Cranfield UNIVERSITY

Flight control system architecture analysis and design for a fly-by-wire generic regional aircraft

J.Gautrey

COA report No.9604
March 1996

Flight Dynamics Group
College of Aeronautics
Cranfield University
Cranfield
Bedford MK43 0AL
England

College of Aeronautics Report No.9604
March 1996

Flight control system architecture analysis and design for a fly-by-wire generic regional aircraft

"The ..... and

Flight Dynamic
College of Aer
Cranfield Unive
Cranfield
Bedford MK43
England

Summary

Fly-by-wire systems are becoming increasingly common in civil transport aircraft due to the economic and technological benefits that this technology provides. These fly-by-wire systems are comprised of two major components; the flight control laws, which govern the aircraft's handling characteristics, and the flight control system architecture, or the hardware, which is used to implement the control laws.

This report will primarily consider the design of the flight control hardware, although control laws will be briefly examined for current civil fly-by-wire aircraft. The background to the architecture is presented, along with relevant issues such as processing distribution and the requirements for system synchronisation. The flight control systems for current civil aircraft are described in detail, and these systems are compared to detailed certification, maintenance and functional requirements.

The findings of the analysis are used to propose a fly-by-wire flight control system architecture for a Generic Regional Aircraft. This architecture is not complex, only uses existing technology and meets the requirements previously determined. It has a capability for deferred maintenance since it is shown that the aircraft can be dispatched with one flight control computer failed and still meet the mandatory reliability requirements defined by the national airworthiness authorities. Control laws are not proposed.

Contents

List of Figures

List of Tables

Notation

AC	:	Alternating Current
ACMP	:	AC Driven Motor Pump
ACARS	:	Airplane Communications and Reporting System
ACE	:	Actuator Control Electronic
ADC	:	Air Data Computer
ADIRS	:	Air Data & Internal Reference System
ADIRU	:	Air Data & Internal Reference Unit
ADP	:	Air Driven Pump
AFCS	:	Automatic Flight Control System
AFTI	:	Advanced Fighter Technology Integration
AFS	:	Automatic Flight System
AIMS	:	Airplane Information Management System
ALS	:	Angle of attack Limiting System
A/PDMC	:	Aircraft / Propulsion Data Management Computer
APU	:	Auxiliary Power Unit
ARINC	:	Aeronautical Radio, Inc.
BGP	:	Byzantine Generals Problem
BITE	:	Built In Test Equipment
BLC	:	Boundary Layer Control
CCDL	:	Cross Channel Data Link
CFDIU	:	Centralised Fault Display Interface Unit
CFDS	:	Centralised Fault Display System
CG	:	Centre of Gravity
CMC	:	Central Maintenance Computer
CMS	:	Central Maintenance System
CPU	:	Central Processing Unit
CSU	:	Command Sensor Unit
DC	:	Direct Current
DFCS	:	Digital Flight Control System
DFGS	:	Digital Flight Guidance System
DLC	:	Direct Lift Control
ECAM	:	Electronic Centralised Aircraft Monitor
EDP	:	Engine Driven Pump
EEC	:	Electronic Engine Controller
EFIS	:	Electronic Flight Information System
EIS	:	Electronic Instrumentation System
ELAC	:	Elevator & Aileron Computer
ELMS	:	Electronic Load Management System
ETOPS	:	Extended Range Twin-jet Operations
FAC	:	Flight Augmentation Computer
FADEC	:	Full Authority Digial Engine Control
FBW	:	Fly By Wire
FCC	:	Flight Control Computer

FCDC	:	Flight Control DC bus
FCP	:	Flight Control Panel
FCPC	:	Flight Control Primary Computer
FCS	:	Flight Control System
FCSC	:	Flight Control Secondary Computer
FCU	:	Flight Control Unit
FGC	:	Flight Guidance Computer
FHA	:	Failure Hazard Assessment
FMEA	:	Failure Modes and Effects Analysis
FMGEC	:	Flight Management Guidance & Envelope Computer
FMS	:	Flight Management System
fpm	:	Feet Per Minute
fps	:	Feet Per Second
FPV	:	Flight Path Vector
FTA	:	Fault Tree Analysis
HUD	:	Head Up Display
IBU	:	Independent Backup Unit
IDG	:	Integrated Drive Generator
IFU	:	Interface Unit
ILS	:	Instrument Landing System
IRS	:	Internal Reference System
JAR	:	Joint Airworthiness Requirement
LAF	:	Load Alleviation Function
LaRC	:	Langley Research Centre
LRU	:	Line Replaceable Unit.
MAFT	:	Multi-Lane Architecture Failure Tolerant
MCDU	:	Multi-purpose Control & Display Unit
MCU	:	Modular Concept Unit
MDDU	:	Multipurpose Disk Drive Unit
MFCS	:	Mechanical Flight Control System
MIL-STD	:	Military Standard
MMEL	:	Mandatory Minimum Equipment List
MTBUR	:	Mean Time Between Unscheduled Removal
MTBF	:	Mean Time Between Failure
MTU	:	Monitor & Test Unit
OMS	:	On-board Maintenance System
PCU	:	Power Control Unit
PFCS	:	Primary Flight Control System
PFC	:	Primary Flight Computer
PFD	:	Primary Flight Display
PMG	:	Permanent Magnet Generator
PPU	:	Position Pick-off Unit
PRIM	:	Primary Computer
RAT	:	Ram Air Turbine
RBD	:	Reliability Block Diagram

RCCB	:	Remote Controlled Circuit Breaker
SAARU	:	Standby Attitude & Air data Reference Unit
SCAS	:	Stability & Command Augmentation System / Stability & Control Augmetation System
SC/EFC	:	Spoiler Control / Electric Flap Control
SEC	:	Secondary Computer / Spoiler & Elevator Computer
SFCC	:	Slat & Flap Control Computer
SSA	:	Series Servo Actuator
STAT INV	:	Static Inverter
STOL	:	Short Take-Off & Landing
SURE	:	Semi-Markov Unreliability Range Evaluator
TAC	:	Thrust Asymmetry Compensation
THS	:	Trimmable Horizontal Stabiliser
TOGA	:	Take Off / Go Around
TRU	:	Transformer Rectifier Unit
USB	:	Upper Surface Blown
VSCF	:	Variable Speed Constant Frequency

1. Introduction

Over the years, new aircraft programmes have brought with them opportunities to introduce new technologies. In the 70s and early 80s, digital technology and the glass cockpit were introduced, allowing significantly increased functionality of flight management and on-board maintenance systems. The demands for functionality continue to increase, conflicting with the demand for lower costs. The real challenge is the selection of technologies which can best meet this desire for functionality with higher reliability and less maintenance, at a reduced cost. The focus has shifted towards the processing of large amounts of data, and system data dependency has increased. The high data transfer requirement has lead to high speed multi-access digital data buses and for more integration of related systems.

Fly-by-wire flight control systems have been developed to enable the benefits of this new technology to be exploited. Fly-by-wire is where the conventional mechanically signalled flight control surfaces are electrically signalled, with the demands being computed by a flight control computer from sensor information on the pilot's inceptors. However, the design of these systems is challenging, and presents a set of problems which are not experienced with a conventional hydro-mechanical flight control system. Another major challenge is knowing exactly what can be accomplished within a particular programme schedule. It is usually necessary to defer some functionality beyond first flight and even entry into service to reduce timescales. The deferral must be discussed and accepted by the manufacturer and the airlines.

Due to an increasingly large number of aircraft subsystems being microprocessor based, and high data transfer requirements, a variety of different digital databuses have been developed. Flight control systems therefore take advantage of these digital microprocessor-based systems. However, alternative means of powering the control surfaces have not yet been applied in a mass produced civil aircraft. The traditional method of hydraulically driving a control surface from either electrical or mechanical signalling is still common.

A fly-by-wire flight control system has many benefits. From an economic point-of-view, a digital fly-by-wire system is lighter, has lower recurring costs and generally has a lower maintenance demand compared to a conventional hydro-mechanical system. A fly-by-wire aircraft can also be developed with better flying and handling qualities so that overall safety is improved, and all deficiencies can be compensated for. This allows the aircraft aerodynamic efficiency to be improved since reduced tail surface sizes are possible with relaxed static stability, which fly-by-wire allows. Stanislaw [1] states that for the Citation III, the expected savings in cable weight alone by using electrical signalling on a databus amount to 374 lbs over a conventionally signalled aircraft, which is equivalent to one passenger plus baggage. A similar saving was found by using fly-by-wire on the Airbus. A weight reduction of 136 kg was made on the A320 [2] by replacing the conventional mechanical control linkages with electrical signalling, while another 56 kg was saved by the use of sidesticks instead of conventional control wheels. According to Bleeg [3] of Boeing, the weight saving on

the projected Boeing 7J7, which is of similar size to the A320, would have been approximately 270 kgs with a fly-by-wire implementation.

This study will consider the primary hardware elements of the system, principally the flight control computers, the actuators and associated hardware, plus a brief consideration of the connected systems and databuses. The hydraulic and electrical requirements directly related with flight control will also be considered at a high level. The avionics displays, other aircraft structure and systems, the electrical load management and ARINC packaging standards will not be considered.

