addition of some explanation as to the cause of the alert: e.g. '*Too low gear*', etc. However, the later marks are still prone to nuisance alarms and there are cases when no GPWS alert is given: the '*no warning*' scenario. This occurs when the aircraft makes a non-precision approach along a perfectly valid glideslope, except that there is no threshold at the bottom of the glideslope (e.g. due to navigational errors). Also, in extremely precipitous terrain the GPWS warning may be given too late for the crew to react, e.g. if the aircraft is flying towards a very steep rising slope.

Reports indicate that the latest mark of GPWS (Mk VII) has a greatly reduced nuisance alarm rate (one operator reports that no nuisance alarms were generated over an 18 month period).

Enhanced GPWS (EGPWS) is designed to overcome all the limitations of earlier marks of GPWS. The enhancements are made in addition to the existing functionality. The main extra addition to the system is a terrain database, containing geographical information (ground altitude and runway threshold locations) for areas around all international or alternative airports. This information is used to provide extra functions:

- **Terrain clearance floor:** An additional clearance 'floor', based on aircraft position, is provided which is independent of aircraft configuration. The floor lies below the 300 feet per nautical mile final approach slope (–2.8 degrees), and blankets the terrain or water around the airport. This is aimed at preventing the type of accident (described above) where aircraft make a perfectly valid non-precision approach in all respects except that there is no runway threshold at the end of the descent path. The EGPWS requires a database containing runway threshold positions: this database (and indeed the terrain database) can be easily updated by inserting a new memory card into the unit. Aircraft position is determined from the FMS/GPS weighted against quality factor.

- **Terrain ahead alerting and warning:** The EGPWS predicts the aircraft trajectory (based on current avionics information) into the future using so-called 'look ahead' algorithms. This predicted trajectory is then checked against the terrain database: if pre-set clearances are lost, the unit issues a *'Caution! Terrain!'* warning, which can typically be up to 60 seconds in advance of a potential impact. More urgent warnings are given as *'Terrain Ahead! Pull up!'*. Commercial aircraft do not typically fly in close proximity to the ground, so relatively low resolution data is sufficient to provide effective terrain awareness: e.g. 100 feet vertical and 0.5 to 8nm horizontal. This new technology enables the system to 'see ahead', even though the signals input to the EGPWS remain almost the same: the only extra requirement is horizontal position.

- **Terrain awareness display:** The EGPWS is designed to provide an output which can be used to depict threatening terrain optionally on an EFIS Navigation Display or a Weather Radar indicator. This information is displayed only if an alert has been generated, and gives pilots a plan-view of the aircraft trajectory in relation to the threatening terrain.

- **Altitude call-outs:** EGPWS has the ability to automatically call out altitude readings when the aircraft is performing a non-precision approach. This dramatically increases the pilot's vertical situational awareness.

EGPWS offers considerable improvements over earlier GPWS, including:

- look-ahead alerting algorithms;
- multiple radio altimeter inputs (to reduce the risk of loss of radio altitude);
- significant reduction in nuisance alarm rate;
- landing short alerting algorithms.

It will become available towards the end of 1996 and will have a unit cost of around $54,000 US (suggested informally by a leading manufacturer).

It is likely that fitting EGPWS to aircraft will significantly reduce the occurrence of CFIT accidents. However, EGPWS is not useful for addressing loss of situational awareness more generally. If an IFPM were simply aimed at reducing CFIT, it could probably not offer significant improvements over EGPWS in many CFIT circumstances. This suggests that proposed IFPM solutions should include EGPWS specifications (or the system itself) to address many aspects of CFIT. However, the IFPM could have a much wider range of functionality to enable it to be applied more widely.

3.3 Ground Collision Avoidance System

The Ground Collision Avoidance System (GCAS, not to be confused with the generic term used by EUROCAE WG44) being developed by Dassault Electronique is similar in concept to EGPWS, in that it uses a terrain database and radio altimeter output to provide forward-looking predictive ground proximity warnings. It has the following functions:

- A navigation function which uses GPS position, radio altimeter output, barometric altimeter output and the INS velocity outputs to produce a dynamic prediction of aircraft position into the future.
- A database function, which contains a world map of terrain elevation. Terrain elevation data is stored on a 100m grid in the vicinity of airports, but on a much looser grid (a few km) otherwise. This approach allows an entire map of the world to be stored in 5Mbytes. Each airport requires about 5kbytes, depending on airport geography. This map can easily be stored in a flash EEPROM memory cartridge, which can then be transferred to a ground station for update.
- An anticollision function, which predicts the likelihood of ground collision based on the following information:
  - the latencies such as the elementary computation cycle;
  - minimum g level to be applied by the pilot during the 'pull-up';
  - velocity vector of the aircraft;
  - bank angle;
  - aircraft configuration (flaps, gear);
  - aircraft altitude, weight.

Some of these parameters are processed in an aircraft model within GCAS, which depends on aircraft type (e.g. large, small, fly-by-wire, turbo prop, etc).

- A navigation monitoring function, which data-fuses the different navigation sources to provide a consolidated aircraft position. It uses a simple form of Terrain Referenced Navigation (see section 3.9.1) to verify aircraft position using the terrain database, radio altitude, barometric altitude and aircraft velocity vector. This function also verifies the quality of the information stored in the database. Such information is stored in the EEPROM in an 'incident memory' to allow post-flight investigations on the ground.

Crews are given warning times of 15–30 seconds during the cruise phase and 5–10 seconds warning on approach. Cautions are never generated (unlike EGPWS), because the designers found that, for example, a 60 second caution results in the pilot trying to investigate the cause of the caution rather than take avoiding action. It is their opinion that pilots are better off only being given warnings, as they know they must react immediately to these.

Development of GCAS is fairly advanced, with a fully-functional prototype already being flown. It is aimed at the same market as EGPWS, although it has different emphasis. It will be like a forward-looking, lower false alarm rate GPWS. However, it will do nothing to increase pilot situational awareness until the last 10 seconds on approach, since the crew are not given any extra displays or cautions until then.

3.4 Enhanced Situational Awareness System

The Enhanced Situational Awareness System (ESAS) is being developed by Westinghouse and Honeywell, aided by GEC Marconi Avionics. It consists of a number of subsystems, including:

- an Electronic Library System (ELS), which contains databases of terrain information, airport and runway locations, etc;
- Head Up Displays (HUDs);
- Enhanced Vision Systems (EVSs).

The system is intended to enable an aircraft to be positioned with an accuracy of about 5m relative to a runway or airport building, an air traffic control designated track or the best track to avoid meteorological phenomenon. This is achieved by using outputs from differential GPS (with other navigational aids) in conjunction with the ELS. The ultimate aim will be to allow aircraft to navigate or land at unequipped airfields, at least down to Category I weather conditions.

ESAS will also enable crews to predict the presence ahead of:

- volcanic ash;
- wake vortices;
- dry hail;
- clear-air turbulence;
- terrain.

ESAS is intended to increase air crew's situational awareness by providing them with more data than is available in current civil cockpits. The key to this is the use of EVSs. These present the pilot with a (perhaps synthetic) view of the terrain or runway ahead on a HUD: the view can be generated either from the geographical database and current position, or from forward-looking sensors such as an infrared camera in the 12mm band or a mm-wave radar (both of which can penetrate fog).

This clearly represents a different approach to solving the CFIT problem than using EGPWS or an IFPM. The cost of the solution may be significantly higher, since using ESAS would involve fitting extra equipment to the aircraft (e.g. an infrared camera). In addition, ESAS is not aimed at solving some of the problems that an IFPM could: for example, sanity checking FMS.

3.5 The Pilot's Associate

The Pilot's Associate program was created to apply the technologies of real-time, co-operating knowledge based systems for exploring the potential of AI to improve mission effectiveness and survivability of singleseat advanced fighter aircraft. The system is aimed at improving the pilot's mission situational awareness, advising on mission status, tactics, etc. It is clearly of relevance to the IFPM, since it has a similar application domain and yet is far more ambitious in concept.

Two parallel developments were undertaken, led by Lockheed and McDonnell Douglas respectively. Figure 3–1 shows an overview of the Lockheed system concept.

The system comprises of five sub-systems: the Pilot-Vehicle Interface, Situation Assessment, Systems Status, Tactics Planner and Mission Planner. The Pilot-Vehicle Interface provides the human-centred focus necessary to support the pilot's decision making requirements. Situation Assessment and Systems Status both fall into a category of 'assessment', and Tactics Planner and Mission Planner may be categorised as 'planning'.

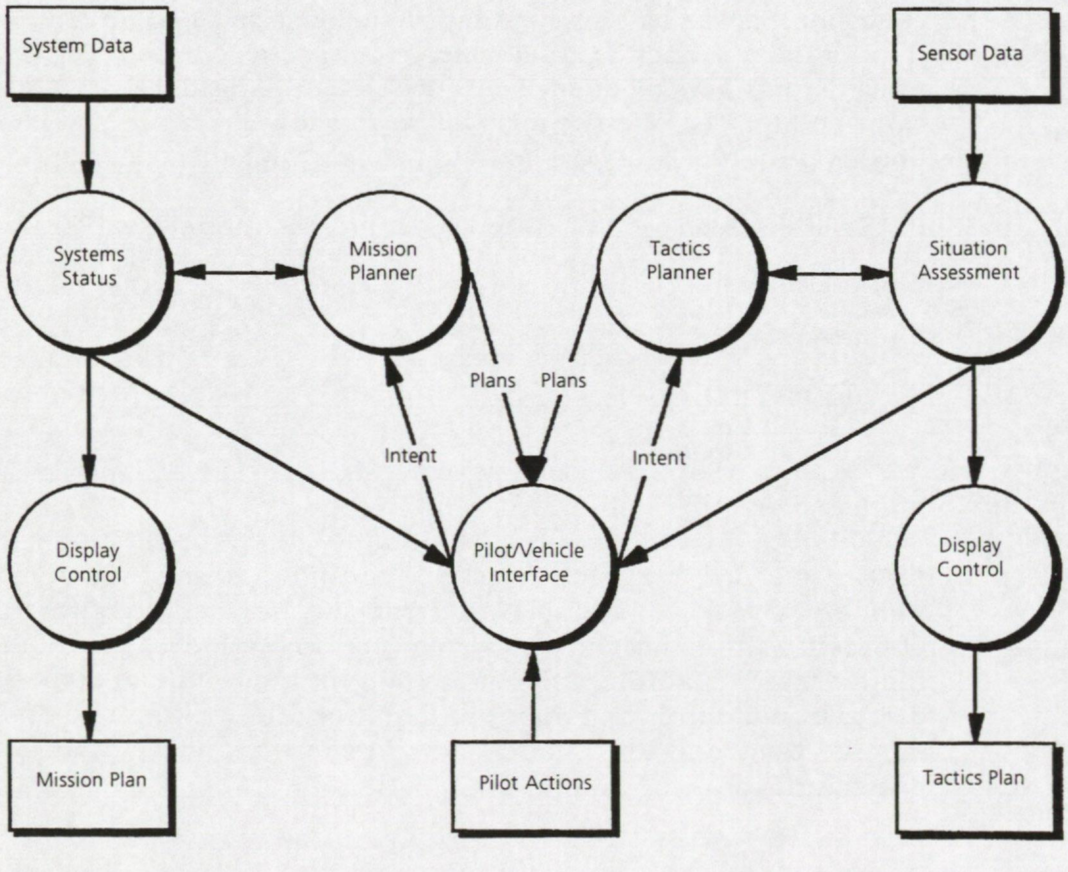

Figure 3–1 Pilot's Associate concept

Lockheed's Pilot Associate therefore uses three different categories of AI systems:

- man/machine interface controller;
- situational assessment modules;
- planning modules.

A similar concept could be used in an IFPM: a situational assessment module could monitor flight status versus current aircraft situation, and a planning module could monitor the flight plan.

The Pilot Associate's functionality includes the ability to help the pilot plan mission changes in highly stressful situations, e.g. when the aircraft is being tracked by missiles. This gives rise to the idea that the functionality of an IFPM could therefore cover the management of flight plan changes in stressed situations (e.g. tactical ATC intervention approaching TMA). This might help break the long chain of events that sometimes cause accidents, at a very early stage, e.g. by preventing erroneous flight plan changes being entered into the FMS.

3.6 The Cockpit Assistant System

3.6.1 *Introduction*

The Cockpit Assistant System (CASSY) is being developed at the University for the German Armed Forces in Munich with support from Dornier GmbH [12]. CASSY is described as a 'Knowledge-based pilot associate', which 'weighs up the entire (aircraft) situation and generates corresponding advice, warnings and proposals'.

CASSY is intended as an artificial co-pilot, which recommends flight plan revisions when needed, warns the pilot if he deviates from his Air Traffic Control clearance and monitors aircraft systems. It has been trialled successfully in two aircraft simulators and in flight tests in June and July of 1994, in co-operation with Dornier and Deutsche Forschungsanstalt fur Luft- und Raumfahrt (DLR).

Daimler Benz Aerospace (DASA) is considering actively developing CASSY. At present, no licenses relating to CASSY technology have been agreed.

The CASSY project is clearly of major importance when considering the IFPM concept, since it is very similar. Section 3.6.2 outlines the design of CASSY. Section 3.6.3 discusses how CASSY performs operationally. Section 3.6.4 discusses the interface used for CASSY, and section 3.6.5 summarises the results of discussions held with the CASSY researchers.

3.6.2 *CASSY design*

CASSY functions are divided into three classes: situation assessment, flight planning and services (comparable with the three types of Pilot Associate modules).

Situation assessment

The situation assessment function is intended to run entirely autonomously. Situation assessment collects and evaluates all data necessary for the corresponding flight phase, for example:

- dynamic data from the aircraft avionics systems;
- ATC or other data from the ground (via datalink);
- static data (e.g. from a standard navigation database, but not including terrain elevation data);
- status of on-board systems;
- status of ground systems;
- pilot actions (i.e. models pilot behaviour);
- commands and intentions of the cockpit crew;
- airline standard safety procedures.

The knowledge-base used for the artificially intelligent situation assessment module is derived from both pilot and system knowledge. Elements included are:

- models of pilot knowledge of flight guidance and control of cockpit systems;
- knowledge of all the systems involved;
- knowledge of procedures or actions to be carried out under certain conditions (e.g. ATC instructions).

CASSY models pilot behaviour on three levels:

- standard behaviour (the behaviour of a 'normal' pilot);
- individual behaviour (i.e. allowing for variations between different pilots, but as yet only implemented in certain segments);
- behaviour in hazardous situations.

These models are used to provide different levels of advice to pilots (e.g. the hazardous situations model is used to provide warnings, whereas standard behaviour may just provide advice).

Flight planning

The flight planning function involves CASSY making internal hypotheses about pilot intentions which are verified or rejected on the basis of actual crew actions. A recognised new pilot intention will then be integrated into the flight plan held by CASSY. Flight planning is ultimately controlled by the crew who review different plan options. After a new flight plan is accepted by the crew, CASSY then 'negotiates' with ATC for clearance via a datalink. The flight plan proposals and accompanying decision criteria are shown on a graphic display. The control of the process (if desired) is by voice input.

This flight plan is then used by the situational assessment part of CASSY, in order to derive what actions ought to be taken by the crew and to issue warnings if these actions are not taken.

Services

The service functionality of CASSY can:

- set-up communication and navigation frequencies, as well as autopilot commands and modes;
- control aircraft systems such as landing gear and flaps;
- present the crew with data from the navigational database.

These services must be called up specifically as requested by the crew.

3.6.3 *Operational performance*

CASSY was demonstrated on the simulator at Munich. A complete half-hour flight was undertaken, including:

- **Pre-take off flight planning.** This involves the pilot merely stating to CASSY the departure point and destination runway. The flight plan is then generated by CASSY's Automatic Flight Planner from a conventional navigational database. This flight plan is displayed on the navigational map display (referred to as the Horizontal Situation Indicator (HSI)), including missed approach path, and the pilot is asked if the plan is acceptable.
- **Take-off.** The simulator was flown under manual control to allow the aircraft to deviate from track (for demonstration purposes), as autopilot flight would have resulted in much less interaction with CASSY (that is not to say CASSY has nothing to offer under autopiloted flight). CASSY generates advisory messages if the flight path deviates from the flight plan (e.g. 'CHECK HEADING') or if aircraft configuration or status is inappropriate for the flight phase (e.g. 'CHECK GEAR', upon successful take off, 'CHECK FLAPS' or 'CHECK ENGINE SPEED').
- **En-route.** The weakest part of the system is inputting ATC clearance into CASSY. ATC instructions and clearances are obtained by CASSY interpreting the pilot's verbal acknowledgement of ATC instructions. The situation would be improved through the use of an ATC datalink, since the clearance data would then be readily available. ATC clearances and vectoring were simulated for the flight's profile. CASSY autonomously updated the flight plan with the vectored track, re-joining the original track at a 'best-guess' waypoint. The pilot was then asked if the plan was to be accepted.
- **Engine failure.** At all times during the flight, CASSY automatically displays the nearest alternative on the HSI. An engine failure was simulated which CASSY immediately detected: CASSY advised an engine speed check on the remaining engine to hold altitude. The HSI then displayed several colour-coded options for the flight re-planning. The pilot chooses the preferred option by e.g. 'SELECT GREEN PLAN'. The new flight plan included all relevant elements, including go-around details.
- **Landing.** CASSY continued in its autonomous situation assessment, issuing occasional heading, altitude and speed warnings. CASSY also assesses the crew: for example, it checks that the pre-landing checklist is completed at the correct time.

An impressive feature of CASSY demonstrated was the 'intent recognition' capability. If the pilot is given clearance to miss a waypoint or turns to avoid a thunderstorm and changes heading accordingly, CASSY attempts to interpret the intention of the pilot. It waits until it has determined the most likely pilot intent, and then asks if the pilot's intention is to e.g. avoid thunderstorm. The pilot can then confirm or reject this hypothesis. Thus the flight plan is maintained autonomously.

Overall:

- the system automatically performs flight planning well;
- the system is able to cope with aircraft system failures and ATC intervention;
- the voice interface works reasonably well;
- recognition/understanding of ATC clearance is a major problem, although improvements are planned (for example use of ATC datalink);
- CASSY would be much more than a 'black-box' add-on to an aircraft. It amounts to a re-design of the man/machine interface.

3.6.4 *Interface*

CASSY's man/machine interface is primarily voice, but is backed up by text. Inputs are accepted as voice commands. Acknowledgements and advice are given through an artificial voice. Extensive information (e.g. horizontal navigation display) is displayed graphically. Dornier claims that using a speech interface to the crew offers several advantages:

- a verbal warning guarantees the immediate attention of the crew, independent of the present line of sight of the crew;
- commands can be issued to the system when the crew have got their 'hands full';
- voice communication is natural for the crew.