This report does not consider the detailed autopilot functions since they do not concern the pilot-handling of the aircraft directly, though they certainly play a large part in the man-machine interface. The cockpit ergonomics will not be considered either, though they also play a large role in flight crew awareness and flying qualities. The study by Field [4] provides an excellent source of information on this topic.

Chapter 2 considers the main types of failures that occur in systems, and the way that they affect the overall system reliability. Methods for assessing the system reliability are presented, along with their advantages and disadvantages, and the main reliability issues are also discussed. Following on from this, in Chapters 3 and 4, the basic functional requirements for an ultra-reliable flight control system are drawn up together with any design implications and the methods by which the flight control system can be assessed. In Chapter 5, the flight control systems of the aircraft considered for this study are analysed with respect to the established requirements. The aircraft considered are the Airbus A320, A330 and A340, and the Boeing 777, although other military fly-by-wire aircraft are described in the Appendices. Recommendations will then be made for a flight control system for a fly-by-wire Generic Regional Aircraft in Chapter 6.

The aircraft descriptions in the appendices represent a literature search carried out for each aircraft. Hence the quantity of data available for each aircraft varies, depending on what was available during the search, and what has been published by the manufacturers. A bibliography is included for each aircraft.

2. System Fault Tolerance

As flight control systems become increasingly complex, the achievement of very high operational availability has become a crucial part of the design process. Traditionally this availability has come through increased redundancy, and voting schemes. However, this can present problems with ultra-reliable systems.

Systems are required to be fault-tolerant, that is they continue to function correctly in the presence of a finite number of component failures. This section will therefore cover the major issues with fault tolerance in ultra-reliable systems. System performance will not be covered since it does not affect the system architecture as much as the reliability of the individual components within the system. However, this is a non-trivial task since it is often difficult to perform enough tests to observe any statistical change in system performance. Hence coding methods which enable the system to be analysed must be used, and are briefly described.

Failure analysis plays an important part in the design of flight control systems, especially for relatively complex fly-by-wire systems since it is imperative that the system is well behaved under failure conditions, and that failures do not propagate throughout the system. Therefore failures have been considered here, as well as the implications on the design of the fly-by-wire system architecture.

2.1 Definitions

This section briefly defines some of the more common terms and concepts that are needed. The definitions have been obtained from [5], and definitions in the Airworthiness Documents, for example JAR 25 [6] must be carefully considered when aircraft certification is being examined. The departure from the required functionality of a system constitutes a failure so that a dependable system can also be described as one that does not fail. Failures are attributable to underlying causes such as faults. Faults can include mistakes in specification or design (i.e. bugs), component failures, improper operation and environmental anomalies (e.g. electromagnetic perturbations). Not all faults provide immediate failures: failure is the property of the external behaviour of the system which is itself a manifestation of internal states and state transitions. An error is the result of a fault, which is localised in a part of a system, and (if uncorrected) can lead to complete system failure. i.e. an error is, in effect, a 'localised failure' within a system which does not lead to an 'external' failure. Fault tolerance is based on detecting latent errors before they become effective, and then replacing the erroneous component of the state by an error-free version. The definitions are important - the term error is generally used to describe programming mistakes or bugs that are properly called faults.

The propagation of a fault so that the output of a processor is erroneous will be termed a processor failure [7], a failure of the channel containing that processor or simply a failure. The propagation of an erroneous value past the comparator to a surface actuator

for at least one iteration of the control programme will be termed a system failure. The fault latency time will be defined as the time between the fault appearing in the processor and the time the fault subsequently appears at a comparator.

The complete computational cycle is broken into frames, each attending to a separate control aspect, for example longitudinal, lateral and directional control [8]. Some variables may need more rapid cycling than others, so the pitch calculations may be of four frames duration, the laterals two frames, and navigation one frame. This is called multi-rate periodic schedule. Each frame will perform several functions such as sensor sampling, control law evaluation etc.

Coverage

Coverage [9] is defined as the joint probability that given a fault, it will be detected, isolated and recovered from. Detection coverage is defined as the probability that a given fault will be detected within a time period that allows fault isolation and system recovery to proceed without causing an unacceptable system disturbance. Similarly, a fault is considered correctly isolated when the fault is identified to the recoverable interface within a time frame which allows recovery without causing an unacceptable system disturbance. Recovery coverage is the probability that given a fault has been correctly detected and isolated, the system will recover within an acceptable time frame. The total time for detection, isolation and recovery within a system often depends on the current mode of operation of the system in question. The probability is often referred to as the letter C, with C=1 implying that the coverage is 100%, when the system will definitely detect, isolate and recover from all of the faults that it encounters.

Work initially carried out on coverage [10] showed that for a typical triplex system, the overall system reliability became independent of detecting the second failure as the coverage for detecting the first independent hardware failure decreased. As the required system reliability increases [11], the required system coverage increases. A value of C=1 is possible and can be demonstrated by a formal proof via design for validation methods (see section 2.4.3), though not for a duplex system. Design for validation begins with a formal specification of the system requirements written in a formal mathematical language. The system design then proceeds in a hierarchical fashion from the highest-level specification of the system down to the detailed implementation of it.

Reliability and fault recovery

The statistical failure rate can be determined by programs such as SURE (Semi-Markov Unreliability Range Evaluator), which can give a range of failure rates dependent on the coverage, and probabilities for recovering from failures [12,13]. Mathematical models of fault tolerant systems must describe the process that leads to a system failure, and the system fault-recovery capabilities. The SURE approach is an extension to the standard Markov modelling approach, which has been used for many years to describe fault-tolerant systems. A Markov model essentially has a series of states. Certain states in

the system represent system failure, and others represent fault-free behaviour, or correct operation in the presence of faults. Each state therefore represents a combination of numbers of working processors, failed with the failure detected and failed without the failure detected (i.e. uncovered). The probability of the system switching between the individual states can be calculated which can give an overall probability for failure. This approach can therefore take account of system recovery, i.e. transient faults, and failures in detecting faults.

For example, system failure could occur if a second failure occurs in a system before the first is removed. The probability of fault occurrence generally taken to be a finite probability per hour, and the time required for fault removal as a normal distribution, i.e. varying around a mean time. Hence the probability of the system failing overall will be bounded by an upper and lower value due to the fault-removal time being considered as a normal distribution. Therefore an analysis can be carried out to determine the failure rate, based on the probabilities of moving from one state to a subsequent one using failure rate data and coverage information of the individual components.

Many analysts are still unfamiliar with the Markov approach since fault tree analysis (FTA) methods have been sufficient for non-reconfigurable, hardware-only systems. In recent years, redundant, software-driven, reconfigurable systems have been designed which cannot be analysed with the FTA method [14].

Traditionally, reliability assessment of system architectures has focused on fault detection, isolation and recovery in the processing systems. A combination of continuous and periodic error checking has usually been combined with monitoring by backup units to achieve the needed reliability. A coverage of 0.98 is possible [15] by using these techniques. However, active monitoring and control can leave the system more vulnerable to false alarms, and erroneous misdiagnosis due to transient events in the monitoring system.

As the required coverage increases, costs tend to rise exponentially. Therefore the design is frozen when the coverage is demonstrated to be greater than the required value. Hence architectural approaches which minimise the required software and hardware coverage for redundant system elements while providing diversity to minimise common mode faults exposure are mandatory if economic complex redundant systems are going to realise their potential.

Where extreme reliability is required, comparison and voting techniques have been used, which ensure almost 100% error detection, with recovery occurring at the comparison circuitry through rejection of the erroneous value. Mid-value selection provides excellent protection against hardware and software faults, however, this is limited to applications where the mid-value selection is acceptable. However, these techniques do not provide protection against failures such as software failure. Therefore careful design is required to avoid common-mode or single point failures being introduced, see section 2.2. For complex designs, where the software is more

complex than the hardware, the benefits of high hardware coverage are swallowed up by the lower software coverage. Additionally, all comparison or voting systems place a high demand on system resources and system weight and cost due to the extra processing and information transportation requirements.

Byzantine Generals Problem

The usual way of looking at this problem is to imagine a situation where there are m Generals, each of whom can communicate with all of the others [16]. A round of communication is where each General nominally sends the same message to all of the other Generals, which includes what that particular General thinks the other Generals have sent in the previous round. A traitor is a General who does not send the same message to every General. The problem is expressed by a theorem which states that "if there are m traitors out of a total of (3m+1) generals then (m+1) rounds of data must be exchanged for the (2m+1) loyal generals to agree upon a plan of action", i.e. to identify and isolate the traitors. Consensus cannot be achieved if there are less than (3m+1) generals, but a 'dumb' traitor could mean that consensus is achieved in less than (m+1) rounds of data exchange, i.e. if that General consistently sends incorrect data to all of the other Generals instead of incorrect data to some of the Generals.

In a flight control system it is usually assumed that a transmitted 'message' is identically received by all receiving processors, irrespective of the failure state of the transmitting processor. The message may be valid or invalid, in which case the receiving processor may take the appropriate action. The Byzantine Generals Problem (BGP) is expressed as follows for a flight control system : A faulty processor may send different versions of the same message to different processors. The asymmetry of transmission is the essence of the problem, and is a result of private communications between the processors.

It could cause problems in the following situations :

1. In a FCS which uses the same selected sensor value in all channels, and which interprets differences in the computed output as an error. If a faulty processor transmits different values of the same sensor to different processors, it is conceivable that a good processor could be conceived to be faulty since it has been working with incorrect input data.
2. In a triplex FCS which employs clock synchronisation, a faulty processor could transmit faulty synchronisation data to one processor, but not another, hence causing the two good processors to loose synchrony. These synchronous algorithms tend to be particularly vulnerable to the BGP.
3. In a FCS which equalises integrators, a faulty processor could transmit different equalisation values to different processors, resulting in integrator drift.
4. In a FCS which switches modes, a faulty processor could transmit an erroneous switching command to one but not all processors. This could cause a good processor to prematurely switch modes and as a result be declared failed by the remaining processors.

The classical solution to this problem is embedded in the theorem. If m processors can be tolerated failed simultaneously, then there is a requirement for 3m+1 processors to be present in the system. The processors also must perform a majority vote on the data received from each data round received in order to determine the correct data to use. However, this can increase the number of processors in the system considerably since seven processors are needed to be able to withstand two simultaneous faults, which could result in an uneconomic and complex system. There are other solutions that can be employed.

1. Employ broadcast communications with error detection.
2. Eliminate or reduce the need for consensus actions.
3. Incorporate sufficient robustness in the system so that when a Byzantine disagreement occurs it will not crash the system.

A broadcast bus will generally ensure that each processor connected to the bus receives the same data, as long as its own receiver is functioning correctly. This will therefore prevent inconsistent data being received by the bus. This benefit is lost however if the processors do not all use the data from the same message to reach a consensus. However, even with a broadcast bus, there are still ways for a BGP to occur, and systems which cannot tolerate a single Byzantine disagreement will not have their problems solved by the use of a single broadcast bus.

One sources of error could be that a transmitter is marginally defective such that a data bit could be read as a 0 or a 1. Noise would also introduce errors into individual receivers. The obvious solution to these problems is to use error detection codes etc. Another solution is to eliminate the need for consensus action. This could be through the use of thresholds that differences between two lanes must exceed for failure to occur, and the use of persistence counting, where the error must persist for a given number of frames for a fault to be generated.

In systems where there is a large degree of robustness tolerance, it is likely that effects such as latent faults and software generic errors will have a greater effect on survivability than a Byzantine disagreement. However, even a robust system can be vulnerable to Byzantine disagreement, notably in the areas of clock synchronisation, integrator equalisation and mode switching logic. Hence each case should be examined carefully before adopting the classical solution, i.e. greater redundancy.

NASA Langley Research Centre (LaRC) have worked on a fault-tolerant digital flight control system [8] using formal methods to provide a rigorous basis for documenting and analysing design decisions. Channel synchronisation and Byzantine fault-tolerant distribution of sensor values are reasonably well understood requirements. Byzantine-tolerant sensor distribution and clock routines are now available.

2.2 Failure Types

This section defines the common failure types, and many of these definitions come from Walker [17].

Random Failure

Traditionally, system designers have only considered random faults which produce symmetric errors. Hence when failures occur, all parts of the system observe the error identically. In most avionics systems this has been acceptable since the time for the error to 'commence propagation' has been small, and the probability of failures being other than symmetric is negligible.

Common Mode Failure

These failures include power supply and environmental events which cause simultaneous failures among multiple users, such as a power supply failure knocking out part of a system. These can also be produced when a system designer fails to produce an item that is 100% 'correct', such as an incorrect algorithm in both the command and monitor part of a system which allows failures to propagate since they are undetected. These errors can defeat the voting function, causing the system to fail without any recognition of the error, i.e. if similar hardware and software are used for comparison purposes to detect errors. These errors are a major concern for system safety. They are generally caused by the improper specification / design / manufacture of system components.

Transient Failure

Transient errors can quickly degrade system resources to an unacceptable level unless handled correctly. Discrimination between transient and permanent error conditions is necessary, preferably through a technique of graceful degradation, and by using procedures where a fault must be present for a number of frames for it to be classed as an error. This is because 'good' resources must not be failed on the basis of one error.

Latent Failures

The ability of a system to detect failures and mask errors depends on a majority of resources being healthy. A latent failure is where faults are allowed to accumulate without detection, and they may manifest themselves at a later date in a simultaneous manner. A particular aircraft manoeuvre may activate particular faults, resulting in system failure.

Because of the complexity of the processor and its memory devices, it becomes increasingly difficult to show when and if a single fault will reach the comparator and be detected [7]. Under these conditions, it is possible for faults to accumulate within a processor such that when a particular fault propagates to the comparator, faults have

occurred in more than one redundant channel. The latency period may have allowed faults to accumulate in another channel, resulting in premature system failure.

Physical Damage

Inadequate functional distribution could cause total system failure, even if minor damage occurs to part of the system. e.g. the DC-10 disaster at Sioux City, where one failure caused all of the aircraft hydraulics to be lost. Therefore critical components must be sufficiently segregated such that a failure would not completely destroy one particular system. This is already taken into account when designing aircraft electrical and hydraulic systems so that a fan disk-burst does not take out all of the critical systems of one particular type.

Single Point Failure

This is a failure type where a whole system will fail if one component in that system fails [8].For example, a voting algorithm for selecting actuator command values may give a single point failure since if it fails then that actuator may also fail.

2.3 Reliability Assessment

In order to verify that the requirements are being met, it is necessary to use methods such as Fault Tree Analysis (FTA), Functional Hazard Assessment (FHA) and Failure Modes and Effects Analysis (FMEA). Many of these available methods initially originated in the nuclear power industry for safety analysis of nuclear power plants. Their use has subsequently been approved by the regulating aviation bodies for avionics certification. FTA, when applied to avionics, can serve several functions, including ensuring that the failure of one single component cannot cause the entire system to fail, identifying critical modules in critical functions and verifying the adequacy of fault detection and recovery schemes. These methods give a very high level approach, but are not suitable for reconfigurable systems and ultra-reliable systems, where other methods must be used.

2.3.1 Probability Calculations

To achieve reliability, the computing tasks are usually replicated to form redundant computing lanes [18]. Inter-lane redundancy management, based on output commands comparison, is generally used to identify the failed lane by output comparison. Thus, by adopting this philosophy, and if the system degrades gracefully, it can be said that (N-2) failures can be survived by a (N) lane system. This ensures that two lanes are still fully functional, and therefore disagreement between them can be tested for. This type of testing can be done to an initial approximation with probability calculations and FTA. These calculations enable the approximate reliability to be derived based on the reliabilities of the individual components. See Appendix A for more detail concerning these calculations.

Examples for a military transport aircraft are available as part of a MSc Thesis at Cranfield University [19,20,21]. According to Bleeg [3], the failures of the different system components (actuators, flight control computers, hydraulic supply, electrical bus, data bus) should be about equal, and the effects due to the failures should also be approximately the same. This implies that no one component is required to be ultra-reliable to compensate for the rest being less reliable, therefore there should be a cost benefit, and the effect of individual failures depends less on the individual component that has failed. However, this would require appraisal on a case-by-case basis.

2.3.2 Flight Control System Architecture Analysis

A brief analysis was carried out to evaluate how the system reliability changed when the system architecture was varied. In order to do this, simple calculations were carried out on a spreadsheet. The qualitative points are interesting, and point to some very useful design considerations. This analysis was completed from a hardware point-of-view. It was assumed that the relationship between the reliability of the system components and time is an inverse-exponential relationship, see Appendix A. It is also assumed that the components fail cleanly and absolutely, i.e. the value for fault coverage, C, is unity.

For the purposes of this analysis, a lane is a processor which performs a particular processing task. A channel represents a flight control computer (FCC), which is comprised of a number of lanes, and there will be a number of channels in the overall flight control system.

Number of Channels

For the analysis, the number of channels or flight control computers was varied between one and five. For the cases where the number of lanes was small, i.e. two, there was a continual improvement in reliability as the number of flight control computers increased from one to five for a given number of lanes per computer. However, with three or more lanes per channel, the reliability improvements were small as the number of computers was increased above two. Hence there is a trade-off between the number of lanes and the number of flight control computers. Analysis showed that as the number of lanes increases above eight, the distribution of the lanes is not important, i.e. whether there are four lanes in two channels or two lanes in four channels. For four to eight lanes, the system reliability can be maximised as there are at least three lanes in each channel. This assumes that there is no redundancy to allow for dispatch with failures.

The following conclusions were made :

1. For three or more lanes per channel, the difference in reliability between having two or three channels is small compared to the difference in reliability between having one or two channels in total.
2. For configurations with more than eight lanes in total, the division of the lanes between the channels has little effect on the overall system reliability.
3. Having two channels with four lanes is better than having four channels with two lanes as a failed lane in the former system would not result in the complete channel, including its other good lanes, being declared failed.

There are formal proofs that a duplex system cannot be designed so that single point failures do not occur [11], i.e. with perfect coverage so that faults will be detected, isolated and recovered from perfectly, since the system cannot be guaranteed to detect which is the failed processor and switch to the second all of the time. There are also formal proofs which show that more complex systems can be designed with this feature. Therefore the ideal flight control system will be of greater redundancy than duplex.