However, aural warnings are amongst the first to be washed out in high workload situations. The interface is therefore backed up by text (i.e. displaying the last voice output and input) and safety critical inputs are confirmed. For example, an entered command 'ACCEPT GREEN FLIGHT PLAN' is firstly displayed as the text 'Accept green flight plan?' to which the pilot must confirm with 'ACCEPT'. This process obviously takes time, and it is not intended that commands issued to CASSY should be time critical: the functions that CASSY supports (e.g. flight planning) that require voice input can all be carried out in somewhat slower time. CASSY is intended as an autonomous situation assessor that only interacts with the crew to direct attention to the most pressing task, if necessary.

It is realised by the developers that the voice channel is already quite overloaded in modern operating conditions, mainly because of the interaction between the crew and ATC. This might be relieved with the advent of ATC datalink, which CASSY probably requires if the interface is to be acceptable.

The interface performs reasonably well operationally, with 85-90% of commands recognised first off. Advice and entered commands are backed up by text which is displayed at the bottom and top of the HSI.

Operationally, it was found that pilots take 3–4 flights to familiarise themselves with CASSY's command set. The command set is context-sensitive, that is the vocabulary the system is trying to recognise is updated regularly and depends upon the flight phase. This decreases the processing time for voice recognition and increases the overall vocabulary.

3.6.5 *Discussion*

CASSY philosophy

CASSY is based on a philosophy that originates from work carried out in the US (mainly by NASA) [13,14]. This is that current automated systems have failed to increase flight safety because, although they cope well with normal situations, they do not cope with abnormal situations. At such times, the automated systems tend to **increase** the workload of the pilot: however, this is just when the pilot needs their assistance. Therefore, the inclusion of highly automated systems means that the pilot is less able to cope with abnormal situations, and may understand the aircraft's situation less well than if the system was not installed.

This has given rise to the idea of 'human-centred' automation, which is a re-think of the conventional way in which automation is viewed. In human-centred automation, just as the humans operating the machine must understand it for correct operation, so must the machine understand the humans. Such a system should smooth the workload of the operators, and (most importantly) direct their attention to the most pressing problem.

CASSY attempts to achieve this by carrying out an autonomous situation assessment. This assessment can be more complete than it is possible for the crew to carry out, as the system should not get absorbed (as crews may) by a single, possibly irrelevant, task.

Note that CASSY is seen as taking on a role as aircraft information integrator: it provides an extra level of data fusion between different aircraft systems which is absent from current aircraft.

CASSY used to prevent controlled flight into terrain (CFIT)

The only specific function that CASSY performs with respect to CFIT is the monitoring of aircraft altitude against minimum safe altitude (MSA). Even though CASSY is not a GPWS, a large percentage of the more recent CFIT accidents (particularly the Airbus incidents) may have been prevented had the aircraft been fitted with a CASSY-like device. The system is designed to break at an early stage the chain of events (human error) that sometimes lead to CFIT, well in advance of a 'last-ditch' GPWS warning. A terrain database could easily be included in the system, which could then take over the ground proximity warning function. Warnings could then be issued taking into account the complete aircraft situation.

Software development

The software modules used by CASSY are characterised by the use of AI methods. For example:

- fuzzy logic is used for assessment of alternatives;
- heuristics (rules) are used for assessment of pilot behaviour and production of rule-based knowledge;

- Petri nets are used for process modelling (a Petri net is an AI method for representing and analysing complex concurrent systems, i.e. systems with many things happening at once).

CASSY has not been developed as a commercial system, but rather as a feasibility study/technology demonstrator. It has therefore not been developed using quality-assured procedures, and as such could not be certified. The team note the current absence of well documented development procedures for knowledge-based systems (KBSs). This situation is likely to be rectified in the future with both NASA and the EC funding large projects to develop such procedures.

CASSY was developed completely from scratch in C and C++, i.e. the development did not use any AI-specific tools. This approach was taken because the development team felt that existing KBS tools could not achieve the required real-time performance.

The researchers note that testing such a large system is difficult: the database used is extremely large and the variety of situations the system could be called upon to deal with is even larger.

Time scales and costs

CASSY has reached a stage whereby it is ready for commercial development: its feasibility has been demonstrated.

Work carried out in conjunction with Dornier has estimated that the cost of developing a commercial version of CASSY (i.e. with proper quality assurance (QA) procedures so that certification is possible) would be in the order of £20M to £50M.

Future enhancements

A military version of CASSY is currently being developed for use on large military transports. This is more complex, and has the additional features:

- a terrain database, to facilitate strategic flight routing;
- a forward looking camera as a data source;
- an inward-looking camera (observing the crew);
- a more thoroughly developed model of individual pilot behaviour.

If CASSY is to provide a more complete situational assessment than the crew, then it needs access to all the information the crew has available. An important part of this information could (in principle) be obtained from the forward looking camera: the technology for, e.g., runway recognition is in existence (used in military applications). The military version will use its forward looking camera for obstacle avoidance in low-altitude flying.

The inward-looking camera is intending to gain more information for crew assessment. For example, the system might use information such as which direction the crew members are looking as input to its crew assessment. This clearly adds to the system's situational assessment capability: however, highly advanced technology would be required.

3.7 FINDER

Sextant Avionique is currently performing AI research for cockpit use, sponsored by the French Direction des Programmes de l'Aeronautique Civile (DPAC).

Sextant has identified en-route diversions as an area in which AI could help crews (in a similar way in which CASSY's flight-planning module might). FINDER is intended to fulfil three roles in the cockpit:

- to help crews to understand and assess abnormal situations;
- to monitor crew errors continuously;
- to react promptly in the event of errors.

Many ATC tactical interventions result in a new flight plan that is far from optimal (in terms of delay or cost). The system is designed to help crew members to optimise their flight plan continually by suggesting solutions based on exhaustive data. As with CASSY, a major assumption is that the aircraft will be 'negotiating' electronically with ATC its 4-D flight plan, via a datalink.

Air France pilots have been heavily involved with the development work, and the FINDER system generally produces the same revised flight plan as pilots but more quickly.

FINDER bases its re-routing decisions (e.g. alternative destination airports) on a range of data, including fuel limitations, runway suitability, customs availability, ground equipment and freight handling. The system will automatically perform a search by area if neither the primary or alternative airports can be reached. The search area is extended until a solution is found or the operating range of the aircraft is reached. It is left to the crew to determine weather conditions at alternative airports.

Alternatively, crews can test preferred diversions to check viability, or the system can calculate the latest point at which an aircraft can still be successfully diverted.

The FINDER's architecture is similar to CASSY's, with the following modules:

- situation assessment;
- re-planning operations-management;
- dialogue management.

FINDER is still undergoing active development: it is not known if it has undergone flight tests as yet. The progress on the project has led the FAA to warn of the difficulties that certification of AI will present, in its Digital Systems Verification Handbook, volume 2.

3.8 ARCHIE

ARCHIE is being developed by a consortium (including GMAv, Bertin et Cie of France, AI specialist Computer Resources International (CRI) of Denmark, and the MicroCentre, University of Dundee), with funding from the EC's ESPRIT programme.

ARCHIE does not appear to be as far advanced as CASSY or FINDER, but is intended to operate along broadly similar lines.

Its situational assessment subsystem is intended to determine which plan the crew is following in real time. This is a significant computational problem and needs considerable processor power; however, it is not beyond the capabilities of the latest processors.

ARCHIE is intended to monitor autonomously the situation until some sort of significant error is made by the crew. At that stage, it will issue, perhaps, a warning which should result in the crew taking corrective action.

The key to success is the system being able to determine what is occurring from two sources: environmental information, such as aircraft status, and procedures/plans. It is the procedures and plans part that requires AI for interpretation.

GMAv has demonstrated a PC-based 'kernel' system, which shows how AI can warn of imminent errors by using 'plan-recognition' capabilities to warn of:

- penetration of prohibited airspace;
- descending through a cleared level;
- taking off in an incorrect aircraft configuration.

3.9 Improved Navigation Systems

3.9.1 *Terrain Referenced Navigation*

A key element in CFIT accidents is aircraft simply 'getting lost'. A major element of any device designed to reduce CFIT is bound to be a terrain database, since the latest data storage technologies are capable of cheaply storing enough information to provide global coverage in useful detail. This terrain database can be combined with the outputs from other existing flight deck instruments (the radio altimeter, inertial navigation system and barometric altimeter) to provide an extra cross-check for current aircraft position by utilising a technique called Terrain Referenced Navigation (TRN).

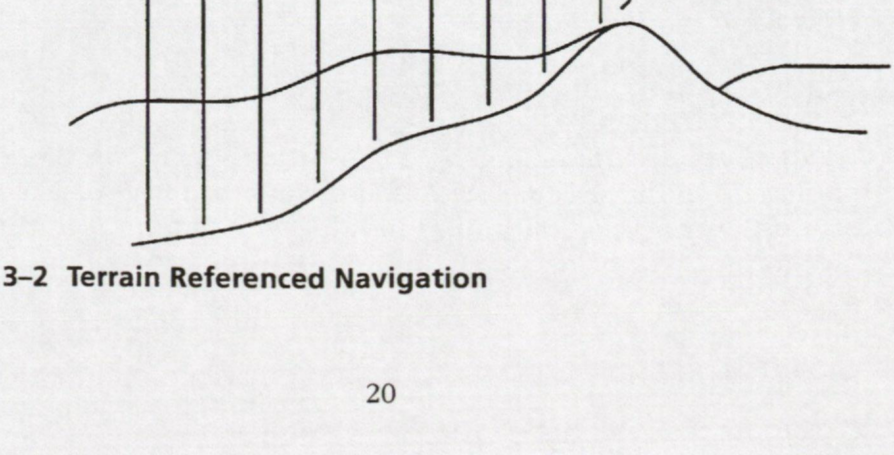

Figure 3–2 Terrain Referenced Navigation

Terrain Referenced Navigation uses the radio and barometric altimeters to measure a profile of the terrain below the aircraft's recent flight path which is then compared to the digital terrain elevation database (see figure 3-2). The result of the process is a sequence of position fixes which can be used to correct the errors in the aircraft's inertial navigation system.

TRN is the basis of many military precise navigation systems because of its high resilience to jamming and relative passivity (only utilises a downward-looking radar). It is also a basic element of GMAv's GOCAT (Ground and Obstacle Collision Avoidance Technique). GOCAT is intended primarily to reduce CFIT accidents and its functionality appears to be broadly equivalent to EGPWS.

TRN clearly only works well in regions which have elevation relief: it will not work over flat terrain or the sea. Some CFIT accidents do occur in regions of flat terrain: however, the system can be made to acquire position within a very short time of making a land fall (400m) and it is possible to use a technique related to TRN: Terrain Characteristics Matching (TCM) to navigate over completely flat terrain.

TCM uses the reflection characteristics over different terrain types (e.g. the differences between dense vegetation or open land) to provide event markers by which to navigate. This is certainly feasible (and is used) for aircraft flying at low altitude: it may be less feasible for higher altitude use, since the footprint of the radio altimeter may become too large to provide the event marks (since it will, at any time, contain many different terrain features).

Operation of TRN is also not possible above 8,000 feet terrain clearance because of the operating limitations of the radio altimeter. Operation of TCM would not be possible unless the signal strength of the reflected signal in the radio altimeter is made available to on-board processors (e.g. this is not available if the only connection between the IFPM and the radio altimeter is an ARINC 429 databus).

It is therefore possible to obtain an extra degree of confidence in navigational data, in all instances when CFIT is a potential problem, using TRN/TCM. TRN operates well in mountainous terrain when the ground clearance is less than 8,000 feet (providing navigation data for one important class of CFIT accidents), and TCM operates well at lower altitude in flat terrain (providing navigation data that might prevent aircraft landing where there is no runway).

3.9.2 *Integrated navigation systems and Kalman filtering*

Accurate and highly reliable navigation is provided in military systems by integrating the data from a variety of navigational sensors. The techniques used are applicable to civil aviation, and may allow the integration of GPS, GLONASS or other future satellite navigation systems data into CFIT-prevention systems. Since it is envisaged that satellite navigation will eventually be used as an important source of civil aircraft navigation information, it seems reasonable to assume that an intermediate stage will be its use in warning systems such as an IFPM.

A key element of the navigation systems is the use of Kalman filtering. This filtering uses the past trajectory of the aircraft to estimate where the aircraft is expected to be at the next data readout from the navigation sensor: the two positions (measured and predicted) are compared. The filter uses knowledge of the sensor accuracy and noise, the aircraft's dynamics and the position predictor's past performance to provide a least-squares estimate of current position (under certain conditions the solution can be shown to be 'optimal', in that it provides a least-mean-squared best fit to current position).

Figure 3–3 shows the architecture for a military navigation system, which is termed a 'federated navigation system' since it uses several independent subsystems. The primary system is the Inertial Navigation System (INS). Output from the INS is fed into each fixing subsystem. The fixing subsystems each include their own Kalman filters. The outputs of these filters are then combined in a data fusion subsystem (another Kalman Filter) to yield a global navigation solution.

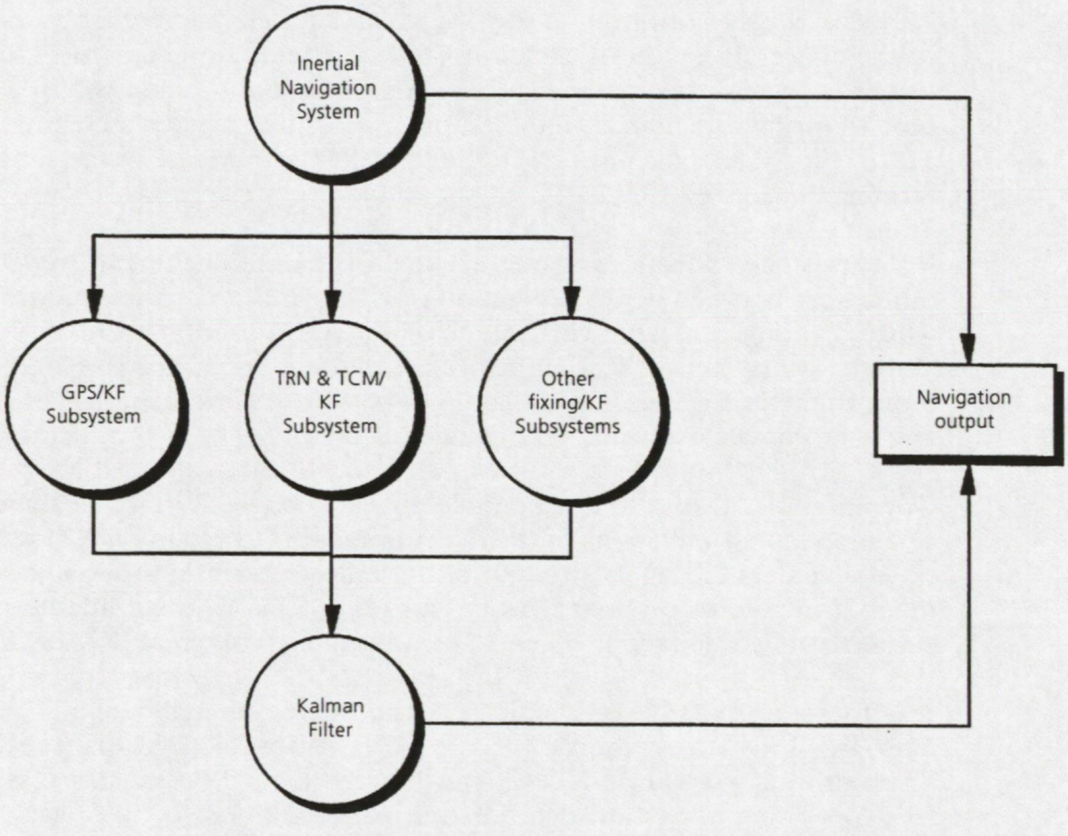

Figure 3-3 Federated navigation system

Each of the fixing subsystems acts as an independent navigation system. This approach offers the advantage of improved failure detection. The global solution is available for comparison against the outputs of the subsystems. When a subsystem failure or degradation is detected the global solution can be recalculated excluding the erroneous system.

3.9.3 *Terrain database production and certification*

Sources of data for a terrain database would be primarily military. For example, the US Defence Mapping Agency have a Digital Terrain Elevation Database (DTED) which covers large areas. The accuracy and reliability of this data is increasing all the time, particularly as new mapping satellites are launched (the US plan to launch a satellite, TOPSAT, capable of mapping the entire surface of the planet in a year with a resolution equivalent to 50,000:1). Unfortunately civil users may not have access to data with high enough resolution for TRN. However, stereoscopic satellite imagery is now available for commercial use (e.g. SPOT imagery). This imagery can be used to generate automatically terrain databases using computerised image processing techniques. For example, it is possible to generate a reasonably accurate (better than 10m elevation accuracy with 50m horizontal resolution) map of a 60x60km area in a day. Digital terrain data is therefore becoming increasingly available.

A commercial aircraft navigation system utilising terrain referencing would have to be certified before it could be used. This presents a difficulty: it would be impossible to provide a database which is certified as accurate, since surface features change with time. Even if a terrain database is accurate over a certain area at a given time, it may then become out of date if, for example, a new radio mast is erected.

An important point is that the terrain database used to generate CFIT warnings need not be to the same precision as the complete database used for the TRN. A lower-resolution terrain profile against which CFIT warnings are generated can be easily obtained from the full-resolution data, and suitable safety margins can be added to allow safety certification. EGPWS utilises just such a low-resolution database, and has indeed been certified safe for use on commercial aircraft.

The problems with certifying a terrain database suitable for use in a TRN system can be reduced. Firstly, the areas in which greater resolution is required are in the proximity of airports. Such regions tend to be subject to strict planning control, and landscape features are unlikely to change without notification. Secondly, a TRN system is to some extent self-certifying. Output from the algorithm that matches the over-flown terrain profile with the database can be used to give a 'confidence measure', i.e. how good the match is. This can be used to place weight onto the TRN output, so that it is only used if a good match exists. Areas where a bad match is achieved could be stored by the system. The 'bad-match' data could be used to generate better databases for future use, probably by centralised collection of the data (as planned with GCAS).

3.10 Artificial Intelligence

3.10.1 *Neural Networks*

Artificial neural networks are computational structures loosely modelled on biological processes. Typically they are constructed from connected layers of simple processing elements. The processing elements (the nodes) implement a simple transfer function from inputs to outputs (such as the summation of inputs and non-linear thresholding). The connections between nodes have associated weights which determine the strength of the connection. These weights are changed during a training phase, using an optimisation algorithm, to 'teach' the neural network to recognise certain data or characteristics. Figure 3–4 shows an example neural network and Figure 3–5 shows an example transfer function of a single node.