It is necessary to distinguish between the number of lanes and channels required for safety, and the number required for dispatchability and maintenance considerations. This is highlighted by the Boeing 777, where there are three flight control computers, each with three lanes. The Boeing 777 can be dispatched for a short period with one flight control computer unserviceable, and dispatched permanently with one lane unserviceable. Therefore the requirement for dispatch with failures has increased the number of lanes. This dispatch requirement is reasonable as it allows the maintenance to be delayed until the aircraft is booked for planned maintenance, and therefore no revenue is lost due to the aircraft being out of service. Airlines are now placing this as a requirement for future aircraft. Therefore the proposed requirement is that the system should be able to be dispatched with one computer failed for a period of one month, or approximately 300 hours flying time.

Number of Lanes per Channel

When considering the number of lanes required within a given architecture, the following assumptions are made;

- The minimum number of lanes required has been assumed to be two,
- Lane failure has a coverage of 100%.

Two lanes has been taken to be the minimum since this allows the outputs from the two lanes to be compared for failure detection. Therefore two out of N lanes are required, N being the number available within each flight control computer. The reliability of the channel rapidly increases when the number of processing lanes increases from two to three, but after this point, the relative increase in reliability for an ultra-reliable system diminishes with additional lanes. This is due to the fact that a two lane system will be 'fail passive', i.e. one failure will result in the system failing whereas a three lane

system will be 'fail operational, fail passive', where one failure can be tolerated before a second failure causes the system to fail. A low likelihood of lane failure therefore reduces the benefits.

The requirement for reconfiguration has an effect on the number of lanes per channel. Computing channels generally have two active lanes, one command lane and one monitor lane, and then the rest of the lanes within that channel are on standby until one of the active lanes fails. Therefore every lane within the computer has to be able to adopt either a command or a monitor function.

However, a system with two lanes does not have to be reconfigurable. This is because failure of one lane will result in one lane remaining, which is not sufficient to perform all of the command and monitoring functions since failures may not be detected. Therefore the computing hardware, software, error detection and reconfiguration within the two lanes should be simpler, resulting in a simpler and more economic design. This command-monitor arrangement is generally known as duplex-monitoring. It is usually taken that the software in the command and monitor computers is written by different teams to avoid common mode errors, or faults that are common to both systems and might not be detected. A benefit is obtained by increasing the dissimilarity by using two different processor types since common mode faults, which may exist within a single processor type, can be detected more easily.

With a flight control computer with three or more lanes, the system is more complex. Each lane has to be able to either adopt the command, monitoring or standby function. Therefore reconfiguration must be possible, which adds a computational overhead, and the system is therefore more difficult to analyse, which will make it more expensive to certify due to the increased testing requirement. However it does have the advantage that loosing a single lane within a computer does not result in the whole computer being declared failed, and therefore for some architectures it might be an advantage.

Actuator Control

This refers to how the computers signal the actuators. There are two main choices, either having the actuators in parallel with the flight control computers, i.e. with any flight control computer being able to command any of the actuators, or serial, where a specific flight control computer can only address specific actuator. Analysis showed that the parallel configuration was less failure prone than the serial version. However, this assumes that there are at least two FCCs, as the two configurations are obviously the same for a single FCC. Where there are three FCCs or more, the analysis shows that there is little difference in the relative reliabilities of the two systems. The reliability of the serial system approaches that of the parallel system as the reliability of the flight control computer / actuator electronics interface increases, so that when the reliability of the actuator electronics is high, there is not a great difference between the two different systems. The reliability considerations can therefore be broken down into the reliability of the FCC themselves, the number of individual FCCs and how they address the individual actuators, and the reliability of the overall system.

In conclusion, there is not a great difference between the reliability of the parallel and serial systems, especially when the overall reliability of the actuator electronics is high. Having the units in series has other advantages, as it provides greater effective segregation of the different channels, as opposed to having a common path, which is advantageous from a fault tolerance point-of-view.

2.4 Ultra-Reliable Systems Hardware considerations

The considerations when designing ultra-reliable hardware components are considered in this section. Reliability modelling techniques such as FTA are satisfactory for validating the failure probabilities due to random hardware failures, given that accurate component failure rate data is available, and ignoring reconfiguration faults [11]. The primary obstacle in the validation of ultra-reliable systems concerns design faults in functionality, not random hardware failures. With random hardware failures, failures are assumed to be independent in electrically isolated redundant channels, and the replicated units greatly increase the overall system reliability prediction. However, if a generic or common mode error exists, this may cause the system to fail, unless dissimilarity exists.

A commonly stated requirement for flight control systems of commercial aircraft is a probability of catastrophic failure no greater than 10^{-9} per mission [11]. This is clearly outside the region where black box testing is feasible since many years continuos testing would be required to produce reliability figures with a high degree of accuracy. Therefore analytical techniques must be used to demonstrate that a system meets the failure requirements.

As current technologies cannot manufacture electronic devices with low enough failure rates to meet the current requirements, fault-tolerant strategies must be used to ensure that the system continues to operate fully in the presence of component failures. The first requirement is therefore to calculate the reliability of the system architecture that is designed to tolerate physical failures. This leads to a stochastic model of the fault arrival and fault recovery of the system. Such models depend on the correctness of the hardware which implements the fault-tolerance of the system. For example, if a redundancy management system improperly diagnoses a good processor as failed, or a voter selects a faulty value then the assumptions of the reliability model may be invalidated. Thus the second subtask must not only establish the absence of errors in the control laws and their implementation in both hardware and software, but also the absence of errors in the algorithm and requirements on which the software is based. Since this cannot be performed through testing, analytical methods must be used using concepts such as 'design for validation' (see section 2.4.3).

Therefore there are two main considerations. The first is physical failure probabilities of both the hardware and software, which was considered partly in the last section, and is briefly considered in this section. The second is design error, which is examined in this section.

2.4.1 Synchronisation

Clock synchronisation can cause problems with flight control system design, as mentioned above, especially as these systems are particularly sensitive to electromagnetic interference, and 'Byzantine Generals Problems' [5]. A plausibly simple approach to redundancy management is asynchronous design [8], where the channels operate independently of each other. However, with an asynchronous design, there may be problems due to computers sampling given sensors at different times, thus introducing differences between outputs that can be compounded quite significantly by the control law gains. Another adverse effect of asynchronous systems occurs when the control laws contain decision points [14]. Here, sensor noise and sampling skew may cause independent channels to take different paths at decision points, i.e. mode switching does not occur simultaneously in different channels, and to produce widely differing outputs.

A good example of the problems with an asynchronous system is the AFTI F-16. During ground qualifications, it was found that differences in sensor values in different channels due to asynchronous sampling caused channels to be declared failed when no failure had occurred. Hence the threshold algorithm had to allow for a wide variety of different values to cope with this, resulting in the thresholds being set at a relatively large value, up to 20% of the total command throw, and in some cases the control law gains being reduced [14]. This increased the capability for fault latency to occur, and also allowed a failing sensor to drag the system down quite a long way before the failure was discovered, primarily due to the larger error thresholds. At the point of detection, the average of the acceptable values will change with a 'thump' as the faulty value is removed due to the large difference between the correct and faulty values, with an adverse effect on the aircraft's handling. A problem with control law switching points occurred on flight 44, where each channel of the Digital Flight Control System (DFCS) declared the others failed since there was disagreement at a switching point. Voting with ad-hoc synchronisation was therefore introduced at the software switching points which cured the problem. A number of Byzantine synchronisation fault-tolerant algorithms are now available.

2.4.2 Processing Distribution

There are several choices which can be made with respect to processing distribution, generally either a centralised or distributed system. A distributed system is characterised by multiple processors throughout the aircraft, with each being assigned computing tasks on a real-time basis as a function of mission or system status. Processing is also performed at sensors and actuators. A centralised architecture is an architecture design where computation takes place essentially in one computer or several computers in one Line Replaceable Unit. A fault-tolerant distributed system can be better than centralised system [22]. For example, these benefits include functional integration, parallel computing, graceful performance growth, selective technology upgrade, appropriate levels of functional reliability, graceful degradation of system in the presence of faults and effective hardware resource utilisation. However, these

benefits apply to the aircraft system as a whole, of which the flight control system is one part, and there can be disadvantages such as lack of individual system separation and the greatly increased complexity. In practice, many of the benefits are not applicable to the flight control system by itself since it is a system which has a high level of reliability and redundancy throughout, and has little requirement to be selectively upgradable. Therefore the flight control system should fit into an overall distributed system, but it is better suited as a centralised system since this type of system is simpler to implement, does not have high data transfer requirements and is easier to diagnose and certify.

The redundancy in a system should depend on the function of the system. Critical systems should be triplex where less critical systems should be duplex and non-critical systems should be simplex [9]. This provides for efficient use of hardware resources, but has mixed or graded redundancy. Using the idea of a distributed architecture, the individual systems, such as flight control, flight guidance and engine monitoring could therefore have their own appropriate level of redundancy.

A federated system is where each major system shares input data from common hardware and then shares the results over the databuses. However, these systems do not support many of the features of distributed systems due to the rigidity of allocation of processing to sites and the low amount of information sharing between processing sites [22]. To provide these functions, it is necessary that functions located at different processing sites be able to communicate with each other at high speed and high integrity. This can place a severe requirement on data processing and therefore the overall aircraft avionics system should be designed so that only the vital information is communicated through the aircraft.

System Monitoring

System monitoring devices can be used to improve the probability of detecting failures within individual processing elements [22]. If there are two primary processors, with one being active and the other in standby mode, they can monitor health messages generated by each other. In the event of a failure in the active processor, the backup processor can take-over and assume responsibility for the processing task. The fault detection / failure coverage is therefore dependent on the state of the backup processor. Fault coverage can be improved by adding a separate system monitor, which can monitor both of the processors, and therefore participate actively in the decision to promote the backup resource to replace the active one. This increases the system monitoring complexity though, which must also be taken into account in the processing pair. The system monitor can also command processing checks when system demands are light, in order to carry out a more thorough built-in check to determine if faults which are more difficult to detect, such as latent faults are present. However, the coverage demands of the initial system compared to the intelligent system monitor are the same, and the same problems exist with ensuring adequate fault detection and isolation. Detection and recovery from software faults is not improved either. There can also be problems with promoting a faulty processor with latent faults after another processor has been declared failed.

Distributed recovery can be implemented by processing outputs from systems at the devices which use the data. Users of the data receive all output from all of the processors, and then use a software routine to accept data which correlates within acceptable limits, or to reject data that does not comply. The output device processors also receive health information about the other processors, and can request such information if they believe a given processor has failed. However, the communication media is placed under an increased strain with the duplicated output data and health data being transported. Also, the required processing at the terminal devices lowers their reliability, and an increased system monitoring function is also required. This system monitoring could be extended to the sensor monitoring to detect sensor failures, if required.

The reliability advantages of an architectural approach like this are great. Failure detection, isolation and recovery occur automatically at the level of the processor using the data. Transients may cause problems, but processors suffering from transients may be brought back into service at a later time as long as the required health routines are performed and the system checks out. The system monitor can keep track of this, and report it for later investigation. Therefore higher coverage is achievable with this approach since fault detection is external to the fault source.

The use of distributed fault recovery places restraints on the system design and sizing. System processors need to be more powerful so that system throughput is greater, and the system time delay is not increased. System architectures can be made inherently reliable if the designer is careful in assigning responsibility to the various processing elements throughout the system. This approach is primarily used where switching or reconfiguration is used. However a system with no hardware reconfiguration is simpler, and would not benefit from distributed processing as much. System monitoring is still desirable since it facilitates the error detection process, and gives increased fault coverage.

2.4.3 Formal Methods

Formal methods are the use of mathematical techniques in the design and analysis of computer hardware and/or software. In particular, formal methods allow the properties of a computer system to be predicted from a mathematical model of the system by a process similar to calculation [5]. They confront the discrete behaviour of computer systems by using discrete mathematics to model it. The proofs they use are based on mathematical induction, and therefore a very large number of possible behaviours are fully covered in a finite proof.

They are powerful system design and analysis techniques for two reasons. Firstly, the formal method provides a degree of confidence in the correctness of the system that is impossible with less formal methods. Secondly and more importantly, the use of formal methods forces the system designer to keep the design simple and modular enough to enable it to be rigorously analysed. Formal methods also enable the

subsystem interactions to be formally verified, and subsystems which are affected can subsequently be re-analysed in order to be re-proven.

Formal models are therefore implemented and tested using the formal methods. Formal models often assume that the architecture is Byzantine fault-tolerant [8]. There are also tight constraints on voting patterns and computational frame characteristics in these models. It is thought that formal methods such as design for validation will be common practice for civil flight control system applications in the foreseeable period [11]. This design for validation technique should be used for both software and hardware design.

Design for Validation

Validation is defined as 'the process of determining that the *requirements* are the *correct requirements*, and that they are complete', and verification as 'the evaluation of the results of a process to ensure correctness and consistency with respect to the inputs and standard(s) provided to that process.' [5] These can be informally characterised as 'validation is showing you got the requirements right', and 'verification as showing you built the system according to the requirements'. The design-for-validation concept consists of the following:

1. The system is designed so that a complete and accurate reliability model can be constructed. All parameters that cannot be derived must be measured.
2. During the design process, trade-offs are made in favour of designs that minimise the number of measurable parameters in order to reduce the validation cost.
3. The system is designed in a manner which enables proof of correctness for its logical structure.
4. The reliability model is shown to be analytically accurate with reference to the modelled system's implementation.

2.5 Software

Software is another major area where there is a large potential for faults, and therefore it must be designed in the same formal way as hardware. Traditional approaches to software design have tended to ignore the potential for software errors. Careful consideration of fault detection, isolation and recovery demands requirements for a given hardware / software architecture combination can minimise the cost of redundant system architectures while still ensuring high availability.

The concept of different versions of software which have the same function is called design diversity, and has been applied to software, as well as hardware. It is generally accepted that design diversity can result in increased reliability, but it is not possible to quantify the increase in the ultra-reliable regime. This leaves us with the problem that we cannot formally test the 'correctness' of each system. Hence they all have to be analysed individually, and when this process is complete, the system design is assumed to be correct for all subsequent analyses. However, research has indicated that multi-version software may not provide as high software coverage as output comparison

techniques provide for hardware coverage due to the potential for identical software specification or implementation errors. Research has shown that this is true for software created by different programmers in different computer languages, i.e. programmers tend to make the same kind of mistakes.

2.6 Testing

This section briefly outlines the key principles behind system testing, which have been summarised from [14]. They can be applied to the complete system, as well as the individual subsystems.

1. Incorrect fault detection, resulting in inappropriate loss of system redundancy is unacceptable. The system should be tested with values that represent the minimum, maximum, maximum rates of change, maximum frequency response and noise as examples.
2. Redundant system designs which use voting and cross channel comparisons must operate on congruent input data sets to avoid incorrect failure detection. This implies problems with asynchronous systems.
3. Fault-tolerant system designs must be evaluated for sensitivity to sensor noise.
4. Failure probabilities should be given for the different mission phases and functions performed by the system. This can help to prevent the designer from under- or over-designing the system.
5. Reliability requirements need to address the software by identifying the testing methods and tools to be used. The key to software reliability is not found in the failure rate, but in the examination of the methods and tools used to ensure proper functionality. The software's life cycle of specification, design and test must be specified such that testing is traceable to the requirements, and proper functionality is shown.
6. Requirements for an independent backup should include
   a) method for detecting the need for a transition to the backup, whether manual or automatic
   b) allowable transition periods or transients
   c) functional requirements of backup, such as operating envelope or reliability. If the backup is going to be flight tested, re-engagement of the primary system must be addressed.
7. Failure transients should be specified in terms of the resulting aerodynamic and structural effects.
8. An integrated design tool which addresses control laws, fault tolerance, hardware and software is needed for fault tolerant control systems.
9. When designing interfaces, the criticality of the information being passed must be considered. This requires a detailed understanding of the importance of the information being passed.
10. The redundancy in an interface must be based on the criticality of the information and the possible failure modes.

11. A fault-tolerant system, which uses cross-channel voting to detect failures, should avoid random, unmeasurable design characteristics, such as asynchronous channel operation. This helps to keep failure transients at low levels, and minimises unexpected interactions that can result from incongruent data sets.
12. The fault-tolerant design should be transparent to the control law functions. The control laws should not be tailored to the system's redundancy level.

2.7 Examples of Fault-tolerant systems

This section will highlight two brief examples of systems and how fault tolerance effects them.

2.7.1 AFTI F-16

With the AFTI F-16 [8], failures are detected in different ways, depending on the system state. For no failures, i.e. three working flight control computers in this case, consensus is used to isolate the defective computer. For detecting the second failure, a built-in test routine in each computer is used. Failures can be isolated within the individual computers. For example, the situation can arise when three or more surface position calculations have failed within a computer, and therefore that computer has been declared failed yet the input/output communications are still working, and therefore the computer can still transmit sensor data to the other channels. Second failures are resolved by the use of knowledge built into the system and was demonstrated by failure modes and effects testing. However, there is evidence that the redundancy management system can become the prime source of faults in the DFCS if it is sufficiently complex - the AFTI F-16 programme showed this.

2.7.2 MAFT (Multi-Lane Architecture Failure Tolerant)

MAFT [17] is a multi-lane architecture suitable for real-time control applications requiring high reliability. It has been applied to the design of a digital flight control system (DFCS) having a failure probability of 10^{-10} failures per hour for a 10 hour mission. MAFT can support design diversity in both software and hardware to guard against generic faults. The partitioning of a MAFT system can be seen on Figure 1.

An advanced distributed processing architecture has enabled failures to be identified at a sub-function level. This is done by partitioning software tasks within a lane into application and system overheads. Databuses then connect the system overhead components of the system which control voting, error detection, reconfiguration, synchronisation and task scheduling. A different set of data buses connect the application programmes, with data for the sensors and actuators being transmitted on them. The system overhead handles the routines for fault tolerance and system management.

This type of system has several advantages. The functions of the system overhead part are transparent to the applications computer and therefore the two can be designed by separate teams, the applications part by the applications engineer, and the overhead part by people more familiar with fault tolerance techniques.