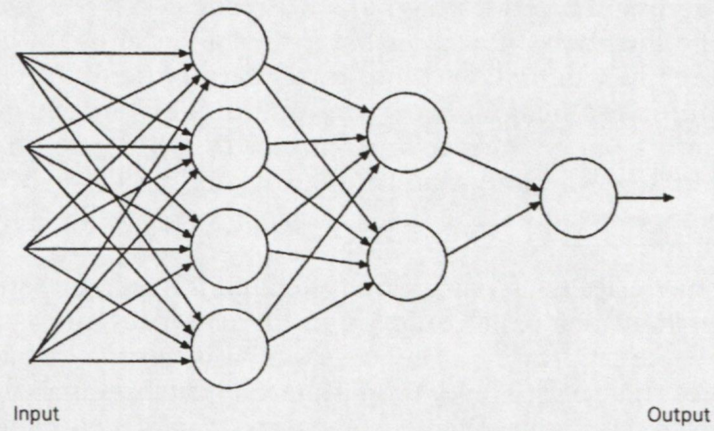

Figure 3–4 Example neural network

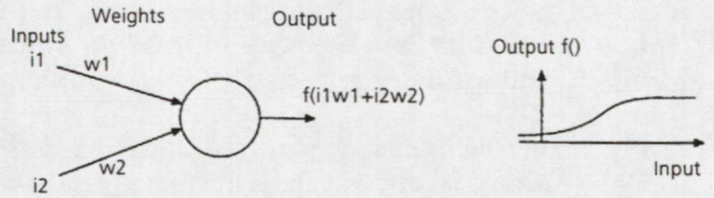

Figure 3–5 Example transfer function of a single node

The principal use of neural networks (NNs) is in pattern recognition, for example hand writing recognition in which the network is 'taught' to recognise different handwriting versions of the alphabet. This 'learning' is then frozen-in by not allowing the weights between the nodes to change anymore.

Neural networks have a number of characteristics which make them more or less suitable for inclusion in the design of an IFPM:

- Neural networks are generally trained on test data to recognise certain features in the input data: knowledge of the underlying pattern mapping (the process being modelled) is unnecessary. This is a definite advantage, since it means that complex patterns can be recognised without need for a highly structured model of the physical system, leading to far cheaper systems.
- Large networks are generally slow to train, although potentially fast to operate once trained since they have natural massive parallelism. The effective size of networks is therefore limited by the computational requirements of the training algorithms, not the actual system they are implemented on.
- It is very difficult to determine what 'rules' a neural network has learnt since the information is distributed throughout the weights in the network. Therefore, confidence in a network's behaviour can only be gained through comprehensive training and testing. This may have a significant impact on the cost of NN development.

• Neural networks are robust to local faults and damage, since damage to or failure of individual nodes may have little effect on the performance of the overall system. Hence if they can be verified, then they may be useful for safety critical applications.

3.10.2 *Fuzzy logic*

Fuzzy logic is one of the most widely used AI principles. It has been applied in commercial systems as diverse as cameras, washing machines and even trains, mainly in control applications.

Conventional computer logic is Boolean, that is, a state is represented by a one (state TRUE) or a zero (state FALSE). For example, the aircraft's ground clearance state might be represented by:

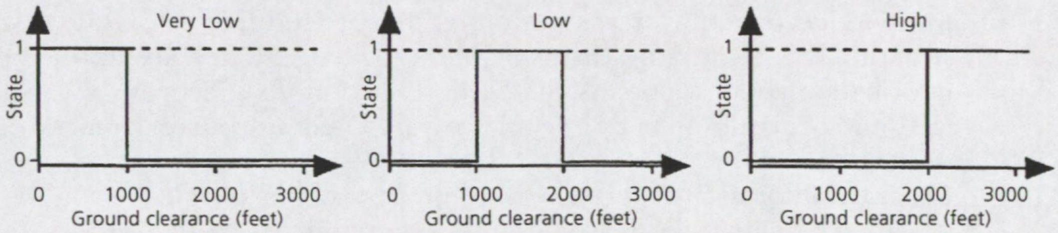

Figure 3–6 Boolean logical states for ground clearance

Each of the ground clearance states, Very Low, Low or High can only have one of two values, True or False.

In a fuzzy logic system, the states are allowed to have a distribution of values (for example from 0 to 1) as shown in figure 3-7 below.

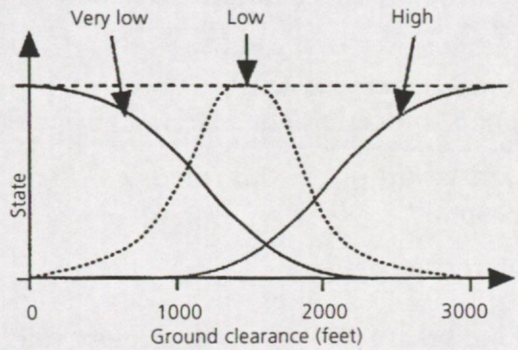

Figure 3-7 Fuzzy logic states for ground clearance

The advantage that fuzzy logic has over Boolean logic lies in its ability to assess alternatives using a large range of input data, where each input datum has a range of values. The action of a fuzzy logic node is similar to a neural network node: the difference is that with fuzzy logic the behaviour of the node is not learned, but programmed. The certification of fuzzy logic systems therefore presents no extraordinary difficulties, and indeed such systems are already used in safety critical applications.

Fuzzy logic principles can also be applied to entities other than states: for example, certain Knowledge Based Systems (KBSs) use fuzzy rules, fuzzy assertions and fuzzy goals. Such systems are sometimes termed 'neuro-fuzzy', because fuzzy logic is used and the operation is akin to that of the brain.

3.10.3 *Knowledge Based Systems*

Knowledge Based Systems (KBSs) comprise a knowledge base and an inference engine. The knowledge base stores collections of facts, heuristics (i.e. rules of thumb for solving a problem) and other knowledge about a process. The inference engine implements the reasoning mechanism by which the most appropriate facts and heuristics are used to make inferences or deductions. These inferences are, or are used to generate, the output of the system. Whilst inference engines tend to be application independent, the corresponding knowledge bases are highly application specific.

Knowledge based systems generate the procedures to apply, in any given situation, by combining the available knowledge. They are appropriate when information about a process can be described more effectively by a collection of facts and heuristics than by a set of pre-computed procedures or algorithms.

Often the information stored is based on an expert's knowledge and the system is designed to mimic the reasoning process conducted by that expert. In this case the system may be known as an expert system.

3.10.4 *Certification issues*

A major uncertainty about the feasibility of an IFPM is the use of AI in such a safety-critical application (for IFPM elements that require AI for their operation). A considerable amount of research has been done in the certification of AI systems by one of the largest users of advanced technology in the world: NASA [11].

There are essentially three different elements to a KBS which each need to be verified:

- The actual expert knowledge upon which the system is based (e.g. gained from pilots, procedures and aircraft characteristics).
- The translation of this knowledge into a language which the system can understand.
- The inference engine.

NASA has found that the best way to attempt validation of the expert knowledge is by review panels: the heuristics upon which the system will operate are considered in detail by as wide a range of experts as possible. This approach is appropriate for huge projects (such as the space shuttle's control software) but may prove to be too expensive for cost-effective IFPM solutions.

Work is also being carried out in Europe on the certification of AI systems, particularly the Euclid programme of research [15]. This EC-funded work is far from complete and is not as advanced as that carried out by NASA.

Ensuring that the heuristics are correctly translated into code which the inference engine can interpret is also a difficult task. It can only be achieved by verifying that results generated by the KBS are correct. This process can be aided by checking that the KBS is arriving at a correct result by correct reasoning: it is possible to construct systems that will answer questions about how they reached a conclusion. This is an important feature in favour of using KBSs in an IFPM, because if a pilot distrusts the advice or warning given the system can (upon demand) explain the reasoning.

Verifying the inference engine is the easiest task, since this tends to be an entirely separate piece of code from the knowledge base. This portion of the program has rigid requirements that can be outlined and tested independently from the rest of the expert system.

The conclusion drawn is that certification of KBSs is possible, even though the systems are more complex than traditional software systems and formal development procedures are yet to be defined.

Validating and certifying NNs presents entirely different problems, since the output of the NN is not 'specified' as such but 'learnt'. NNs may still produce acceptable output (based on the training in other circumstances) even when the inputs to the network have never been received before.

Therefore the only way of certifying a NN for a safety-critical application is by testing the output for all possible inputs after it has been trained.

NNs have previously been used as integral parts of AI systems in the following way: to reduce a huge mass of input data to a lesser number of hard facts. These facts are then the input to a KBS. This system concept is depicted in figure 3-8. This approach (if required) could be used in an IFPM.

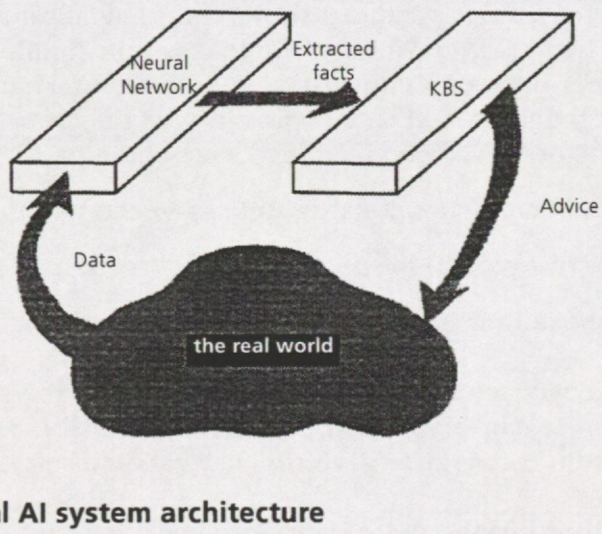

Figure 3–8 Typical AI system architecture

3.11 Summary

This section has examined the areas in which work has been carried out which is of relevance for the IFPM. The main conclusions to be drawn are:

- Enhanced GPWS or GCAS offer considerable advantages over previous versions of GPWS. Replacement of old marks of GPWS by the newer systems on commercial transport aircraft should in itself reduce the rate of CFIT accidents.
- Other work is ongoing to increase air crew situational awareness. This work (such as ESAS) is a different approach to reducing CFIT accidents than the concept of using an IFPM.
- A great deal of work is being done on behalf of the military into providing artificially intelligent aids to pilots. This work appears to be producing successful results.
- Work is also ongoing in the civil sector, on projects such as CASSY, FINDER and ARCHIE. These projects are similar in concept to the IFPM.
- Considerable progress has been made in the last decade in the use of terrain databases (which would form an integral part of an IFPM) for navigation, using a technique called Terrain Referenced Navigation. Inclusion of TRN in an IFPM would enhance the integrity of a key piece of data in the system: that of current aircraft location.
- Issues concerning the certification of AI are being investigated. Certification should be possible, but is likely to be expensive.

4 HUMAN FACTORS

4.1 Introduction

Analysis of aircraft accidents shows that a significant proportion are due to some kind of human error. This section looks at the human factors contribution to CFIT and other accidents, and how an Intelligent Flight Path Monitor might help prevent them through its interactions with the crew.
Three factors have been identified which have particular significance:

- lack of crew situational awareness (section 4.2);
- air crew/ground misunderstandings (section 4.3);
- use of advanced cockpit automation (section 4.4).

The first two factors have caused significant numbers of accidents/incidents in the past and it can be seen that problems can be reduced through the use of advanced technology (e.g. vertical navigation displays or ATC datalink).

For the third factor, use of advanced cockpit automation, it is not at all clear that advanced technology can be a solution. This is discussed at some length.

4.2 Situational awareness

It is estimated that 66% of CFIT accidents are attributable to a lack of 'Situational Awareness' (SA) [2]. SA can be thought of as the crew's access to a 'comprehensive and coherent situation representation which is being continuously updated with the results of recurrent situational assessments'. In other words, a pilot is constantly evaluating the current state of affairs in order to form a mental picture of current events. CFIT accidents sometimes involve not just a lack of knowledge regarding the aircraft's situation with respect to the ground: a lack of knowledge of the state of aircraft systems can also contribute.

For a crew to have a correct mental 'picture' of the aircraft's situation requires knowledge of:

- the present state of the aircraft and its environment;
- the 4-D flight plan;
- airline procedures and aircraft performance limitations.

(It is interesting to note that these are exactly the data required by an IFPM to assess a situation and provide warnings/advice.)

Increasing the crew's vertical SA will contribute greatly to the reduction of CFIT accidents, that is the crew's awareness of their situation with respect to vertical navigation and terrain should be enhanced. There are essentially four methods by which an IFPM could do this (in order of increasing complexity):

(1) Automatically produce ground clearance 'call-outs' when, for example, making non-precision approaches to airfields (ground clearance as measured by the radio altimeter). This approach is quite appropriate when the airfield is situated in flat terrain, and is an approach used by EGPWS and some other safety systems. It would not be appropriate to increase vertical SA at airports with multiple step-down approaches in mountainous terrain (e.g. the CFIT 'blackspot' airport Kathmandu).

(2) Provide pilots with a 1-Dimensional vertical navigation display. Figure 4-1 shows an example display, for an aircraft just beginning a step-down approach. It shows the crew aircraft altitude versus horizontal distance. This kind of display is the simplest possible graphical aid to assist in increasing vertical situational awareness. However, it suffers from lack of representation of horizontal navigation: if the flight plan involves many horizontal waypoints/turns, the full situation is not represented. However, it may be of use in displaying deviations between the current flight path and the 3° glide slope on final approaches (see figure 4–2). This might help prevent CFIT accidents in which aircraft land where there is no runway threshold.

(3) Provide pilots with a 2-Dimensional (plan view) vertical navigation display. Figure 4–3 shows an example display, similar to that provided by EGPWS in an alert situation (display is on the weather radar). The figure shows a time-series of images as displayed to the pilot if the aircraft were approaching terrain. The advantage of this display over the 1-D display discussed in (2) above is that crews are given the complete navigational (both horizontal and vertical) situation. The difficulty with such a display is representing the vertical information on the plan view, without cluttering the display. This is overcome in the EGPWS by displaying terrain as shaded areas, according to the 'threat' it poses to the aircraft: the most threatening terrain (i.e. terrain which the predicted trajectory of the aircraft intercepts with) is displayed in

red, with less threatening terrain displayed in less bold colours. The only limitation on this display is that it cannot sensibly display the runway threshold approach situation, e.g. to display glideslope situation. A 1-D display might be more suitable for this.

(4) Provide pilots with a 3-Dimensional vertical navigation display. This system would present pilots with a perspective view of their surroundings (see figure 4-4). This type of display may be incorporated in ESAS: it would be possible to add artificial features to the view displayed (e.g. runway lights or visual approach slope indicators, VASIs) to enhance the pilot's situational awareness. Such a display has disadvantages however. The ability of the pilot to make precise check readings on specific features may be limited, which can introduce ambiguities with respect to the frame of reference of the display. It is also bound to be more expensive to implement than 2-D or 1-D displays, because it is far more complex.