Instead of having redundancy within a channel, MAFT globalises the redundancy to achieve the same effect in a distributed manner. The system is designed to be inherently symmetric by the use of broadcast media, i.e. broadcast links from one to many instead of direct links from one to one, and therefore it is less susceptible to asymmetric failures, such as the Byzantine Generals Problem. Since the system is structured for global verification, a means already exists for re-broadcasting the required information, and reaching agreement with an interactive consistency algorithm.

Common mode errors are addressed by the use of loose system synchronisation (since exact synchronisation is not required), multiple version software and physical distribution. Exact synchronisation is not necessary because the processors can react to data as soon as they receive it as opposed to having to wait for all the data, for example the results of the calculations from the other processors, to arrive at once. Loose system synchronisation means that noise will not affect all signals, in the same way, and therefore will be detectable since the synchronisation is not exact. Distributing processes in hardware and in time improve MAFT's resilience to common mode failures. Transient failures are handled with a flexible penalty weighting scheme, which essentially allows graceful degradation and re-admission. Latent failures are reduced by a comprehensive self-test strategy which is also based on global verification.

3. System Requirements & Design Implications

For Avionic systems, there are several regulations which are relevant within the Joint Airworthiness Requirements (JARs) [6]. For the hardware requirements, the most relevant is JAR 25.1309 Equipment, Systems and Installation [6]. This JAR is concerned with the likelihood of occurrence of failures, the provision of warnings to the crew, and the analysis of these failures, coupled with the demonstration that the aircraft meets these requirements. There are also other requirements which cover more detailed parts of the design, such as circuit protection devices in the aircraft electrical system, and these must also be complied with. This section has considered solely the hardware and its reliability and no analysis has been made of the control laws here.

References such as [23] which detail work done on the Boeing 7J7 have been consulted, an aircraft which never got past the drawing board, but whose flight control system was developed into the Boeing 777 system. The broad system requirements have been listed under the appropriate requirements.

3.1 Functional Requirements and Implications

The key requirements are listed as follows. The probability of loss of function for flight control computing due to random failures, generic errors or common mode faults must be less than 10^{-10} per flight hour, in order to ensure a 10^{-9} per hour reliability for the overall aircraft [3,11]. Also, it shall be assumed that components that are not 100% analysable and testable are subject to generic errors or common mode faults. This extremely high integrity requirement can only be met by the use of fault-tolerant avionics than can survive random hardware failures as well as generic faults which may manifest in the hardware or software. The probability of single or combined system failures which can prevent continued safe flight and landing shall be less than 10^{-9} per flight hour.

Other requirements that have been recommended concern failure transients, and are as follows [18]. The probability that any control surface shall be faulty without being recognised by the flight control system for greater than 80 ms shall be 10^{-10} per flight hour. The probability of loss or failure of the fly-by-wire system due to a random failure in the primary flight control system shall be less than 10^{-10} per hour. The system shall be capable of surviving a generic failure case which might occur, either in the hardware of software. Maintenance is a consideration as well since it has been determined that a system may require maintenance from time to time, and being able to defer the maintenance will minimise the cost of ownership.

All fault and redundancy management within the functions shall be automatic if the crew do not have any way of resetting this system. Any required maintenance functions shall be provided, and required interfaces supplied for the on-board maintenance system, if one is fitted. Performance requirements relative to failures are dependent on the degree of control performance degradation permitted, aircraft transient disturbances and frequencies of occurrence. Work performed by McDonnell Douglas has identified

the required handling level for given failures [24,25]. Bleeg [3] suggests that failures in the following control modes should be no worse than the following probabilities of failure per flight hour.

Normal	10^{-7} per hour
Reversionary	10^{-9} per hour (design requirement for whole aircraft)
Direct Coupled	10^{-10} per hour

It can be seen that the critical failure probability is 10^{-9} per hour which is the level that must not be exceeded for a catastrophic failure. Therefore the probability of having to use a direct-coupled control law before the aircraft 'fails' at its designed failure rate of 10^{-9} per hour is extremely low. This implies a high level of reliability within the flight control system, with the direct law providing a 'final backup' when everything else has failed, or circumstances which have not been predicted have arisen. A never-give-up strategy should be adopted which addresses the situation when the primary flight control system degrades below the minimum operational condition. The never-give-up strategy provides a high probability of keeping the flight control system active when there are good reasons, guarding against false condemnation of good resources and recovering from false condemnations or temporary faults by bringing a failed resource back on line if it checks out. Since this strategy encompasses requirements outside normal operational requirements, failure probabilities are not given. However, it should not compromise system performance, and the previous requirements still have to be met.

Critical systems shall remain functional after a generic fault [3]. Reduced or degraded capacity is permitted, but continued safe flight and landing is required. Failure of non-critical functions shall not affect critical functions, which implies functional segregation for systems with different levels of criticality. Functional partitioning between critical and essential systems shall be maintained. Essential systems shall at worst fail-passive in response to a generic fault. No single fault shall cause the flight control system to degrade below the minimum operational level. According to Bleeg [3], the probability of an active failure of the primary flight control system shall be less than 10^{-5} per flight hour when operating within a minimum operational configuration. However these figures reflect the views of Boeing, Airbus fly-by-wire aircraft still have the same overall system reliability, but accept that the aircraft may enter an alternate control law earlier, especially with deferred maintenance. However, even with deferred maintenance, the probability of an Airbus operating under an alternate control law is low.

Redundancy is required for reliability of functions. A single thread reliability of 10^{-4} to 10^{-5} is suitable, giving a mean time between failures of 10,000 to 100,000 hours. Dissimilarity is required within the flight control system for common mode/ generic error protection. Physical separation is required in the event of mechanical damage. Electrical power separation is required in the event of power failure. Data sharing is required. This has the advantage that a complete set of redundant resources is available to each lane. However, this is more complex to implement, and common mode failures

must be guarded against. This minimises the complexity of input interfaces with the flight control computers if databuses are used. Finally, graceful degradation should be used in the event of failures.

3.2 Design Guidelines

This section will highlight the design guidelines which will enable the functional requirements to be adhered to.

3.2.1 General

The major design considerations have been grouped into their respective sub-headings. These specific requirements have been formulated from a literature survey, and therefore represent the views of different people from different organisations. Therefore their use should be as a starting point as opposed to an absolute list which has to be adhered to.

Technology

The system should be capable of expansion for future needs, with the software having the capability of being easily upgradable by the airlines without requiring certification to allow it to be tailored to their own needs. This is more relevant to maintenance functions and built in checklists as opposed to flight control software.

High tech seems advantageous, but only technology that gives an advantage should be used. As simple as possible is good since it enables the development, certification and maintenance processes to be as inexpensive as possible. Individual systems should also be able to withstand any two failures without loss of function, though some degradation is acceptable. However, this degradation should be graceful to enable it to be well controlled by the pilot.

Functional Partitions

Vital elements of the flight control system must be located away from each other. E.g., in the 7J7, the ACEs must be divided between the forward and aft electronics bays.

Critical, essential and non-essential functions shall be separated by the greatest extent possible. Functions should be partitioned so as to allow incremental validation during the test cycle rather than having to rely on flight test. Functions should be partitioned to minimise the impact of airframe or engine changes during or after flight test.

Physical Considerations

There is a need to guard against physical damage, terrorism etc. This can be accomplished with separate electronics bays. However, failures only need to be withstood up to structural limits - i.e. all critical hardware needs to be within the critical structure. Component locations, separations, and capabilities are to be selected to assure that despite damage, if the aircraft is flyable, is remains controllable. The ability for critical functions to support continued safe flight and landing under the assumption that components within any spherical five foot sphere may be destroyed is also desirable.

Dispatch Requirements

For a particular flight control system, the required mandatory minimum equipment list (MMEL) shall be provided and defines the required hardware which must be available at the start of a flight in order to achieve acceptable performance, functional, and safety requirements.

System Interface Considerations

The need for independence or availability dictates the considerations for duplication of functions. However, functions are to be partitioned in such a way as to minimise data and control flows. The flight critical, essential and non-essential services should also be separate. This should improve the reliability of flight critical communication systems since they have the minimum number of subscribers. This also gives economies since more rigorous testing requirements are generally specified for flight critical systems than for essential systems, and therefore the essential systems need not go through such a long and rigorous testing procedure.

For a system with databuses there are other considerations. A command path outside the databuses is desirable if there are questions concerning the databus reliability, especially if all the databuses are susceptible to common mode failures. This would mean that there is still a command path in the event of the buses failing.

Databuses are expensive to develop, but once standards have been established, they are useful. MIL-STD-1553B is not considered suitable for civil applications since it requires a bus controller, which is a weak link in the chain and this type of bus is also difficult to expand. ARINC 429 is suitable for mono-directional applications where cross talk is not required, but can otherwise be limited. ARINC 629 is more complex, but is bi-directional, flexible and upgradable and can have benefits, especially in large aircraft, where wire lengths can become significant. However, the more complex standards, such as ARINC 629 should not be used unless they can be shown to be more effective than alternative systems when evaluated on a on a case by case basis.