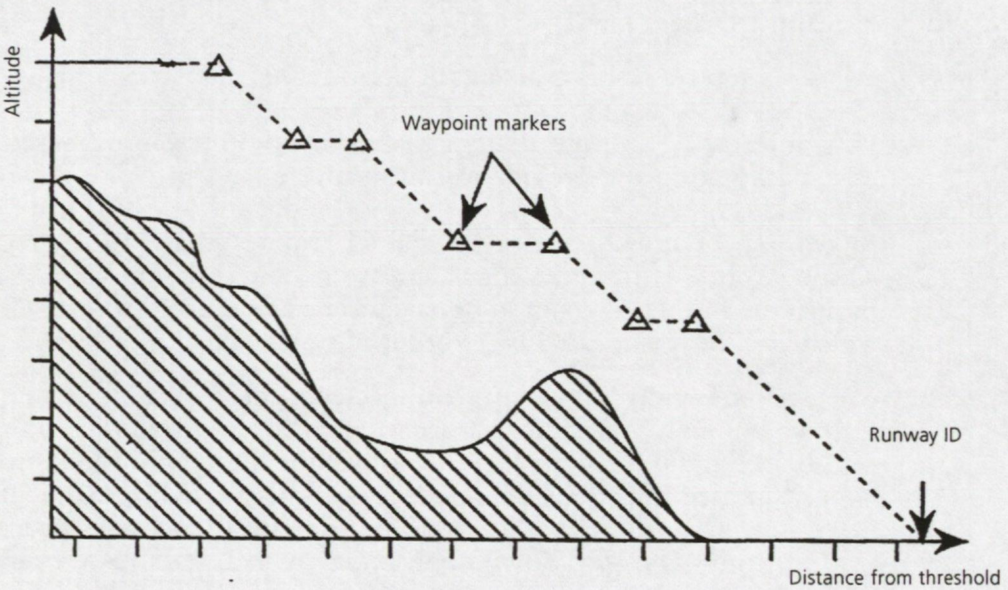

Figure 4–1 One-dimensional vertical navigation display, step-down approach

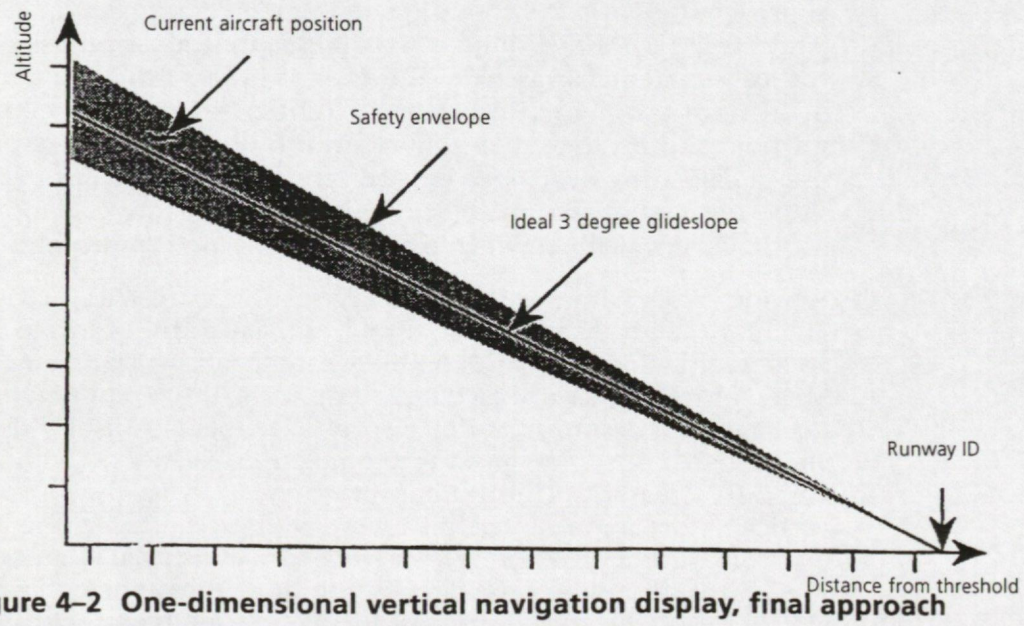

Figure 4–2 One-dimensional vertical navigation display, final approach

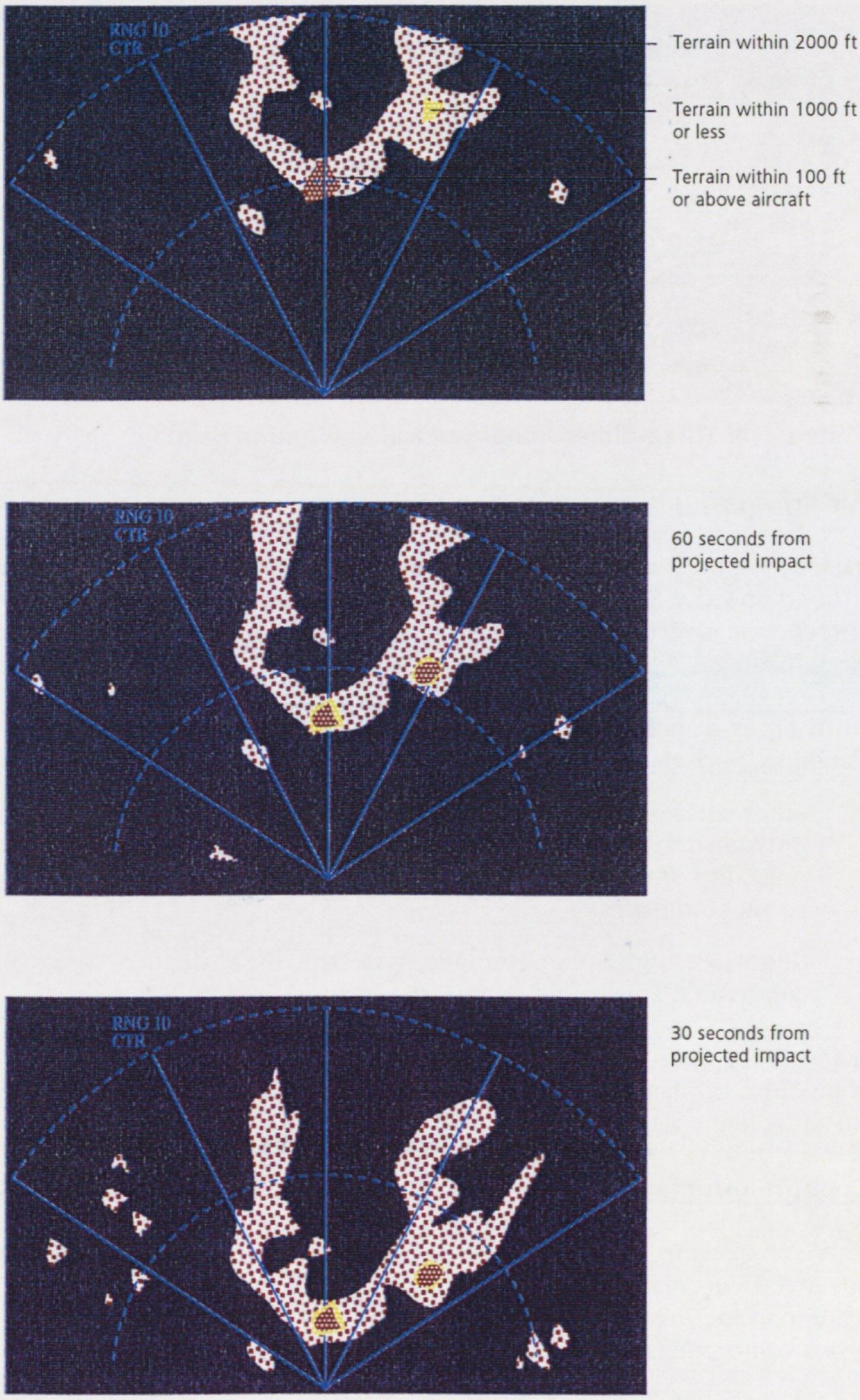

Figure 4–3 Two-dimensional vertical navigation display

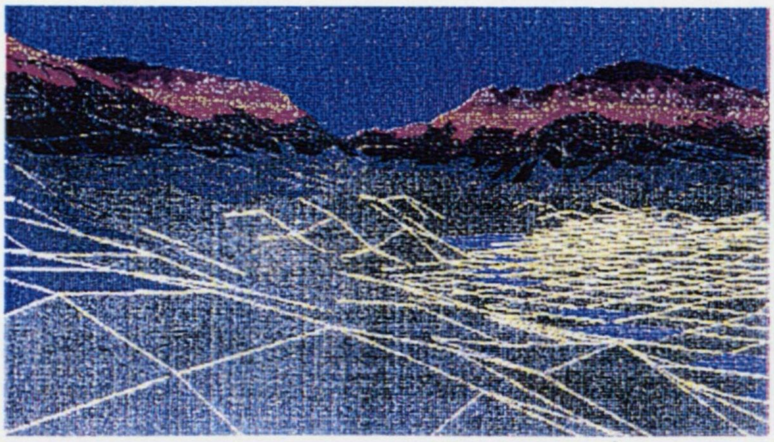

Figure 4–4 Three-dimensional vertical navigation display

4.3 Air crew/ground misunderstandings

There have been a number of accidents involving misunderstandings between the ground and the air crew. These range from misunderstandings involving ATC to the crew inadvertently setting the barometric altimeter to the incorrect ground level reading.

Both types of failing could be improved upon with the use of aircraft/ground datalinks. Such datalinks could be used to:

- Automatically provide the aircraft with meteorological/other data, which is only currently available via voice link. This would drastically increase the reliability of such data: instruments such as the barometric altimeter could be set automatically.
- Negotiate flight plan changes, with the IFPM dealing directly with ATC computers. This would remove the 'man-in-the-loop'.

If the IFPM were negotiating the aircraft's flight plan, there would have to be some form of plan-view display, so that the crew could interactively influence the resulting flight plan.

4.4 Cockpit automation

This sub-section briefly highlights some of the issues associated with using advanced automation in the cockpit, because they are of particular relevance when considering use of an Intelligent Flight Path Monitor. References 13 and 14 give a comprehensive discussion of this problem.

The degree of cockpit automation has advanced rapidly, from the simple autopilots available in the 1940s to the sophisticated systems available on today's modern aircraft (e.g. the A–320's envelope protection system means that this aircraft, even under 'manual' control, does not necessarily respond to pilot system inputs). In addition, modern pilots have access to a much wider and ever increasing range of information.

This trend towards more information, greater complexity and more automation can isolate the pilot from the vehicle and decrease awareness of the state and situation of the aircraft or system being controlled.

This can occur for a number of reasons, including information overload which can lead to attention 'channelling', when the crew's attention gets fixed on a possibly irrelevant piece of information.

A fundamental problem is that current automation systems tend to work well in ordinary situations, so that pilots become used to them and perhaps come to rely on them. A good example is the Northwest Airlines MD–80 accident in Detroit 1987 (accident 'b' in Appendix A), where the crew probably failed to run the taxi checklist which resulted in incorrect take-off configuration. The automatic configuration warner the crew were used to failed to operate.

If an extraordinary situation occurs, the pilot might be less able to handle it if used to automated equipment, because there may be less understanding on the pilot's part of what the system is doing. A typical example of this type of incident is autopilot/pilot misunderstandings.

Current cockpit automation systems do not always decrease the pilot's workload in emergency situations, and yet that is the situation in which pilots require assistance.

The installation of automated cockpit systems has reduced accident rates. However, there still might be occurrences of preventable accidents.

Such accidents might be prevented by a combination of methods, including the use of:

- **Error evident displays.** An error evident display indicates incorrect system input to the crew before it has a chance to adversely affect the aircraft. Note that this does not prevent the original error: instead, it gives the crew a chance to detect their error and remove it. The map mode of the horizontal situation indicator (HSI) or the vertical navigation display discussed in section 4.2 are excellent examples of error-evident displays.

- **Error trapping interfaces.** It should be feasible to give the cockpit interface enough intelligence to be able to detect incorrect pilot input and provide warnings as necessary. This requires the system to be able to assess the aircraft's situation, as well as or better than the pilot, since pilot inputs are obviously highly situation dependant. The advantage of such an automated 'situational assessment' system would be that it could take a more complete view of the aircraft system and (potentially) assimilate far more information, without getting 'channelled' by possibly irrelevant information. The situation assessment must include an assessment of the crew, as they are obviously the major influence on the aircraft behaviour.

- **Predictive systems.** It is not sufficient to simply alert crews when an alarm condition exists: instead, forecasting algorithms should be employed to predict trouble before alarm conditions are reached. An obvious example would be automatic fuel management taking into account the flight plan/weather conditions. Another example would be prediction of over-consumption of engine oil. Such predictive warnings are included to some extent in, for example, the Airbus' Electronic Centralised Aircraft Monitor (ECAM). This system includes a 'systems parameter trending' function, which automatically displays some system parameters when their value drifts out of normal range but well before reaching a warning level. However, this system does not have knowledge of strategic intent.

- **Intent-driven systems.** If aircraft systems have the capability of understanding pilot strategic intent, then error-trapping interfaces become more practical. For example, the pilot could inform the system of the intent 'to fly from Gatwick to Milan', and this could be used as vital input to sanity checking error traps, such as FMS entries, fuel, etc. Alternatively, an artificially intelligent system could employ intent recognition algorithms (as used in CASSY).

- **Tactical workload smoothing.** If the aircraft system is performing its own situational assessment, it should be feasible for the system to manage carefully pilot workload. This would involve the system directing crew attention to information to allow the processing of potential problems before they become emergencies.

Note that the measures described above cannot be implemented satisfactorily by fitting a 'black box' IFPM. They amount to a re-design of the entire man/machine interface, since the IFPM should control the information supplied to the crew.

4.5 User interface specification

The interface between the IFPM and the air crew needs to be designed carefully, taking into account the factors above.

It is assumed that the IFPM remains purely a monitoring information supplier and tactical workload smoother, and that control of the aircraft would remain with the crew.

The primary requirements which drive the interface specification are that the IFPM should:

(1) Not add to the workload of the crew in any way (to avoid overload), nor reduce it in normal situations (to avoid underload). Under normal flight conditions in which the crew are following procedure, the IFPM should have little or no crew interaction. Its main purpose should be to allow the crew to deal more effectively with abnormal situations.

(2) Rapidly provide a simple explanation of why an alert has been generated. (Cf experience of very early GPWS marks, which only provided a simple 'Pull up!' warning without explanation. This led to the real cause of the alert sometimes being missed by crews.)

(3) Provide more detailed information to the crew only upon request or if absolutely necessary.

(4) Provide the crew with the line-of-reasoning of the AI system in less time-critical situations (training/flight planning). This requirement means that the crew should be able to interrogate the IFPM as to why a conclusion has been reached, and the system should indicate its reasoning.

These requirements might be fulfilled with the following interface:

- The IFPM should run entirely autonomously, requiring no input from the crew for its correct operation.

- The IFPM output should be by voice, backed up by text and graphics.

- Direct IFPM input is unnecessary for correct operation. However, suitable input for requesting specific IFPM services might be via (for example) conventional input devices, touch screens, etc, in the short term and via voice commands backed up by text confirmations in the long term (cf CASSY). However, the human factors issues of using voice recognition technology in a civil cockpit would need to be investigated.
- Alerts/warnings should contain cause information.
- More detailed information should be graphically displayed either by crew command or to help explain an alert (e.g. a 2-D terrain display should only appear if the aircraft is in a hazardous situation, cf EGPWS).

4.6 Summary

This section has examined the human factors issues in connection with the use of an IFPM.

The main conclusions to be drawn are:

- Human factors research suggests that the man/machine interface used by highly automated systems needs extremely careful design, to ensure that the human operators do not become overloaded with information at critical times, and that they understand what the automation is doing. It is possible to conceive of IFPM-like designs which might be embedded into aircraft systems, greatly improving the interface.
- The direct output from the IFPM to the crew should probably be voice, backed up by text. The technology for this is readily available.
- Input to the IFPM could be by conventional means in the short term and perhaps (subject to human factors investigation and the availability of suitable technology) by voice recognition in the long term.
- The IFPM should control the aircraft's graphical displays to increase crew situational awareness as necessary. For example, in a terrain-warning situation the best display is a 2-D plan view. However, a 1-D profile may be appropriate in some circumstances.

5 IFPM DATA SOURCES AND REQUIREMENTS

5.1 Introduction

This section lists the data sources that could be used as input to an IFPM. The section concludes with an outline of the requirements that an IFPM might fulfil.

5.2 Data sources for the IFPM

Table 5–1 lists the data sources which may be of value to the IFPM. Also contained in the table are details of what information the data source provides and how the data could be accessed.

The majority of the data are available on existing aircraft databuses (ARINC 429 is assumed, which is used on all but the most modern commercial aircraft such as the B777, which uses ARINC 629).

Data on older, non-digital aircraft is likely to be significantly more difficult/expensive to acquire. It may be impractical to fit an IFPM to such aircraft, depending on functionality and aircraft specifics.

Future possible external sources are assumed to be:

- Data made available by the introduction of ground/aircraft datalinks.
- Satellite navigation aids (which also provide altitude information).

The most important internal data sources will be the terrain databases and the knowledge base.

Table 5–1 Data sources for the IFPM

Source:	Provides:	Available via:
Radio altimeter	Radio Altitude, provided the aircraft ground clearance is less than 8,000 feet	ARINC 429 ARINC 629
Barometric altimeter	Barometric Altitude, providing altitude, with frame of reference depending upon altimeter setting (QFE, QNH, QNE)	ARINC 429 ARINC 629
Navigation system	Current aircraft position, latitude and longitude (derived from INS and fixing systems)	ARINC 429 ARINC 629
GPS/ GLONASS	Current aircraft position and altitude	Dedicated link? Incorporated into ARINC?
Avionics	Control surface settings, engine status, aircraft configuration, fuel status	ARINC 429 ARINC 629
Aircraft sensors	Aircraft status information: e.g. sink rate, etc	ARINC 429
FMS/ Autopilot	Flight plan, take-off weight, autopilot settings	ARINC 429 ARINC 629 Dedicated link
Geographical database	Terrain information, ATC structure, airport/runway threshold locations	Internal to IFPM/ ELS
Knowledge base	Data on aircraft, procedures, expert knowledge	Internal to IFPM
Weather radar	Weather situation ahead of the aircraft	Weather radar databus
ATC datalink	ATC clearance negotiation, meteorological data, other data	VHF, Mode S or satcom datalink
TCAS or SSR	Proximity of other aircraft	Dedicated link
Pilot voice input	Commands to the IFPM	Voice recognition (internal to IFPM)
ILS	Course & track	ARINC 429 ARINC 629

5.3 Requirements

This subsection identifies the top-level requirements for an IFPM. Paragraphs that describe a requirement are marked with an 'R', whereas general preamble paragraphs are unmarked.

R1 A major requirement on an IFPM is that it shall provide warnings that are *timely.* Existing warning equipment, such as GPWS or TCAS provide '11th hour' warnings, which are a last resort. The IFPM shall provide warnings which give the crew time to react to the situation so far in advance that the more basic warnings are never generated: ideally, the IFPM should detect system input errors as they are entered and before they have time to affect the aircraft. A suitable warning time might be 60 seconds for a life-threatening situation. Such long-term warnings might rely on flight plan details to minimise nuisance alarms, and the system will have to continually check that a flight plan is being followed.

R2 The IFPM shall run autonomously, i.e. require no direct input from the crew in order to monitor the flight and provide warnings.

R3 The IFPM shall not add to the workload of the crew in any way.

R4 The IFPM shall direct crew attention to the most relevant information display given the aircraft status/situation.

R5 The IFPM shall, at all times, keep the 'man-in-the-loop'. Decisions (e.g. accepting new flight plans) should always rest with the pilot.

R6 Warnings and cautions given shall contain 'cause' information. In situations that are not time-critical (e.g. flight planning or verification and pilot training), the IFPM should be capable of quickly explaining the line of reasoning it is following if an alert is generated. Detailed information should be presented to crews graphically on command or if the situation demands (in e.g. a potential CFIT incident).

R7 The nuisance alarm rate for the system shall be extremely low so that crews have confidence in the system. An estimate for the required nuisance alarm rate can be obtained from the nuisance alarm rate of current GPWS equipment.

Suitable nuisance alarm rates can be estimated as follows:

A major British airline estimated that in 1993 and 1994, there was a total of 1,332 GPWS alerts on their aircraft [2]. The vast majority of the reported incidents were determined to be nuisance. During this period, the airline flew about 700,000 flights, so an estimate for the nuisance alarm rate for the GPWS equipment used is about one per 500 flights.

A reasonable requirement to place on the IFPM nuisance warning alarm rate is therefore that it should be ten times lower, at one per 5,000 flights.

A higher rate of nuisance alarms for cautions may be tolerable, if cautions are issued at a higher rate than warnings.

R8 Prioritised warnings shall be generated if:

- the aircraft is in a situation that demands a GPWS warning (as per the GPWS warning specification);

- the aircraft configuration is inappropriate for the current flight situation and the aircraft situation is critical, e.g. during take-off or landing (as per current configuration warning specification);

- the aircraft is in danger of colliding with other aircraft (from TCAS/SSR data).

R9 Prioritised cautions shall be generated if:

- the aircraft is in imminent (e.g. <60 seconds) CFIT danger;

- the flight path deviates by certain margins from the entered flight plan;

- the aircraft configuration is inappropriate for the current flight situation but less critical, e.g. during the en-route flight phase;

- the current autopilot mode is inappropriate for the current situation;

- the aircraft's current status (e.g. fuel, engine lubricant, etc) is inadequate for the entered flight plan, meteorological conditions or general aircraft situation (slow-over fault detection);

- flight plans are entered into the FMS which are not in-line with ATC structure, aircraft status, etc;

- the flight control input is inappropriate for the current aircraft situation (e.g. throttle setting not increased after levelling off after descent, or manual flight commands entered with autopilot engaged);

- checklists are not performed at appropriate times.

These cautions shall be elevated to warning status if appropriate pilot action is not taken to correct the error and the aircraft situation has become more critical.

R10 The IFPM could be used to provide advice and guidance to crews for:

- setting other cockpit systems (e.g. communications frequencies, autopilot modes);

- helping the pilot plan last-minute flight plan changes, such as alternate airports in emergency situations;

- suggesting flight plan changes to avoid weather ahead.

R11 The IFPM shall prioritise warnings, such that the most important are given first (for example ground proximity warnings should take precedence over aircraft proximity warnings).

R12 Warnings, cautions and advice shall be given to the crew verbally, with warning indicators/messages in addition.

R13 The IFPM shall provide a cost-effective solution: i.e., it must have quantifiable safety benefits which outweigh the development/production/installation costs. This may mean that an IFPM might only use existing data sources and display instruments.

A major objective for the IFPM is that it shall never miss warnings in a dangerous situation, nor should it generate false warnings.

The IFPM should be designed so that it is immune from common mode errors and data incest.

6 IFPM BASELINE DESIGN

6.1 Introduction

This section outlines a possible IFPM design. The design is modular, so that elements can be included or removed depending on the type of aircraft and operating environment in which it is flown.

The impact of new data sources and technology, along with specific instances of the design applied to different aircraft types/scenarios are discussed in section 7. The baseline design proposed is based on the requirements and data sources described in section 5.

6.2 IFPM baseline design, top-level view

Figure 6–1 shows an overall system diagram for a baseline IFPM design. Entities that perform actions/assessments are depicted as circles (for example the IFPM's flight plan sanity checker) and entities that provide data are shown in rectangles. Dynamic (time-varying) data flow is indicated by solid arrows and 'static' data flow (time invariant or very slowly varying) is indicated by dashed lines.

The design uses existing and future possible data sources for its input. The possible data sources and aircraft/IFPM interface are as per table 5–1.

Databases used are:

- a digital terrain map;
- a digital map of ATC structure (including standard navigational data);
- a database of airport/runway locations;
- a database of aircraft performance data.
- a procedural knowledge base;
- a pilot expert knowledge base.

These databases could be part of the IFPM itself or situated on a future aircraft's Electronic Library System (ELS).

The map databases could be of varying resolution, with high resolution data in the vicinity of airports and lower resolution data over sea or in regions well away from airports.

The IFPM design has three main modules:

- situation assessment;
- flight planning;
- interface.

Each of these are discussed in turn in sections 6.3, 6.4 and 6.5.

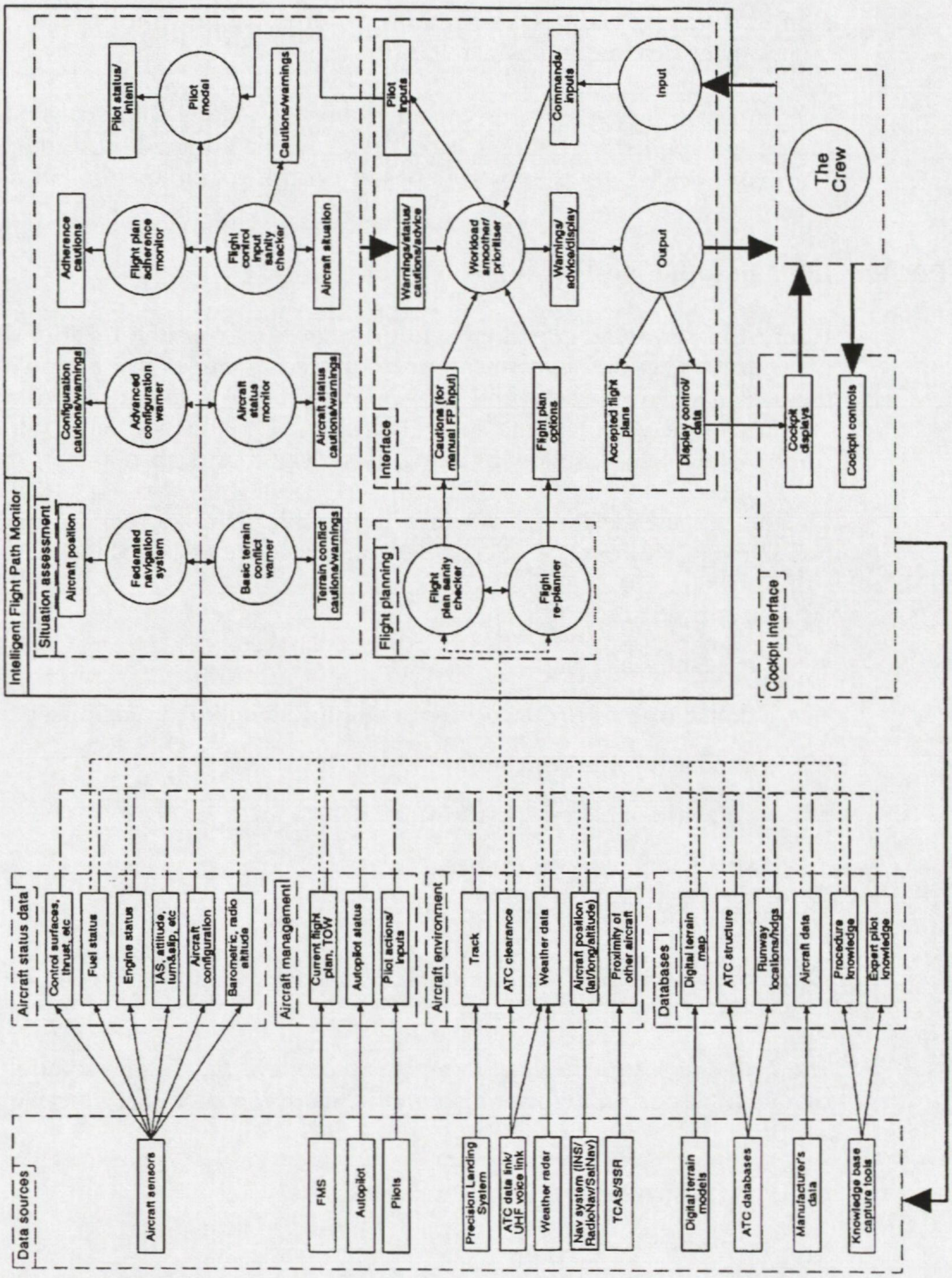

Figure 6–1 Overview of the baseline IFPM design

6.3 Situation assessment module

The situation assessment module can be broken down into the sub-elements:

- a federated navigation system;
- an advanced configuration warner;
- an aircraft status monitor;
- a basic terrain conflict warner;
- a flight plan adherence monitor;
- a flight control input sanity checker;
- a pilot model.

The sub-elements are summarised in tables 6–1 to 6–7.

Each table summarises:

- the mode of operation of the sub-element, including algorithms for alert generation where appropriate;
- the conditions under which the sub-element operates (e.g. manual flight, automatic flight, flight plan in operation and up to date);
- the specific data inputs requirement (status data, aircraft management data, environment data, databases in use);
- the technology suitable for production of the sub-element.

The list of example applications given for each sub-element (under 'Mode of operation') is not intended to be exhaustive. However, the list of data inputs is intended to be complete, but subject to revision.

Table 6–1 Federated navigation system operation summary

Federated navigation system	
Mode of operation:	
Produces a sanity-checked aircraft position (latitude, longitude, flight level, ground clearance) which is continually updated. This output is used by other sub-elements in the situation assessment module. The federated navigation system fuses the data output from existing aircraft navigation systems, and, in the future, satellite navigation systems. If the aircraft is at comparatively low altitude (below 8,000 feet above ground level) the system uses output from the radio altimeter and the corrected altitude (above sea level) to verify the aircraft's position using terrain referenced or matched navigation.	
Operating conditions:	
Always operational	
Inputs:	
Status data	barometric altitude radio altitude QNH/QFE
Aircraft management	none
Environment data	inertial navigation system output radio/satellite navigation system output
Databases	terrain database
Output to:	
Aircraft position required for all sub-elements of situation assessment module (except pilot model). Also required for flight re-planner (flight planning module).	
Suitable technology:	
Federated navigation systems are already used widely in military applications. The technology is therefore relatively mature: Kalman filtering is used for data fusion.	

Table 6–2 Advanced configuration warner operation summary

<table>
<tr><th colspan="2">Advanced configuration warner</th></tr>
<tr><td colspan="2">Mode of operation:</td></tr>
<tr><td colspan="2">For example:
Take-off configuration warning:
check aircraft configuration for take-off, including flap settings taking into consideration take-off weight, etc.
En-route:
buffet zone warning, if pilot input such as to bring aircraft near danger (using: altitude, speed, weight).
Landing configuration warning:
check aircraft configuration for landing.</td></tr>
<tr><td colspan="2">Operating conditions:</td></tr>
<tr><td colspan="2">Always operational</td></tr>
<tr><td colspan="2">Inputs:</td></tr>
<tr><td>Status data</td><td>control surfaces
flap settings
thrust settings
aircraft weight (take-off and en-route)
configuration (flaps, gear, air brakes)
altitude
speed</td></tr>
<tr><td>Aircraft management</td><td>current flight phase (inferred if manual flight)
pilot actions and status</td></tr>
<tr><td>Environment data</td><td>weather data
aircraft position</td></tr>
<tr><td>Databases</td><td>ATC structure
runway locations/headings
aircraft performance data
procedure and piloting expert knowledge
runway/airport data (e.g. runway lengths, etc)</td></tr>
<tr><td colspan="2">Output to:</td></tr>
<tr><td colspan="2">Interface module (configuration warnings and cautions).</td></tr>
<tr><td colspan="2">Suitable technology:</td></tr>
<tr><td colspan="2">Actual configuration warnings can be generated from heuristics, e.g.:
'If flight phase = preparing to take-off then check configuration is take-off'
Current flight phase could be determined by fuzzy logic, used to assess one of a number of possible alternatives, e.g. preparing for take-off, taking off, TMA after take-off, en-route, TMA prior to landing, preparing to land, landing. This would be a 'plan recognition' or 'intent recognition' system, similar to that used in ARCHIE or CASSY.
The flight phase determination would use:
a procedure/piloting expert database;
output from the pilot model;
the current active flight plan (if there is one);
aircraft position (if appropriate).
The determination would not use data from aircraft sensors other than the navigation system to determine current flight phase, to avoid common mode errors.
Once current flight phase has been determined, configuration warnings can then be generated using input from aircraft performance data, weather situation, current weight, aircraft sensors.
It is possible to determine flight phase without the use of AI (used, for example on Airbus' ECAM). This uses aircraft avionics to determine flight phase, as specified by ARINC 726. The potential difficulty with this approach is that common mode errors may occur: it is better to avoid using, e.g. simply the aircraft altitude to determine flight phase, if other independent determination is possible. However, some of the approaches used to determine flight phase by the ECAM may have application for the IFPM (particularly a non-AI system) and they should certainly be used as a basis.</td></tr>
</table>

Table 6–3 Aircraft status monitor operation summary

Aircraft status monitor	
Mode of operation:	
The aircraft status monitor is intended to provide 'predictive' status warnings. For example: Monitor fuel consumption in each engine. Check the fuel consumption/fuel remaining against the flight plan. Monitor engine lubricant consumption in each engine. Extrapolate consumption against time of flight remaining, check for conflicts. Monitor aircraft attitude, check for 'slow-over' faults. A highly advanced IFPM could also monitor instrument readouts (from video camera observing them). This could check consistency, instrumentation faults, etc. However, this possibility is left out of the design as it is felt that the necessary technology is still far from being available.	
Operating conditions:	
Manual flight	✔ (or automatic flight)
Flight plan in operation	required for long-term predictive warnings
Automatic flight	✔ (or manual flight)
Inputs:	
Status data	fuel status engine status aircraft attitude
Aircraft management	current active flight plan
Environment data	weather data
Databases	aircraft performance data procedure knowledge base
Outputs to:	
Interface module (status warnings and cautions)	
Suitable technology:	
Straight-forward mathematical algorithms can be used to give the warner a forward-looking, predictive capability, which would use traditional software development techniques. To be effective, the status warner requires information on the strategic intent of the crew, i.e. it must have access to information like time of flight remaining. This would be obtained from the flight plan (if in operation) or by intent inference information from other situation assessment sub-elements.	

Table 6–4 Basic terrain conflict warner operation summary

Basic terrain conflict warner	
Mode of operation:	
Calculates forward trajectory envelope of the aircraft 60 seconds in advance, taking into account aircraft's velocity, attitude, performance data, weather and pilot model output if included in design (this could control the 'width' of the envelope). Checks forward trajectory envelope for possible terrain conflicts, using terrain envelope modulation to reduce nuisance alerts. Conflicts cross-checked against runway threshold locations (with aircraft trajectory – i.e., does the aircraft appear to be landing at a known runway) and aircraft configuration. Caution generated if forward trajectory: directly intercepts terrain with no runway, (configuration independent); intercepts runway threshold but configuration not landing. Warning generated in accordance with: GPWS warning specification (i.e. excessive descent, terrain closure rate, descent after take-off, insufficient terrain clearance, inadvertent descent below glideslope, excessive bank angle, wind shear).	
Operating conditions:	
Always operational	
Inputs:	
Status data	aircraft velocity aircraft configuration engine status aircraft weight aircraft attitude
Aircraft management	no inputs
Aircraft environment	meteorological conditions aircraft horizontal position (lat, long) ground clearance ILS course glideslope deviation
Databases	terrain database
Outputs to:	
Interface module (terrain conflict warnings)	
Suitable technology:	
The technology required for this sub-element is already well developed, for example within EGPWS. It could use conventional software development techniques.	

Table 6–5 Flight plan adherence monitor operation summary

Flight plan adherence monitor	
Mode of operation:	
This function checks that the current flight plan is adhered to. It operates under manual flight. (Assumption: flight plan is at all times adhered to by autopilot if aircraft status and flight control input OK (e.g. correct autopilot mode), both of these checked by other IFPM sub-elements.) The aircraft's forward trajectory (based on aircraft's velocity, performance data and pilot input) is compared against the flight plan. If deviations larger than a certain threshold are detected, a caution is generated.	
Operating conditions:	
Manual flight	✔
Flight plan in operation	✔
Automatic flight	✖
Inputs:	
Status data	aircraft velocity engine status aircraft weight altitude
Aircraft management	pilot status (from pilot model) current (sanity checked) active flight plan pilot flight control inputs
Environment data	none
Databases	aircraft performance data procedure knowledge base expert pilot knowledge base
Outputs to:	
Interface module (deviation from flight plan cautions)	
Suitable technology:	
The cautions can easily be generated from conventional software.	

Table 6–6 Flight control input sanity checking operation summary

<table>
<tr><th colspan="2">Flight control input sanity checking</th></tr>
<tr><td colspan="2">Mode of operation:</td></tr>
<tr><td colspan="2">Error trapping function.

The function sanity-checks pilot system inputs, before they have time to adversely affect the aircraft's situation. This does not mean that flight control inputs will be buffered to allow assessment of their impact. Instead, the aim would be to trap erroneous input that has a long-term effect on the aircraft (for example, checking that autopilot mode is appropriate for the aircraft situation, and other examples outlined below).

The function also checks for lack of appropriate pilot input.

To carry out this task, the flight input sanity checker sub-element must carry out a situational assessment for the aircraft. This situational assessment output would form the core of determining if flight control input is appropriate.

For example, check that:

checklists are performed at the appropriate time and caution pilots if they are not;

pilot actions are such as to maintain an adequate level of aircraft kinetic energy when levelling off after descent (manual flight);

the autopilot mode is appropriate for the flight situation;

the pilot does not manually input flight controls inappropriately with the autopilot engaged.

The key to the success of a fully-functional IFPM would be in the ability of this sub-element to perform autonomously a situational assessment which is as complete or better than an alert pilot can perform, by continually considering a broad range of input information.</td></tr>
<tr><td colspan="2">Operating conditions:</td></tr>
<tr><td colspan="2">Always operational</td></tr>
<tr><td colspan="2">Inputs:</td></tr>
<tr><td>Status data</td><td>general aircraft status data required</td></tr>
<tr><td>Aircraft management</td><td>current flight pla
autopilot mode
pilot actions/inputs</td></tr>
<tr><td>Environment data</td><td>weather
ATC clearance
other aircraft proximity
aircraft position</td></tr>
<tr><td>Databases</td><td>ATC structure
runway locations
procedure knowledge base
expert pilot knowledge base</td></tr>
<tr><td colspan="2">Outputs to:</td></tr>
<tr><td colspan="2">Interface module (cautions/warnings/advice/aircraft situation)</td></tr>
<tr><td colspan="2">Suitable technology:</td></tr>
<tr><td colspan="2">A combination of heuristics (for knowledge application using the KBS) and fuzzy logic could be used for the situation assessment.

Heuristics can be used on the output of the situation assessment module to produce cautions/warnings, for example:

'If aircraft situation = levelled off after descent and throttle setting = idle then caution pilot.'</td></tr>
</table>

Table 6–7 Pilot model operation summary

Pilot model	
Mode of operation:	
The pilot model is primarily aimed at assessing pilot status (e.g. current workload for pilot/copilot, current pilot/copilot activity). The output of this modelling is used as input to other warning/cautioning sub-elements to determine the appropriate level of warning. It is also output to the interface module to determine the appropriate level of interaction and communication between the IFPM and the pilots.	
Operating conditions:	
Always operational	
Inputs:	
Status data	none
Aircraft management	pilot actions/inputs
Environment data	none
Databases	expert pilot knowledge base
Outputs to:	
Other sub-elements in the situation assessment module (pilot status). Interface module.	
Suitable technology:	
Heuristics could be used to assess pilot behaviour. Neural networks might perhaps be required to model differences and variations between different individual pilots and copilots, using a 'training' mode for initialisation.	

6.4 Flight planning module

The flight planning module is broken down into two sub-elements:

- a flight plan sanity checker;
- an automatic flight re-planner.

These two sub-elements are summarised in tables 6–8 and 6–9.

Table 6–8 Flight plan sanity checker operation summary

Flight plan sanity checker	
Mode of operation:	
Error trapping function. Checks the flight plan within the FMS as it is manually entered or changed. The sanity-checks consist of examining the flight plan for conflicts with terrain/airspace structure, checking there is enough fuel to execute the flight plan given meteorological/aircraft status data and ensuring that the plan ends at a known runway location with the correct heading. Also sanity-checks the automatically generated flight plans from the other sub-element within the flight planning module.	
Operating conditions:	
Manual flight	✔ (or automatic flight)
Flight plan in operation	✔ (required)
Automatic flight	✔ (or manual flight)
Inputs:	
Status data	fuel status engine status
Aircraft management	current active flight plan
Environment data	weather data ATC clearance
Databases	ATC structure database digital terrain map airport locations aircraft performance data procedure knowledge base
Outputs to:	
Interface module Automatic flight re-planner sub-element	
Suitable technology:	
Cautions can be generated using conventional software techniques.	

Table 6–9 Automatic flight re-planner operation summary

Automatic flight re-planner	
Mode of operation:	
The automatic flight re-planner continuously (regardless of aircraft status) updates three extra alternative flight plans (other than the current active flight plan). The alternative flight plans are shortest-distance routes to alternative airports or missed approach/circuit plans via ATC structure, in case of emergency (e.g. engine failure). The flight re-planner can also update the current flight plan to account for changes in ATC clearance or weather. The flight re-planner can also re-plan at the command of the crew, e.g. to a different requested destination.	
Operating conditions:	
Manual flight	✔ (or automatic flight)
Flight plan in operation	✔(required)
Automatic flight	✔(or manual flight)
Inputs:	
Status data	fuel status engine status
Aircraft management	current active flight plan
Environment data	weather ATC clearance current aircraft position
Databases	ATC structure airport locations aircraft performance data procedure knowledge base
Outputs to:	
Interface module. Flight plan sanity checker (to check that generated flight plans are consistent with current aircraft status).	
Suitable technology:	
Automatic flight plans can be generated using conventional software techniques.	

6.5 Interface module

The interface module consists of three sub-elements:

- a pilot workload smoother/task prioritiser;
- an output device (to handle direct IFPM output to the crew);
- an input device (to handle direct IFPM input from the crew).