Transient Disturbances

Fault tolerant features should be included to minimise or preclude transient disturbances resulting from sensor or internal flight control computer failure. This includes providing for automatic fault detection and appropriate reconfiguration. The level of transient disturbances, i.e. their magnitude and persistence, and the handling qualities rating should be related to their likelihood of occurrence.

Technical/ Programme economic and risk considerations

There shall be no technology uncertainties that could have a major impact later in the technical programme. With the advent of concurrent engineering, much design and development takes place in parallel, and therefore the architecture shall not be sensitive to reasonable variations in aircraft aerodynamic or structural characteristics. Airlines are now demanding a decrease in maintenance costs, combined with an increased period between maintenance actions. Hence fault tracing is mandatory for complex systems, and maintenance functions have become commonplace. However, the maintenance functions should not interfere with the flight critical systems.

3.3 Specific System Requirements

This section indicates how the requirements may be adhered to by the different aircraft systems.

3.3.1 Power Supply Systems

These systems include pneumatic, electrical and hydraulic systems, although the pneumatic system will not be considered here since it plays little part in flight control.

Electrical System

According to Glashagen [26], the current types of AC electrical generation are suitable, and the costs of ownership do not warrant a transfer to a radical new system, particularly if the system has not yet matured. There is also a generally acknowledged need to sustain sufficient power for 60 minutes from batteries. Supply to the flight control system and autoland needs to be uninterrupted under engine failure and transient loads situations, with no-break power transfers.

A dedicated APU start battery should be provided for large aircraft, and there should also be a non-time limited standby source available, e.g. powered by a Ram Air Turbine (RAT) or other similar non time-limited source. For a two crew cockpit, the systems that are required to be operated in the short term after a failure should be automatic except for APU start and external power connection in order to achieve an acceptable workload under failure conditions. Other considerations are for Extended Range Twin-jet Operations (ETOPS), maintenance, and compatibility with existing ground power sources, which may require multiple ground power sources for a large aircraft.

This should ensure that the JAR requirements [6] are met. The electrical power requirement for extended range twin-jet operations (ETOPS) is for sufficient power availability to supply services necessary for continued safe flight to an alternate destination without requiring exceptional piloting skills with one engine out coupled with the loss of another source of power. This requires three independent power sources, any one of which can support the required services for the maximum diversion time.

Hydraulic System

The hydraulic distribution should be such that the control between the various control axes is split between the different hydraulic systems in approximately equal proportions, meaning that there will not be a critical system, therefore the loss of functionality is more or less independent of the system lost. Also, the loss should not significantly degrade mission capability, i.e. the aircraft should be able to continue on to its planned destination with little loss of capability, under the same operating procedures. For an aircraft with three hydraulic systems, no more than two hydraulic supplies must be routed beyond critical structure so that not all of the hydraulic power is lost in the event of non-critical damage to the aircraft structure.

The system should be able to withstand any two failures, i.e. for a three system aircraft, any one system should be capable of operating the aircraft safely, assuming no other failures. In the light of the Sioux City DC-10 accident, hydraulic fuses should be fitted in areas susceptible to fan disk burst or other similar damage so that a system is not drained in the event of failure. This also means that non-critical parts of the structure should be protected from system breaks by hydraulic fuses and flow monitoring.

Each system should have sufficient power sources to meet the maximum requirements under normal operating conditions, which may mean that several sources are required. Hence the sources for each system should be scheduled in order that fluctuating requirements can be catered for automatically. The system should also have the ability to be powered by the RAT alone, with critical large users, such as the landing gear having an alternate means of power, such as mechanical 'drop-down' to cater for situations where the non-time limited source is required.

3.3.2 Flight Control System

Ideally, the aircraft should remain under control with all combinations of non flight-critical structure destroyed. However, in practice, the structural failure probabilities should also be considered, and failure which is deemed to be less likely than 10^{-10} per hour can effectively be ignored.

Transients should be protected against, up to a controllable level, the allowable limit depending on the probability of occurrence. In practice, this implies a limit on how bad the handling qualities are permitted to degrade to for a given failure probability. The McDonnell Douglas work on failure and handling qualities is one way of determining how good the aircraft handing qualities should be in an ideal situation with a given failure [24,25].

There should be adequate provision within the flight control system for control laws which cater for alternative and direct control laws. The case of loss of all computer controlled flight control also needs to be considered, either for a manual landing in the event of complete flight control system failure, or for a short period while the flight control system is brought back on line. In practice this implies some form of mechanical backup, with which the pilot can control the aircraft.

For analysis, the flight control system has been divided up into its respective components.

Actuation

When considering a direct control mode, i.e. where the inceptors are effectively connected directly to the control surfaces, there is little signal processing. Hence an option is to have a direct link from the inceptors to the actuators, which can be used when the flight control computers (FCCs) fail. Analysis of this system showed that it drastically improved the overall reliability of the system since the reliability is now essential independent of the reliability of the FCCs. The direct connection can also be a separate component of the actuator electronics unit itself, so that if the rest of the actuator control unit fails, there is still a connection between the inceptors and actuators. This type of system is very reliable, and is the most suitable way of obtaining a direct control law since it bypasses the most complex components in the flight control system. It also assists with certification, see section 5.3.6.

The actuation requirements are governed by the control requirements in terms of control power, slew rate and deflection limiting, and the reliability requirements in terms of redundancy in signalling and actuation. This implies multiple path signalling is required, and also multiple actuators may be required to avoid single point failures in the signalling part of a single system, and also to cope with excessive control surface loads or to resist flutter. However, the basic requirement of control of the aircraft with two hydraulic system failures still applies.

Under failure, the aircraft should not be put in a position where is it rendered uncontrollable by a control surface run-away. Hence failure detection is required, with a control surface having an auto-centring function in the event of failure of all actuation on that surface. A failed actuator should not hinder the operation of a working actuator, hence this must be taken into account.

Flight Control Computers

The safety and integrity requirements are likely to be met using a conventional design with two primary flight computers, each with triplex dissimilar lanes. However, in order to achieve the desired reliability goal, significant secondary fault tolerant capability is required in order to withstand random hardware failure, and to provide a dispatch with failures capability.

When considering the flight control computers, dissimilarity is good since it enables the systems to be protected from common mode and random faults, such as component failure. This can be either in the hardware, or software or both. There is also a need to have sufficient redundancy within the flight control system to enable the aircraft to be dispatched with some components failed. This is desirable from an operational point of view since it means that faults can be repaired at a later date when the aircraft is in for scheduled maintenance, and hence the airline flight schedule need not be disrupted.

Systems with similar hardware and different software are certifiable, but common mode failures are possible in the hardware, which may be difficult to detect. This must be borne in mind when designing a system. Having two dissimilar systems with similar hardware within each system is acceptable.

From the preceding points, and an analysis of the data generated by this study, it can be concluded that for a serial system (see section 2.3.2), the overall reliability is governed by the FCCs and by the actuation electronics. In practice, this means that for a system with three or more lanes in the FCCs, the system is much more sensitive to the reliabilities of the actuation electronics than of the individual lanes. With a parallel system, the overall reliability is sensitive to the reliabilities of the individual lanes and the actuation control electronics in approximately equal proportions. This tends to indicate that if the reliabilities of the actuation control electronics are low, then the parallel arrangement should be used. However, this has other disadvantages such as common paths within the architecture, and the lack of system separation compared to a serial system.

The AFTI F-16 has an independent backup unit (IBU) to cope with failure of the three primary channels in its flight control system since direct control laws, as used with civil aircraft, are not acceptable with this aircraft as it is unstable in pitch [14]. The independent backup unit study addressed the following issues.

1. How reliable the IBU should be, what redundancy level was needed, and if output command voting would be required.
2. What flight control performance was required of the IBU
3. What the engagement method should be.
4. How to minimise transients on engagement and disengagement of the IBU.

A triple level of redundancy was chosen, with a portion of one flight computer card in each of the three Digital Flight Computer System (DFCS) boxes being dedicated to the IBU. An output selector, which can select valid commands after a single failure was included for the horizontal tail to improve the system's fault tolerance in that axis. Space limitations within the computer prevented output selectors for all surface commands. The IBU was engaged manually or automatically. IBU tracking of the primary system for engagement purposes was rejected due to the requirement for independence since a failure in the primary system could not be allowed to affect the operation of the IBU by propagating into it. However the DFCS does track the IBU to minimise re-engagement transients to the DFCS. This was accomplished through the DFCS monitoring the IBU control surface commands, which was also done for built-in test and in-flight failure detection. The flight envelope where the IBU was capable of controlling the aircraft was smaller than the flight envelope of the DFCS, which could have caused problems if control had transferred to it near the edge of the flight envelope. During the flight trials, the IBU was not engaged as a result of a failure of the triplex DFCS.

Sensors

This section will briefly consider the various sensors and actuators on the aircraft, including the requirement for redundancy.

Sensors, such as position sensors used to monitor actuators and to sense the pilot demands, are inherently reliable compared to other components in the system. However, they could still cause a single point of failure, and must therefore be duplicated. Duplication can also help with system segregation since it ensures that the command paths to the systems are separated, which ensures that no failure within one FCC could be propagated back into a second FCC through a sensor.