Tables 6–10 to 6–12 provide summaries of the sub-elements.

Table 6–10 Pilot workload smoother and prioritiser operation summary

Pilot workload smoother and task prioritiser
Mode of operation:
The function ensures the crew are presented with as smooth a workload as possible. Cautions and warnings are prioritised in accordance with established practice, e.g. aircraft fire less important than close proximity of terrain. The function also ensures crew attention is drawn to the most important information, given the output of the situational assessment module.
Operating conditions:
Always operational
Inputs:
Processes the output of the situational assessment module (cautions, warnings, advice, pilot status). Pilot voice commands via the voice recognition system (if applicable).
Outputs:
To the voice synthesiser and cockpit displays.
Suitable technology:
The prioritiser algorithms could use heuristics and fuzzy logic to assess the most important information to display. Pilot workload smoothing would be achieved primarily by the IFPM offering pilots automatic services (for example, automatic flight re-planning) in times of high workload. Assessment of the requirement for such services could be based on simple heuristics.

Table 6–11 Output operation summary

Output
Mode of operation:
Controls both the direct and indirect IFPM output to the crew. Direct output could be by synthesised voice, backed up by text displayed on the EFIS. The tone of voice could be altered according to the situation (e.g. urgent warnings could use a different tone). Indirect output could be e.g. what is displayed on the EFIS (e.g. change mode from Horizontal Situation Indication to Vertical Situation Indication in a potential CFIT incident).
Operating conditions:
Always operational
Inputs:
Warnings/cautions/advice from the workload smoother/prioritiser sub-element.
Outputs:
Graphical displays, voice output, text output.
Suitable technology:
Voice synthesis technology is mature and already in use in modern cockpits.

Table 6–12 Input operation summary

Input
Mode of operation:
Handles the direct crew input to the IFPM. This could either be manual input (e.g. touch screens) or voice command input. If voice recognition is used, could interpret pilot voice communications (e.g. inter-crew communications, or crew to ATC) to gain extra situation information.
Operating conditions:
Always operational.
Inputs:
Pilot/copilot voice inputs, manually input commands.
Outputs:
Interpreted commands to workload smoother/prioritiser.
Suitable technology:
Touch-screen or simpler input devices could be used as back-ups to the primary input method, voice. Voice recognition systems for safety critical applications are still in their infancy. The situation can be improved through the use of context-sensitive prioritisation of recognised vocabulary, where the context used is dependent on the aircraft situation. This operates by placing most likely phrases for a given situation at the top of the voice recognition system's search. This allows faster recognition, without limiting the vocabulary of the recognition system. It is assumed that reliable voice recognition technology will be available in a time-frame of 5–10 years.

6.6 Summary

This section has examined a baseline IFPM design. The design illustrates what could be achieved, with a 'wish-list' of IFPM functionality. Table 6–13 summarises the identified IFPM functions.

Table 6–13 IFPM functions (summary)

IFPM function	Summary
Federated navigation system	Sanity-checks aircraft nav systems output
Advanced configuration warner	Infers flight phase, checks aircraft configuration is appropriate
Aircraft status monitor	Provides predictive status warnings based on strategic intent of crew
Basic terrain conflict warner	Forward-looking terrain conflict device, based on terrain database
Flight plan adherence monitor	Checks flight plan is followed (if appropriate)
Flight control input sanity checking	Autonomous aircraft situational assessment performed Traps erroneous or lack of flight control input
Flight plan sanity checker	Traps erroneous flight plan input
Automatic flight re-planner	Reduces pilot workload in emergency situation
Pilot workload smoother and task prioritiser	Smooths pilot workload, prioritises tasks based on situational assessment
Pilot modelling	Assesses pilot status

More detailed consideration of the practicality of the design for different aircraft types/scenarios is described in section 7.

7 IFPM SYSTEMS FOR DIFFERENT AIRCRAFT AND SCENARIOS

7.1 Introduction

Section 6 presented a baseline IFPM design, in which every desirable, safety-increasing function is included for completeness. This section looks at how this functional design gets modified for fits to different aircraft types, operating in different scenarios.

This section starts with a review of future possible data sources and technologies relevant to the IFPM and the impact they might have on its design (section 7.2). This review is included because it impacts greatly on the feasibility of an IFPM design for a given time frame and aircraft type.

Two instances of IFPM design are then considered:

- A design suitable for retro-fit to an existing aircraft, using existing data sources and technologies (section 7.3);
- A design suitable for future aircraft, using future data sources and technologies (section 7.4);

Section 7.5 summarises and compares the designs.

All the designs considered are for large commercial transports. The main difference in a design for commuter aircraft will be in terms of acceptable cost, since (at least, in principle) the requirements and data sources remain the same. Cost (along with risk) of the various options is discussed in section 8.

7.2 Impact of future possible data sources and technologies

7.2.1 *Data sources*

The main assumptions about possible future data sources are:

- An aircraft/ground datalink will be used as ATC equipment is upgraded.
- Satellite navigation aids will become reliable enough for use in non-control applications such as the IFPM.

  These additional data sources will impact on the design in the following manner:

- Use of an ATC datalink greatly enhances the possible capabilities of an IFPM, since it allows ATC clearance data into the system far more easily. For example, CASSY (as it is currently designed) accesses ATC clearance data by interrupted pilot call-backs. This method is clearly prone to error and would be a weak link in the data chain for an IFPM. Implementation of ATC datalink would therefore improve the following functions:
  - The flight control input sanity checker requires ATC clearance data in order to be fully operational. However, it would still be possible to offer limited functionality without ATC information.
  - The flight plan sanity checker requires ATC clearance data, to check for compliance with clearance. Without ATC clearance data, it is only possible to check against known ATC structure.

- The automatic flight re-planner requires ATC clearance data to produce a flight plan with clearance. Flight plan options can still be generated without ATC clearance data, but the crew then have to obtain clearance.

- The ATC datalink could allow the IFPM to be part of the flight plan negotiation loop that may exist in future ATC scenarios. For example, the automatic flight re-planner could present the crew with flight plan options. The crew-selected option could then be negotiated by the IFPM with the ground ATC system.

- A ground centre can provide more detailed information over a datalink to the aircraft than is currently available, such as airport status information and detailed meteorological information. This ground centre might be an air traffic control centre, flow management unit or an airline operations centre. This information would be used by the following sub-elements:

  - The advanced configuration warner could use weather data (for example, runway surface moisture) as input to configuration warnings. However, less detailed configuration warning is possible without such data.

  - The aircraft status monitor could use weather data (for example, wind speed and direction over the remaining journey, weather conditions such as de-icing required) to predict more accurately fuel burn for the remaining journey. The function will operate without such data, albeit less accurately.

  - The basic terrain conflict warner could use meteorological conditions to provide more accurate prediction of forward trajectory.

  - The flight control input sanity checker could use weather data as part input to its sanity checks.

  - The flight plan sanity checker could use weather data as input to flight plan checks.

  - The automatic flight re-planner could use airport status information and meteorological data. Automatic flight plans could be generated without such data, however more useful plans would be generated with it.

  Many of the IFPM functions would therefore be greatly improved if given access to detailed meteorological conditions: however, they would all still function to a lesser extent without such data.

- Use of satellite navigation systems should greatly improve the reliability of position determination (including altitude). This would be used as part input to the federated navigation system.

7.2.2 *Technologies*

Technologies not yet mature enough for use in safety-critical applications, but which would be required for some of the IFPM functions are:

- Artificial Intelligence (AI) systems, for example Knowledge Based Systems (KBSs).

- Voice recognition technology.

These technologies impact on the design in the following way:

- AI technology is required for the following IFPM functions:
  - The advanced configuration warner would use a neuro-fuzzy system to autonomously assess flight phase and recognise pilot intent.
  - The aircraft status monitor needs access to the strategic intent of the crew. This only requires AI for the autonomous strategic intent recognition. An interface could be defined for manual input of this information, negating the requirement for AI in this function.
  - The flight control input sanity checker requires a neuro-fuzzy system to perform autonomous situation assessment.
  - The pilot model requires a knowledge-based expert system to assess pilot behaviour. It might also use neural networks to model differences between pilots.
  - The pilot workload smoother and task prioritiser would use a neuro-fuzzy system to assess the highest priority task.
- Using voice recognition would enhance the IFPM's capabilities, for example:
  - The IFPM's pilot model could interpret pilot voice communications as part of its input.
  - Direct input to the IFPM by voice (backed up by text confirmations) could result in a smoother crew workload, since it might make it far easier for the crew to enter direct commands. However, the use of voice recognition technology in a commercial aircraft cockpit would need careful human factors investigation.

7.3 Design for retro-fit to existing aircraft

Figure 7-1 shows an architecture diagram for an IFPM which could be retro-fitted to existing aircraft. It uses only existing technology, and therefore the design does not make use of artificial intelligence, voice recognition, ATC datalink or satellite navigation.

The figure shows how the IFPM interfaces with existing aircraft systems. Warning devices such as the wind shear detector or GPWS are not necessarily replaced by the IFPM, instead outputs from these devices are fed in.

The internal databases used by the device do not include procedure and expert pilot knowledge. These databases would only be included in a device using AI software techniques. However, knowledge on operating procedures and piloting techniques is implicitly included in the design, in that it would be used to define the functionality of the module sub-element software. This is the way in which such 'knowledge' has traditionally been included in aircraft software.

The design shown is aimed at providing three top-level functions:

- **Fusion of the data from existing aircraft systems.** This allows the IFPM to take into account the entire aircraft situation, so that it can prioritise warnings and draw the crew's attention to the most important and relevant information. This should be possible (at least to some extent) using conventional software techniques.

- **Assisting in flight planning.** This should reduce workload in emergency situations (e.g. engine failure or other such emergency). One criticism of current automatic systems is they operate well in normal situations but fail to cope with abnormal situations.
- **Increasing crew's aircraft situational awareness.** Crew situational awareness can be increased by the IFPM providing the crew with context-sensitive, prioritised displays. For example, if the aircraft is potentially at risk from CFIT, the IFPM can display some sort of vertical navigation display (as discussed in section 4).

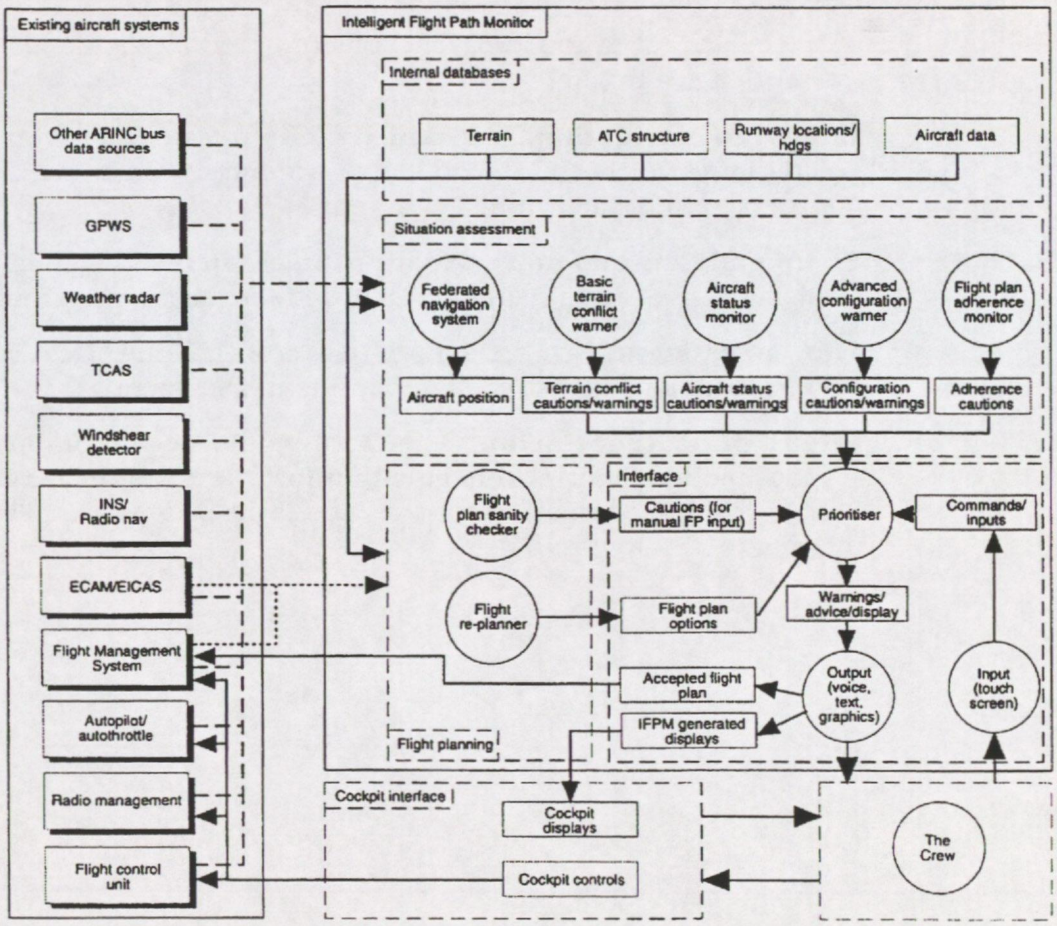

Figure 7–1 IFPM architecture for retro-fit to existing architecture

The design shown in figure 7–1 would be more than a 'black-box' add on, since it would make use of existing displays (for example, to increase situational awareness). However, it would not require any new devices to be fitted: it would obtain all its data from existing sources.

7.4 Design for future aircraft, with future technology

Figure 7–2 shows an architecture diagram for an IFPM suitable for new (yet to be designed) aircraft using new technologies. It is a fully-functional instance of the functional design shown in figure 6–1. It shows how the design might fit in with other aircraft systems.

Inclusion of an IFPM into a new aircraft design would amount to a re-design of the cockpit interface. The IFPM sits between the crew and the automated aircraft systems, and controls the 'human-centred' interface. Thus, if the situation demands, the IFPM controls the cockpit displays.

The additional/improved top-level functions provided by the design (compared with the retro-fit design) are:

- **Improved navigational reliability.** Use of satellite navigation would greatly improve the IFPM's ability to produce a sanity checked aircraft horizontal position and ground clearance.
- **Completely autonomous situation assessment.** This is achieved both through the use of artificially intelligent software and the air/ground datalink.
- **Pilot assessment.** New technology (e.g. artificially intelligent software and voice recognition) allows access to pilot status and intent.
- **Flight plan negotiation.** The IFPM would be the on-board system responsible for flight plan negotiation in future possible ATC scenarios. Responsibility for acceptance of a revised flight plan would still reside with the crew.

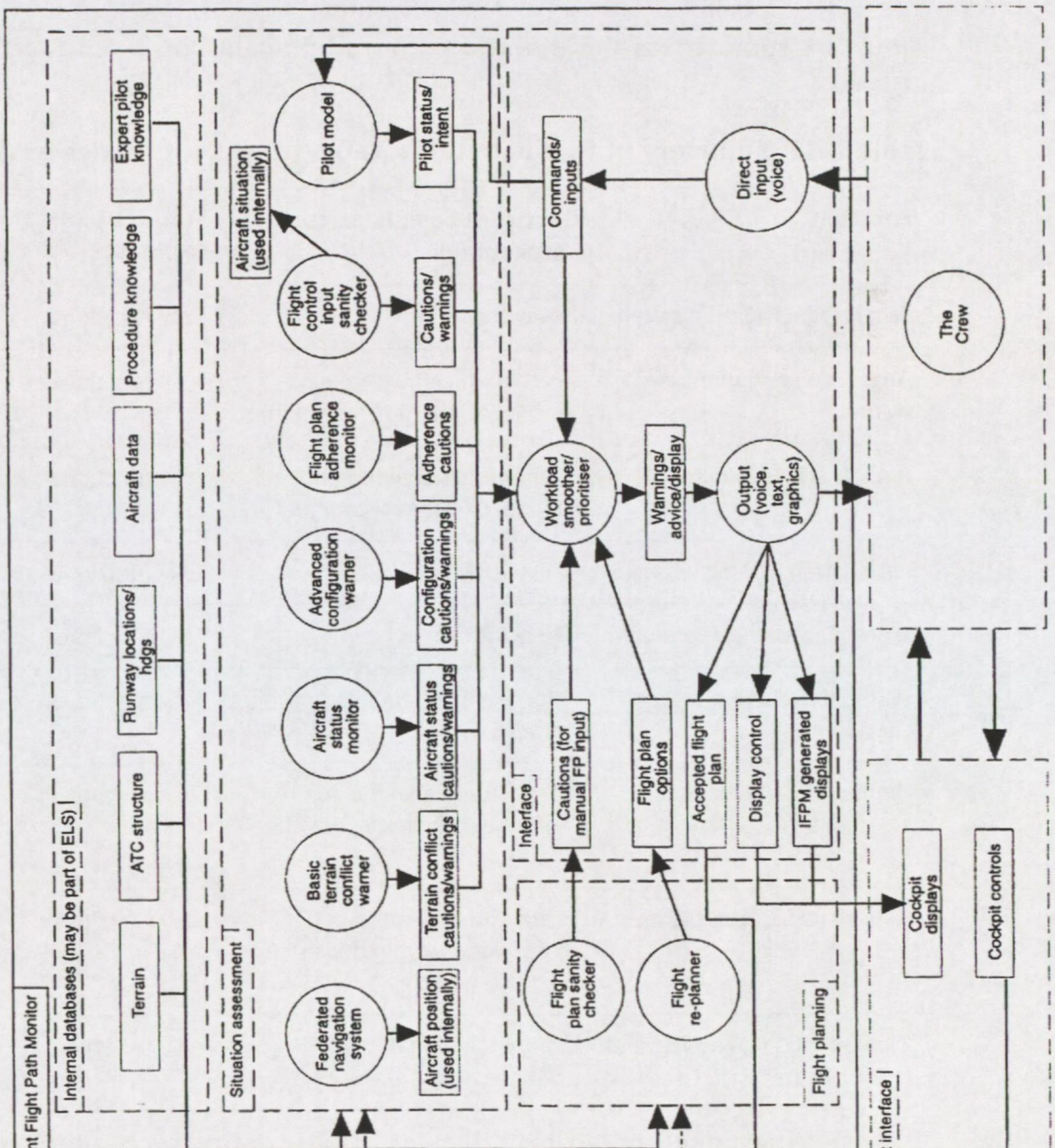

Figure 7–2 IFPM architecture for future aircraft using future technology

7.5 Comparison and summary

Table 7–1 summarises the differences in functionality between the two design instances.

Table 7–1 Summary of functionalities (retro-fit and future designs)

Function	Retro-fit design, existing technology	Future design, future technology
Federated navigation system	Fully functional	Fully functional
Advanced configuration warner	Partly functional (no pilot model or intent recognition)	Fully functional
Aircraft status monitor	Partly functional (no pilot model or intent recognition)	Fully functional
Basic terrain conflict warner	Fully functional	Fully functional
Flight plan adherence monitor	Fully functional	Fully functional
Flight control input sanity checking	Not feasible (requires AI + pilot model)	Fully functional
Flight plan sanity checker	Partly functional (no ATC information, limited weather data)	Fully functional
Automatic flight re-planner	Partly functional (no ATC information, limited weather data)	Fully functional
Pilot workload smoother and task prioritiser	Partly functional (task prioritisation possible)	Fully functional

It is true that much could be achieved using existing technology to improve effectively the man/machine interface in modern, highly automated aircraft, resulting in increased pilot situational awareness. This is reflected in the functionality of the retro fit design. However, this design has limitations and weaknesses, mainly introduced by:

- the lack of verifiable ATC clearance information onboard the aircraft;
- the complexity of assessing aircraft situation from the myriad of alternatives using existing software techniques;
- the doubt as to whether aircraft situation can be properly and reliably assessed autonomously without access to pilot voice information (via voice recognition technology). Autonomous operation is essential if the IFPM is to succeed in smoothing pilot workload.

These difficulties could all be overcome through the introduction of new data sources and technologies, as discussed in this section.

The costs, risks and timings associated with producing an IFPM are discussed in section 8.

8 COSTS, RISKS AND TIMINGS

8.1 Introduction

This section looks at the costs, risks and development/implementation time scales associated with production of an IFPM.

Section 8.2 estimates the failure condition categorisation for each of the IFPM sub-elements, and hence derives software levels. Failure condition categorisation is a measure of how important the software system is to flight safety. This has a crucial bearing on the development costs, the risks associated with development, and the time scales on which the software can be produced.

Section 8.3 estimates rough costs for producing each of the IFPM sub-elements, and states the risks involved. A summary is provided, presenting total system costs/risks for the two design instances considered in section 7 (retro-fit to current aircraft design and design for future aircraft).

Section 8.4 estimates development/production/implementation/certification time scales.

Section 8.5 summarises the main results of the section.

8.2 Software categorisation

Guidance for determining the certification aspects of software are described in the Joint Aviation Authorities AMJ 25-1309. Software systems are categorised according to the effect their failure has on aircraft safety. These failure conditions are:

A **Catastrophic.** Failure would prevent continued safe flight.

B **Hazardous.** Failure would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions, to the extent that there would be:

- A large reduction in safety margins or functional capabilities.
- Physical distress or higher workload such that the flight crew could not be relied upon to perform their tasks.
- Adverse effects on occupants including serious injury.

C **Major.** Failure would reduce the capability of the aircraft or the ability of the crew to cope with adverse conditions, to the extent that there would be:

- A significant reduction in safety margins or functional capabilities.
- A significant increase in crew workload or conditions impairing crew efficiency.
- Discomfort to the occupants, possibly including injuries.

D **Minor.** Failure would not significantly reduce flight safety and would involve crew actions that are well within their capabilities.

E **No effect.** Failure would not affect the operational capability of the aircraft or increase pilot workload.

The software development cycle which must be followed (to enable safety certification) depends critically on which of these categories contains the system.

For example, if the software system is in category A then the software might be developed according to the 'multiple-version dissimilar software' approach. This design strategy means that two or more components of the software are developed independently in a way that avoids sources of common error between components. All versions of the software are then run in the system independently from each other. This independence is obtained by partitioning the system running the software. Partitioning provides isolation between software components to contain and/or isolate faults and potentially reduce the effort of the software verification process.

By contrast, software that falls into category E can be developed along very loose guidelines. It is sufficient for this software to simply meet its functional specification.

As a rough guide, it might cost 10 times as much to produce software (of identical complexity) for a category A system as for a category D system. This is simply due to the extra overhead incurred in producing the exhaustive verification and validation procedures required for the category A system, as compared with the category D system. For cost estimates, a linear extrapolation between the two cases will be assumed, so that level B software is 7 times more expensive than level D software, and level C software is 3 times more expensive than level D software.

Software for systems in categories A to D must in any case comply with strict quality assurance procedures. This is a potential problem for AI software: these procedures are still being defined. This is a major element of risk in IFPM development, and is discussed in 8.3.

Table 8–1 shows the estimated category for each of the IFPM sub-elements, together with a rationale for placing them in that category.

Table 8–1 Estimated failure condition categories for the IFPM sub-elements

Sub-element	Category	Rationale
Federated navigation system	C	Position output is used as advisory to generate ground proximity and other warnings. Incorrect determination of position would probably result in false alarms at highly inappropriate times, which could cause a significant increase in crew workload. However, system already has a degree of redundancy (e.g. INS/radio nav, TRN in addition) so a fail-safe system should be relatively easy to implement.
Advanced configuration warner	B	Incorrect configuration warnings during take-off or landing phases are highly undesirable, as they would increase crew workload. False configuration warnings, if generated, are more likely during these phases.
Aircraft status monitor	C	False aircraft status warnings would increase crew workload. However, the problem is less severe than for configuration warnings.
Basic terrain conflict warner	C	False terrain conflict warnings are likely to occur in TMA, when the workload is already high.
Flight plan adherence monitor	D	Lack of flight plan adherence does not necessarily compromise flight safety. Warnings are only advisory.
Flight control input sanity checking	C	False flight control input sanity checks could result in perfectly valid and safe input being questioned. This would increase pilot workload and may directly compromise flight safety.
Pilot model	D	Output only used as advisory to other IFPM sub-elements.
Flight plan sanity checker	D	Entry of flight plans incorrectly would not significantly reduce flight safety. At worse, it would increase crew workload slightly or cause inconvenience to passengers (e.g. delays).
Automatic flight re-planner	D	Incorrect automatic generation of flight plans would not significantly reduce flight safety. At worse, it would increase crew workload slightly.
Pilot workload smoother and task prioritiser	B	Directing crew attention to irrelevant information could compromise flight safety. Incorrect operation of the workload smoother could result in increased crew workload.
Output	B	Incorrect display (e.g. of terrain) could compromise flight safety.
Input	D	Direct input to the IFPM not safety-critical, as should be designed to operate without any input.

8.3 Costs and risks

This subsection provides estimates for the cost/risks associated with the development of each IFPM sub-element.

If substantial hardware is required for the sub-element, a cost estimate (per unit) is also provided.

Where appropriate, effort required to produce software modules is estimated from CASSY module development time. CASSY has three modules. Each has taken about 5 man years of effort to develop. However, software was not developed according to strict QA procedures: the software level associated with these modules is probably not even D. For estimation purposes, it is assumed that a CASSY module could be developed in 10 man years to level D.

As a rough guideline, a cost of £100k is assigned to each man-year of effort.

The risk estimate is based on:

- Does the software require new technology for its operation? If it does, it places the software in the medium to high risk category, depending on how near the technology is to being exploitable at present.
- Are similar software systems already available? If so, this places the software in the low risk category.

Table 8–2 Federated navigation system development cost/risk

Federated navigation system	
Hardware:	
Special requirements:	Requires terrain database hardware.
Cost:	GMAv estimate cost at £15k for database hardware.
Software development:	
Effort:	10 man years. Majority of effort would be in obtaining terrain database and validating modified versions of military systems.
Adjust according to level: (C)	30 man years
Estimated development cost:	£3M
Risk:	Medium. Federated navigation systems and TRN systems already developed for military applications. Major risk would be in obtaining terrain database with sufficient detail to allow TRN. Problems then in certifying database. Application could obtain special dispensation, since TRN output would be advisory only.

Table 8–3 Advanced configuration warner development cost/risk

Advanced configuration warner	
Hardware:	
Special requirements:	None. ARCHIE has demonstrated a kernel system operating on a PC.
Cost:	– (Probably insignificant cf software)
Software development:	
Effort:	10 man years
Adjust according to level: (B)	70 man years
Estimated development cost:	£7M
Risk:	Medium. Largest risk is associated with development of the AI system required for autonomous assessment of aircraft phase/situation. It is the certification of such a system that presents the difficulty.

Table 8–4 Aircraft status monitor development cost/risk

Aircraft status monitor	
Hardware:	
Special requirements:	None. Algorithms to provide predictive status warnings are fairly simple.
Cost:	– (Probably insignificant cf software)
Software development:	
Effort:	5 man years
Adjust according to level: (C)	15 man years
Estimated development cost:	£1.5M
Risk:	Low to medium. Risk element is in obtaining strategic intent of crew. However, this information is already becoming available from the FMS in modern aircraft (e.g. B757 has strategic intent information relating to fuel management, which is used to perform a consistency check between the departure point, destination and fuel load and the MD–11 also attempts to infer the intentions of the pilots under certain flight regimes). Alternatively, it should be possible to infer strategic intent from flight plan.

Table 8–5 Basic terrain conflict warner development cost/risk

Basic terrain conflict warner	
Hardware:	
Special requirements:	Requires reduced-resolution (cf TRN system) terrain database. However, the database needs to be certified.
Cost:	EGPWS system: a leading manufacturer estimate unit cost of $54,000 US. Hardware cost must only be a small proportion of that, and hardware requirements for this sub-element very similar.
Software development:	
Effort:	None. Already developed.
Adjust according to level: (C)	–
Estimated development cost:	–
Risk:	Low. Required technology already under development (GCAS) and in some instances available off-the-shelf (EGPWS).

Table 8–6 Flight plan adherence monitor development cost/risk

Flight plan adherence monitor	
Hardware:	
Special requirements:	None. Adherence algorithms are relatively simple and require no special hardware.
Cost:	– (Probably insignificant cf software)
Software development:	
Effort:	5 man years
Adjust according to level: (D)	5 man years
Estimated development cost:	£0.5M
Risk:	Low. Flight plan adherence software already developed for other applications (eg CASSY). This software would merely need re-constructing according to accepted QA procedures for this software level.

Table 8–7 Flight control input sanity checker development cost/risk

Flight control input sanity checker	
Hardware:	
Special requirements:	Must perform real-time autonomous situation assessment. Real-time AI systems are only just becoming viable with the latest processor technology.
Cost:	Unknown, but maybe insignificant cf software costs. For example, even a state-of-the-art workstation costs around £20k.
Software development:	
Effort:	20 man years
Adjust according to level: (C)	60 man years
Estimated development cost:	£6M
Risk:	High. Requires complex AI system for its full operation, which carries with it a certification risk. Best approach would be to develop previous software, for example similar in operation to CASSY.

Table 8–8 Pilot model development cost/risk

Pilot model	
Hardware:	
Special requirements:	High processing power required, since complex AI system.
Cost:	Unknown, but maybe insignificant cf software costs.
Software development:	
Effort:	10 man years
Adjust according to level: (D)	10 man years
Estimated development cost:	£1M
Risk:	High. Requires complex AI system for its full operation, which carries with it a certification risk. Best approach would be to develop previous software, for example similar in operation to CASSY.

Table 8–9 Flight plan sanity checker development cost/risk

Flight plan sanity checker	
Hardware:	
Special requirements:	Requires database with ATC structure, runway locations, etc. However, this is already available within existing modern aircraft cockpit system.
Cost:	–
Software development:	
Effort:	5 man years
Adjust according to level: (D)	5 man years
Estimated development cost:	£0.5M
Risk:	Low. Does not require AI and can be based on existing systems.

Table 8-10 Automatic flight re-planner development cost/risk

Automatic flight re-planner	
Hardware:	
Special requirements:	Same as flight plan sanity checker.
Cost:	–
Software development:	
Effort:	10 man years. More complex than flight plan sanity checker.
Adjust according to level: (D)	10 man years
Estimated development cost:	£1M
Risk:	Low. Does not require AI, and is under development with existing systems (e.g. FINDER).

Table 8–11 Pilot workload smoother and task prioritiser development cost/risk

Pilot workload smoother and task prioritiser	
Hardware:	
Special requirements:	Non-AI version (e.g. for retro-fit design) might have no special requirement. AI version might require significant processing power.
Cost:	–
Software development:	
Effort:	10 man years
Adjust according to level: (B)	70 man years
Estimated development cost:	£7M
Risk:	Medium. Software controls IFPM outputs, and is therefore critical to correct operation.

Table 8–12 Output sub-element development cost/risk

Output	
Hardware:	
Special requirements:	Voice synthesisers cheap and readily available. Existing aircraft displays can be utilised, controlled via standard data buses (e.g. Weather radar display on non-EFIS aircraft or on navigation display via ARINC 453 data bus).
Cost:	Aircraft dependent. Glass cockpit aircraft display modification is typically three times more expensive than 'classic' aircraft displays, mainly due to the effort required in validating software changes to the display symbol generators.
Software development:	
Effort:	3 man years
Adjust according to level: (B)	21 man years
Estimated development cost:	£2M
Risk:	Low. Other systems (e.g. EGPWS, TCAS II) have already faced exactly the same problem

Table 8–13 Input sub-element development cost/risk

Input	
Hardware:	
Special requirements:	Voice recognition system desirable for future technology system.
Cost:	Unknown, but unlikely to be a dominant cost.
Software development:	
Effort (man years):	Assumed that voice recognition technology will be developed in any case by other parties.
Adjust according to level: (C)	–
Estimated development cost:	–
Risk:	Medium. Relying on other parties to develop safety-certified voice recognition technology.

Table 8–14 summarises the cost/risk estimates for the IFPM designs of section 7.

Table 8-14 Summary of software development costs/risks

IFPM sub-element:	Risk	Retro-fit design cost (M£)	Future design cost (M£)
Federated navigation system	Medium	3	3
Advanced configuration warner	Medium	7	7
Aircraft status monitor	Low/Med	0.5	0.5
Basic terrain conflict warner	Low	0	0
Flight plan adherence monitor	Low	1.5	1.5
Flight control input sanity checking	High	not used	6
Pilot model	High	not used	1
Flight plan sanity checker	Low	0.5	0.5
Automatic flight re-planner	Low	1	1
Pilot workload smoother and task prioritiser	Med	7	7
Output	Low	2	2
Input	Med	–	None – assumed that technology developed for other applications.
Totals:		22.5	29.5

The two cost totals (£22.5M and £29.5M) only include the software development costs of the individual functional elements of the IFPM design. The total software development costs would be larger, maybe by as much as a factor of two, after the inclusion of the costs that would be incurred during integration testing and aircraft flight testing.

No costs for certification are included in the above estimate, as the costs incurred in certifying such a system are highly uncertain (far more so than the software development cost).

The unit cost for IFPM hardware is also hard to estimate. CASSY software (which attempts similar processing) has been demonstrated running on a high performance workstation which costs around £20k. It seems likely therefore that the extra hardware required for an IFPM per aircraft (processing power and database storage) would not amount to a huge cost, perhaps less than £200k.

The cost of installing an IFPM (e.g. as a retrofit) is also hard to estimate. Although the system requires no new data sources, installation of a fully-functional IFPM would certainly not be a minor modification and the modification would require significant certification effort.

8.4 Implementation time scales

8.4.1 *Timings for availability of new technology*

As discussed in section 7.2, new technologies that impact on the IFPM design include:

- ATC datalink;
- Satellite navigation for safety-critical applications;
- AI systems for safety critical applications;
- Voice recognition technology.

Discussion of how these technologies are likely to be implemented and corresponding time scales are included below.

ATC datalink

There are three leading technologies for provision of datalink:

- Mode S secondary surveillance radar;
- VHF datalink;
- Satellite datalink.

The development of these technologies for use in aviation is proceeding very slowly, not least because it is not yet certain which should become the predominant datalink technology for aviation, or how the 3 sub-networks will be integrated into the aeronautical telecommunications network. In addition, there are few well developed potential applications which would drive implementation of data link: a fully functional IFPM would be one potential application.

As an example of the likely time scales within which the datalink might become available, Mode S will only allow full scale, safety-critical aircraft/ground communication (required for IFPM input) by 2005 at the earliest.

Other datalinks might be able to provide aircraft/ground communications before 2005 and indeed trials of oceanic clearance delivery are being conducted in the UK using a VHF datalink. However, implementation of large scale datalink applications will require considerable evolution of ground systems and widespread implementation is unlikely before 2005.

Satellite navigation for safety-critical applications

Satellite navigation could be used by the IFPM to improve the certainty of aircraft position by providing another data source against which to check position.

The GPS Standard Positioning Service is currently freely available and is finding many applications. The barrier which is stopping its use for general navigation on commercial aircraft at present is that it is impossible to ensure data integrity and accuracy from the GPS satellite transmissions themselves. This is being rectified by the launch of a set of complementary geostationary satellites in the near future (end of 1995 for launch, less than 5 years for service to become available). This should then allow the use of GPS as a complement to existing radio navigation aids (e.g. VOR, DME but not ILS). Replacement of these systems by satellite navigation is not likely in the short to mid term future.

Higher precision services which would, for example, allow landing approaches to be made are not likely to come into service for large transport aircraft until later on (perhaps arriving with later satellite navigation implementations).

The IFPM could therefore make use of GPS output to complement existing radio navigation aids in the short-term future, perhaps within 2 to 3 years. It could act as the data-fusion element to combine navigation outputs.

Safety-critical AI software

At the time of writing, there are no AI applications (known to the authors) that have undergone safety certification. This represents a major obstacle for IFPM functions that require such technology. Safety certification requires software to be developed within a standard design methodology, but agreement has not yet been reached on an internationally acceptable standard for AI systems.

There are several drivers pushing forward the possibility of AI software for safety critical applications, as identified in section 3. These are:

- military applications (e.g. US Pilot's Associated program);
- space applications (e.g. NASA's work);
- civil initiatives (e.g. the EC's ESPRIT program).

The combined effort being placed in these programs is sure to produce advances that will eventually allow certification. It is hard to estimate how long this might take, but a reasonable estimate is 5-10 years.

Voice recognition systems for safety-critical applications

Voice recognition systems are rapidly becoming more reliable. For example, CASSY's voice recognition input successfully interprets 90% of input commands (in operational assessments).

There are a huge number of potential applications for reliable voice recognition technology. Therefore, a reasonable assumption is that the technology will not have to be developed especially for an IFPM.

It is therefore likely that suitable voice-recognition technology will be available within 6-8 years.

8.4.2 *Design for retro-fit to existing aircraft*

The fastest way to implement some sort of IFPM design would be to carry forward one of the existing research programmes. Even if this is done (rather than starting a design from scratch), implementation time scales could still be quite long.

For example, CASSY has been developed from scratch over a period of about three to five years. A certifiable IFPM would have to be designed and produced from scratch in a quality-controlled environment (to allow certification). It seems likely, therefore, that IFPM development time would be at least three years, and could take five. The device would then have to be certificated through trials, etc: this is likely to take at least as long. It therefore seems probable that the shortest time scale on which a usable IFPM could be produced is 6-10 years.

8.4.3 *Design for fit to future aircraft using future technology*

A fully functional IFPM requires future technology, in particular the ATC datalink, which is unlikely to be implemented (with enough functionality) until 2005 (see section 8.4.1). However, IFPM development could proceed in parallel with the implementation of ATC datalink, so there is no reason why it could not be developed as an application.

8.5 **Summary**

This section has considered the costs, risk and timings associated with development of an IFPM. The main conclusions are:

- The costs of developing IFPM software do not appear to be huge (£50-60M) compared with the costs of developing other aircraft systems (e.g. fly-by-wire software for the B777 cost orders of magnitude more to develop). These cost estimates are in line with those estimated by Dornier for developing CASSY into an operational system: they estimate it would cost £20-50M. The costs of certifying such a system are uncertain.

  The development costs may be amortised providing the market for the device is large enough. For example, suppose the market was 10,000 aircraft: the software development costs would then only be £5-6k per device. The design proposed is modular, so that elements (such as the basic terrain conflict warner) could find wider application than just large transport aircraft, for example commuter jets. This would decrease the significance of the development costs further.

- IFPM hardware unit cost would not be prohibitive (e.g. a top-end workstation which could run the software, as demonstrated with CASSY, costs around £20k). It is conceivable that the unit hardware cost for an IFPM may be less than ten times as much.

- The major risk involved is in using AI techniques to produce real-time software running in a safety-critical environment. This appears never to have been done before for a civilian application.

9 CONCLUSIONS

The occurrence of CFIT accidents could be greatly reduced by providing aircraft with improved versions of GPWS (such as Enhanced GPWS or GCAS). These systems use digital terrain maps to provide the warning device with a forward-looking and more intelligent capability. This allows the system to:

- Warn of rising terrain ahead of the aircraft, well before radio altimeter generated warnings.

- Warn crews performing non-precision approaches, if an attempt to land where there is no runway is made.

- Increase crew situational awareness by providing vertical navigation information.

- Greatly reduce the false alarm rate which plagued earlier systems and reduces crew confidence in the system, by warning envelope modulation.

An IFPM aimed at reducing CFIT could probably not offer significant safety improvements over EGPWS or GCAS in many CFIT circumstances. However, the IFPM could be used in a wider range of circumstances and has more to offer.

A particular problem, which could potentially be addressed by an IFPM, is that modern advanced-technology aircraft are not necessarily much safer than older generation aircraft, mainly due to poor man-machine interface design. At present, the different aircraft systems operate more or less independently of each other. There is no 'integrating' device taking an overview of the aircraft's situation. In addition, the crew can loose awareness of what the aircraft's automatic systems are doing, particularly in abnormal flight situations.

These phenomena could be tackled in several ways, including:

- Improve the interface on existing systems to increase 'mode awareness', and prevent automated systems from getting any more complex than they are at present. This should obviously be done for existing systems with known problems with the interface design. However, there is still a risk that crews are presented with too high a workload in abnormal situations: the automated systems are not helping the crew when help is needed most. Also, the crews might become used to the automated systems and therefore be less able to cope in abnormal situations.

- Reduce the level of automation. This might solve the new problems that have been encountered, but give rise to reoccurrence of the older problems that were the original drivers for automation.

- Increase the 'intelligence' of the aircraft systems so as to provide crews with a smooth workload under all situations (to prevent underload or overload) and prioritise crew tasking. This is an attractive alternative if it is feasible, since it realises the goal of automation. This amounts to a change in interface design philosophy, to a more 'human-centred' approach.

The last alternative fits the concept of Intelligent Flight Path Monitoring, however it constitutes more than just a 'black box' addition. A fully-functional implementation would provide the crew with an intelligent monitoring system, that performs an autonomous situation assessment for the aircraft, drawing crew attention to the most relevant information. Such a device would (potentially) be immune to the known human failure modes (information saturation, vigilance, etc).

The feasibility of such a system has been demonstrated with the Cockpit Assistant System (CASSY), subject to the availability of new technology such as reliable voice recognition technology and ATC datalink.

A major difficulty that would be encountered in producing such a system suitable for commercial operation would be in its certification. Safety certification of artificially intelligent systems appears to be feasible (although it is likely to be expensive). Safety certification requires software to be developed within a standard design methodology, but agreement has not yet been reached on an internationally acceptable standard for AI systems.

The development costs of such a system do not appear to be huge, at around £50M: however, the certification costs are uncertain. The implementation time scales of the new technology required are such that it would not be possible to provide a fully functional system until around 2005.

However, a lot could be done to improve the performance, autonomous assessment and ease of use of automated systems using only existing technology. Sophisticated warning functions could be provided without placing any higher specifications on other aircraft systems. Automatic flight re-planning could be provided (without using AI) that might significantly reduce crew workload in abnormal flight situations. The development costs of such systems do not appear to be prohibitive. However, it seems likely that the shortest time scale on which the equipment could be produced and in use is 6 years.

10 RECOMMENDATIONS

10.1 Short-term

Short-term solutions to the identified safety problems in existing large commercial transport aircraft include:

- Fitting enhanced GPWS equipment into aircraft. Such systems are exemplified by EGPWS or GCAS. These systems should become available in 1996 and, if fitted, will reduce the CFIT accident rate. Given that the unit cost of systems like EGPWS is comparatively low ($54,000, less than the cost of a new coat of paint for a large transport aircraft), this appears to be a highly cost-effective solution.

- Changing poorly designed existing aircraft system interfaces to be more 'human-centred'. For the large part, this may involve changing the software (e.g. to reduce the number of autopilot modes).

For smaller aircraft (e.g. commuter jets), fitting GPWS would also reduce the incidence of CFIT. As price is the main barrier to this, it is worthwhile considering if simpler GPWS equipment could be specified for such aircraft, which may allow provision of cheaper equipment.

10.2 Long-term

Aircraft manufacturers and airlines should be encouraged to consider building aircraft with more intelligent man/machine interfaces. At present, different aircraft systems are not fully integrated. The only unifying element is the human crew, which is subject to well-known failure modes.

It is clearly worthwhile considering the provision of an integrating device taking an overview of the aircraft's situation, as it could significantly increase flight safety. This application (which could be termed an Intelligent Flight Path Monitor) could continually take into consideration a wider range of information than is possible for the crew. The aim of this device would be two-fold:

- To smooth the crew workload, so that it is uniform even under abnormal flight conditions.
- To direct crew attention to the most important information.

11 REFERENCES

1 MOORE C G AND FAIRBANKS M C, *'Response to tender no 7D/S/1240: Study into the feasibility of an intelligent flight path monitor',* Smith System Engineering technical proposal 3A040D001/1.0, 15 September 1994.

2 *'Controlled Flight Into Terrain'*, Royal Aeronautical Society Conference Proceedings ISBN 1 85768 026 X, 8 November 1994.

3 HUGHES D AND DORNHEIM M A, *'Accidents direct focus on cockpit automation',* Aviation Week & Space Technology, 20 January 1995.

4 BATEMAN D, *'Development of ground proximity warning systems (GPWS)'*, Proceedings of Royal Aeronautical Society conference on Controlled Flight into Terrain, 8 November 1994.

5 CHAZELLE X, *'A new concept for combating controlled flight into terrain'*, IEE colloquium on 'Terrain databases and their use in navigation and collision avoidance', digest number 1995/066, 4 April 1995.

6 SMITH B et al, *'Accident-proof at a price'*, Flight International p 31, 14 April 1993.

7 HOLMES D I AND RETELLE J P, *'The Pilot's Associate',* AGARD conference proceedings no 474 'Knowledge based system applications for guidance and control', 18 September 1990.

8 DUDEK H L AND LUX P, *'Increased safety through knowledge-based pilot assistance'*, Dornier Post, April 1992.

9 DALY K, JEZIORSKI A AND SEDBON G, *'Artificially intelligent computers may one day advise pilots what to do next'*, Flight International p 25, 24 August 1994.

10 BROATCH S A AND HENLEY A J, *'An integrated navigation system manager using federated Kalman filtering'*, Proceedings of the IEEE National Aerospace and Electronics Conference, Dayton, OH, 20-24 May 1991.

11 CULBERT C, RILEY G AND SAVELY R T, *'Approaches to the verification of rule-based expert systems'*, NASA Johnson Space Centre, Houston, Tex: First annual workshop on Space Operations Automation and Robotics, 1987.

12 ONKEN R & PREVÔT T, *'CASSY- cockpit assistant system for IFR operation'*, 19th ICAS Congress Anaheim, USA, September 1995

13 BILLINGS C E, *'Human-Centred Aircraft Automation: A Concept and Guidelines'*, NASA Tech Mem 103885, Moffett Field CA, 1991.

14 WEINER E L, *'Reflections on Human Error: Matters of Life and Death'*, Proc Human Factors Society 33rd Annual Mtg, 1989.

15 HILL G, *'The design certification aspects of intelligent systems'*, Proc RAeS conference *'The role of intelligent systems in defence'* ISBN 1857680561, 27–28 March 1995.

Appendix A Relevant Accidents

Table A–1 presents a selection of aircraft accidents relevant to the discussion in the main document. Sources: World Aircraft Accident Summary and references 2, 3 and 13. The list is by no means exhaustive for CFIT or human error associated accidents, and is provided for reference only. For example, there where 23 CFIT accidents involving large commercial jets on a world-wide basis between 1989 and 1993.

Table A–1 Selection of relevant aircraft accidents

Ref	Year	Aircraft type	Location	Summary
a	1986	Viscount	UK	Landed wheels up.
b	1987	MD-80	Detroit	Incorrect configuration on take-off.
c	1988	A320	Gatwick	Crew selected inappropriate descent made on approach, resulting in an accident being narrowly avoided.
d	1988	A320	Habsheim (France)	Low, slow, idle pass at air show resulted in crash. Overconfidence in the flight envelope protection systems.
e	1988	B727	Dallas	Incorrect configuration on take-off.
f	1989	B737	Brazil	Aircraft set off on 270° heading instead of 027°. Aircraft crashes due to fuel starvation. GNE accident.
g	1990	A320	Bangalore	Inadvertant use of altitude aquisition and open descent modes. Mode awareness problem.
h	1990	B707	New York	Fuel starvation after ATC put aircraft on hold.
i	1990	B737-200	Unalakleet (Alaska)	Valid 3° approach from an incorrect step-down fix resulting in crash well short of runway. GPWS 'no warning' situation.
j	1991	B727-200	Taegu (Korea)	Landed wheels up due to misunderstanding between crew members.
k	1991	A310	Moscow	Pilot manual flight inputs with autopilot engaged.
l	1991	A320	Paris	Aircraft mishandled on ILS approach by use of auto-flight controls, resulted in an accident being narrowly avoided.
m	1992	A320	Strasborg	Crew set descent rate to 3300 fpm instead of 3.3 degrees. Mode awareness problem.
n	1992	A310	Katmandu	Hit mountian ridge at 11,500 feet during appraoch in monsoon conditions.
o	1992	A300-B4	Katmandu	Hit high ground on approach in clear weather 8nm from runway.
p	1994	A300-600	Nagoya	Pilot manual flight inputs with autopilot engaged.

Appendix B Operator's view – Air 2000

B.1 INTRODUCTION

This appendix presents the results of discussions with Air 2000, and as such are the views of the IFPM concept as perceived by their senior staff. Air 2000 is organised in such a way that the senior managerial staff are also pilots and engineers, who can therefore present a balanced, commercial view. Air 2000 operates primarily as a charter airline: views from airlines operating scheduled flights may be different.

B.2 REQUIREMENTS

An operational requirement exists for monitoring the flight path of commercial aircraft during the take-off and landing phases. The aim of such monitoring would be to provide more timely CFIT warnings, hence reduce these incidents. The device would be of most use on non-precision approaches, or on approaches to airfields with which the pilot is not familiar. The use of some form of terrain referenced navigation or terrain characteristic navigation would be valuable, to either increase the integrity of existing navigation systems or to provide an alternative means of navigation on non-precision approaches (e.g. a back-up for satellite navigation systems). The use of a vertical navigation display would be extremely useful in increasing pilot situational awareness, thereby reducing CFIT accidents. Such a monitoring device would probably only be fitted (in preference to GPWS) if it was mandatory (for commercial reasons).

The requirement for flight path monitoring in the en-route phases of flights is less. Although gross navigational errors are known to have occurred, these have rarely led to loss of life (only two recent examples: the B737 accident in Brazil in 1989 and the Korean aircraft that was shot down when it accidentally strayed into USSR restricted airspace). Also, such incidents mainly occur in minimum navigation performance airspace (Oceanic), where there is only a marginal increase in collision risk with other aircraft and no CFIT risk at all. However, if flight path monitoring is carried out in any case to cover other operations, it could easily be extended to cover en-route airspace operations and would provide a useful backstop.

Using an IFPM to check if the current autopilot mode is appropriate for the aircraft situation is not a good solution to pilot/autopilot misunderstandings. It would be better to fix this problem at source by re-designing interfaces and perhaps including greater monitoring of the aircraft situation within the FMS, rather than the 'band-aid' solution of fitting yet more equipment. However, if the IFPM was to provide a cheaper solution than re-issue of FMS/EFIS software/hardware, then there may be scope for requiring the IFPM to carry out autopilot monitoring.

Similarly, it is not appropriate for an IFPM to give configuration warnings more complex than those given by current aircraft systems. If warnings more complex warnings are required, they should be given by extensions to existing aircraft configuration warners. Nevertheless, if the IFPM could provide configuration warnings autonomously and independently from the other systems, it would provide a useful backstop.

It may be appropriate for an IFPM to warn of low-energy situations as part of the CFIT warning capability. The aircraft's energy could be considered by the IFPM in the context of the current aircraft situation.

If an IFPM can autonomously perform an independent sanity check on total fuel quantity or fuel remaining for a flight, it might provide a useful back-up to existing procedures. The incident involving a B767 (about a decade ago) in Canada in which there was confusion between lbs and kgs when loading fuel (which resulted in an emergency landing) could have been prevented by such a system. Or the incident in 1990 when a B707 crashed due to fuel starvation (New York) might have been prevented.

IFPM involvement in flight planning would be extremely difficult given the current Air Traffic Management scenario. Current ATC structures and procedures are such that it is not possible to plan flights in sufficient detail for an IFPM to have sufficient knowledge. For example, tactical ATC intervention is extremely frequent and it is rare for a flight to carry out its filed flight plan: this plan is really only a rough guide for what might occur on a given flight. This situation may well change in future ATC schemes, e.g. schemes in which ATC computers negotiate a 4-D flight plan with the aircraft's flight management system. Alternatively, the impact that 'free flight' schemes might have on flight planning and execution should be considered. For example, the IFPM could form an independent monitoring application on the aircraft, checking for conflicts ahead of the aircraft and advising pilots on ways of resolving these conflicts (e.g. avoiding manoeuvres or speed control).

In the shorter term, the IFPM may find some use in helping to re-plan flight changes, e.g. to suggest alternative routes. The information to allow crews to re-plan exists within the cockpit already: however, a computerised device may well be more efficient.

B.3 SUMMARY

In summary, the primary operational requirement for an IFPM should be to provide CFIT warnings and increase pilot situational awareness with respect to vertical navigation. Such warnings should be generated by monitoring the aircraft velocity/status with respect to current position/terrain.

Shortcomings that exist in existing aircraft systems should be addressed 'at source', not using the 'band-aid' solution of an IFPM.

However, a device that generates warnings based on an independent aircraft situation assessment could provide a useful safety backstop.

An IFPM may be of use in re-planning flights en-route, for example by suggesting alternatives.

An IFPM suitable for future aircraft may include extra functionality, e.g. to form the aircraft 'negotiator' for future ATC scenarios or to independently monitor the aircraft's traffic status in a 'free flight' scenario.

Appendix C Operator's View – Virgin Atlantic

C.1 INTRODUCTION

This appendix presents the initial reactions to the IFPM concept from Virgin Atlantic's flight operations department.

C.2 VIEWS

A system which reduces the potential for CFIT can only be welcomed, and if such a system can be expanded to provide a safeguard against aircraft entering unsafe circumstances other than potential CFIT this, too is a welcome development.

In the shorter term, EGPWS or GCAS and a 1 or 2-D navigation display should be a priority. This would provide immediate safety benefits and would most readily be integrated in current aircraft for retro-fit.

Further development of a system incorporating AI is very desirable and will depend as always on cost/benefit to the user.

Integration of certain current aircraft systems into an IFPM would be a potential cost benefit for new aircraft systems.

Any system should only be regarded as complementary to, and not a substitute for, well defined (and rigidly adhered to) operational procedures, even if it provides the clear benefits of an IFPM.

For example, GNEs are avoided at Virgin Atlantic by methodical and cross checked data entry procedures. This is not to say this system is infallible; an IFPM would be an invaluable backstop.

It is vital that pilots are 'kept in the loop' by direct involvement with all major tasks. Whilst it is felt that the use of an IFPM as a sophisticated fuel manager is a good idea, its role should be restricted to one in which advice and/or warnings are given but the 'Manager' should remain the pilot. Configuration changes should be left partly at least to the crew. On one of Virgin Atlantic's current aircraft types, fuel management is mostly automatic. Certain tasks, however, are left to the crew; these too could easily be automated but the philosophy is to ensure crew awareness of system status by direct participation. The same philosophy could be read across to other systems and procedures.

'What's it doing now?' is the well known cry of the pilot first exposed to the new generation of EFIS/FMS aircraft, particularly those formerly used to operating with a Flight Engineer. The temptation is very great for pilots to make FMS keyboard inputs at inappropriate times (typically in the last stages of an approach) when the emphasis should be on aircraft handling/flight path monitoring. An IFPM must therefore be free from pilot input to avoid further temptation and greater workload.

Over confidence in FMS is cited as a contributory factor to accidents/incidents. There may be a danger that safety within an IFPM-equiped aircraft may suffer from the same misplaced confidence. Virgin Atlantic's policy is 'trust but verify': the substantial benefits of EFIS/FMS/EICAS/Autoflight are used to advantage, while at the same time a healthy scepticism is held of these systems. All automatic mode changes are announced by one pilot and verified by another. This approach should not be changed to one in which an over-developed sense of security is engendered by the comfort of knowing the IFPM is always there to take care of problems.

An airline which operates charters (especially the ad-hoc type) may be the greatest beneficiary of an IFPM in that short-notice flights to unfamiliar airfields in non-sophisticated ATC environments are likely.

The scheduled airline uses a fixed number of destinations which are usually:

- well known to crews;
- served by precision navigation aids;
- controlled by modern ATC equipment;
- backed up by a developed infrastructure.

These factors combine to make the safety benefits of installing an IFPM perhaps greater for the charter airline operator.

C.3 SUMMARY

In summary, the IFPM concept was met with enthusiasm, albeit with certain caveats.

In the short term, the use of enhanced versions of GPWS which include vertical navigation displays should be a priority, as it would have immediate safety benefits.

In the longer term, the development of an artificially intelligent third pilot should yield safety benefits. However, such a device should keep pilots 'in the loop' and should not be a substitute for well defined and rigorously adhered to procedures. An IFPM should run autonomously (i.e. require no pilot input for its operation). Care should be taken to avoid crews placing too much trust in the IFPM, it should only ever be a backstop.