With duplicated sensors, there is a desire to compare the outputs from duplicate sensors in order to detect failures. This monitoring could either be performed within the FCCs themselves or in a separate system monitoring unit. For synchronous systems, there is a desire to use the same sensor values for each processing channel which implies that all FCCs must receive all sensor values. However for an asynchronous system, this is not necessarily required, and therefore the monitoring can take place outside the individual channels, i.e. not all of the sensor values are required within all channels as long as sufficient are available for a comparison to be made.

It is desirable to monitor actuators closely. This ensures that the flight control channel is working as a whole, and that any failures within the actuator are quickly detected, which is a requirement to minimise the failure transient. The actuators should be monitored by the devices which control them, i.e. if there is a separate actuator control unit which drives the actuators then this should perform the actuator monitoring task. This gives the advantages of distributed processing, as highlighted in section 2.4.2, and also helps to minimise the amount of data flow around the avionics system. However,

any monitoring will increase the amount of data flow required, therefore it should be considered carefully during the design process.

Voting

A little thought reveals the essence of the problem concerning the interaction between voting strategies, task schedules and data dependencies [8]. For example, consider a particular actuator command. The requirement is for the majority-voted value to be equal to the 'correct' value, i.e. the value produced by a simplex processor with no faults. Clearly, if a majority of processors are working correctly at the time of the command, and if they receive the correct input values then this will be possible. Input values either come from sensors, and our requirement here is that all processors receive the same values, or the values are the outputs of previous tasks, which may or may not have been voted on. In the case of voted outputs from a number of FCCs, it is possible to return to the conditions that established the correctness of the voted outputs; in the case of non-voted outputs, the requirement is that the FCC is working correctly when the task executes, and the inputs were, in turn, correct at that point. Thus the voting algorithms used to fail systems must be arranged so that resources are not failed due to a faulty input to a working subsystem, which causes that subsystem to fail, and is available elsewhere within the complete system does not cause the subsystem to de declared failed.

Other ideas such as plural voting, where the majority wins, and the failed machines are not phased out have also been considered [8]. An alternate idea is to break the lock-step synchronisation that currently exists, whereby computers would still have to be synchronised to vote, but can perform the intervening tasks as they wish. This would mean that in the case of a system having a transient fault, the fault may affect several systems in a small way as opposed to knocking out one complete control dimension. For example, if lightning hits an aircraft with asynchronous channels where each channel is performing a different task, it may only affect one computer due to the point that that computer is in its computational cycle, and therefore only that particular function will be lost. The tasks may also be divided up non-symmetrically between the processors. For example, flight-critical tasks may run on all processors while a non-essential task may only run on one processor.

One of the most common routines that is used is mid-value voting. In the AFTI F-16 example considered [14], the channel selected to signal the aircraft actuators is a function of the failure state of the channel and hydraulic systems. In the non-failed state, the 'middle' channel's data is used, which minimises the errors between the different channel commands that would otherwise be detected by the actuators.

Flight Envelope Protections

Different philosophies exist concerning flight envelope protections. The exact philosophy varies, but it can either be hard, where the pilot is prevented absolutely from exceeding limits, or soft, where the pilot should be dissuaded from exceeding limits, but retains overall control, and can exceed the flight envelope if required. The desirable philosophy will depend on the implementation of the complete system such as inceptor and cockpit design and not just on the control laws, and therefore should be evaluated as such. Therefore this subject will not be pursued further in this report.

4. System Evaluation Methods

This section addresses how systems in general can be evaluated. The evaluation here will summarise the key points that must be considered when designing a flight control system. Not all of the issues will be considered in this report since some are more related to economic decisions. However, this list will be useful when considering the tasks that need to be done in order to design, build and certify a fly-by-wire flight control system.

4.1 System Hardware

There are many criteria against which the system hardware may be evaluated. The major areas that need be covered when evaluating systems have been listed here, in an appropriate order [27].

- Capability
- Reliability
- Maintainability
- Certificability
- Cost of Ownership
- Technical Risk
- Weight
- Power

Traditionally, the three most important factors are capability, reliability and maintainability. The most important is usually capability - can the hardware do the job that it was intended for? The task of the system designer is to maximise the system capability within the imposed constraints.

Reliability is one of the most important items since high reliability usually implies reduced maintenance, and hence reduced costs of ownership. However, there are times when this is not true; a system that is 'excessively' reliable may have large acquisition costs to offset the high research and development costs. Reliability also encompasses fault-tolerant design issues.

Maintainability is also of prime importance. Since a system will reach a point where it will require preventative or corrective maintenance, the ease with which faults can be detected and defective components replaced is critical. Hence built-in testing, hardware access and ease of replacement and automatic troubleshooting become very attractive options.

There are trade-off's between all of these key issues however. A system that is very reliable can be located in a relatively inaccessible place since it is less likely to need attention. Also, a system that is just capable of doing the job may well be much more attractive than a system that has a greater functional ability, but is more expensive to

acquire and requires more regular maintenance. Hence these issues will be considered when evaluating the systems presented in this report.

Certification is also an all-important requirement, and governs all facets of an aircraft's design. In order to expedite certification, the aircraft's avionics architecture should be straightforward and easily understood. The certification process concentrates on failure mode analysis, and how the aircraft performs under these conditions. A tried and tested architecture will be more readily certified than one that contains previously untried and uncertified technologies. Hence when considering the avionics architecture, the question of the 'newness' of the system must be considered.

Cost of ownership encompasses items such as initial purchase, spares acquisition, transportation and storage, training (for both air and ground personnel), hardware development and test, depreciation and interest. Achieving the optimum requires careful attention by the avionics designer and costing specialist.

A high technology solution may also be undesirable for the same reasons, since it will be expensive to both develop and certify. There will also be other risks such as time penalties and the risk that the technology may not work for the application in hand. Finally, weight and power requirements must be examined. Again, there will be trade-off's since a lightweight and low power consumption design may be less capable or reliable than a heavier design, and may be of higher cost.

4.2 System Software

The software will not be considered in this evaluation since it is beyond the scope of this report. The sections included above have been prepared to assist in the design process, and to bring their importance to the fore since the system software design and evaluation are a critical part of the design task.

4.3 Handling and Control Laws

Handling has an important role to play in system reliability since it can help or hinder the job of the pilot, and therefore affect the overall system reliability, i.e. the aircraft / pilot combination, when the aircraft is being flown under manual control. Therefore the suitability of the handling and control laws to the system should be considered, as well as the suitability of the handling to the task, and the effects of system degradation on the flying and handling qualities. However, this requires other factors, such as cockpit design to be taken into account.

5. Analysis of Aircraft Chosen

This section will consider how the aircraft compare to the individual requirements listed in the previous sections. The Airbus A320, A330, A340 and the Boeing 777 have been chosen for the analysis. Other fly-by-wire aircraft such as the McDonnell Douglas C-17 and Kawasaki Aska are descried in the appendices, but have not been included in this analysis due to the fact that they are optimised for a different task. The Avro Regional Jet description has also been included since this is a mechanically signalled regional aircraft. The descriptions of the aircraft can be found in Appendices C to H. The analysis will focus more on the functional aspects of the systems, such as the capability and reliability, and less on the more economic aspects such as cost. This is not due to the latter factors being less important, but reflects the focus of this report.

5.1 Technological

For the application of fly-by-wire technology to regional aircraft, there is no benefit for using much of the technology that has gone onto the latest large civil transport aircraft. This is because the economic benefits are reduced since the percentage of the cost of the fly by wire system has to be more or less constant with respect to the total aircraft cost, and therefore the actual cost per aircraft for the fly-by-wire system for the Generic Regional Aircraft must be reduced compared to the cost of a fly-by-wire system for a Boeing 777. Therefore the issues of functionality and redundancy must be carefully considered, and compromises made so that the system can be produced within the technological and economic constraints applied. The fly-by-wire system for this Generic Regional Aircraft will therefore have a greater functional capability compared to a comparable mechanical or conventional system due to the maintenance functions etc., but will not have some of the functions of the Boeing 777, such as the sophisticated system monitoring system. The system reliability, i.e. safety is of the utmost importance though, and this cannot be compromised.

5.2 Power Generation Systems

The hydraulic and electrical systems tend to be very similar to those on a mechanically signalled aircraft since their functionality is more or less the same, and the technology is established. Hence the evaluation will be performed at a functional level by considering the system architecture, and the effect that failures are likely to have on the aircraft.

5.2.1 Hydraulic

The hydraulic systems of the aircraft considered are very similar insofar as both the Airbus and Boeing aircraft have three 3000 psi systems. The systems are also driven by the same arrangement of engine-driven pumps, AC motor pumps for peak demand and a Ram Air Turbine (RAT), though the Boeing 777 also has an Air-Driven Pump on the centre system, which is used for peak demand when required. The division of services between the two aircraft is different however. The 777 has the Left and Right systems

as the primary flight systems, with the Centre system being used to power the landing gear and steering utilities as well as the primary and secondary flight controls. The Airbus aircraft have the Blue hydraulic system as the primary redundant flight control system, with the Green and Yellow hydraulic systems providing the additional control surfaces required, and the brakes, steering and landing gear. These differences merely reflect a difference in choice, and as all three systems can provide adequate flight control, there is no reason to fault either manufacturer's approach. The additional utilities are placed depending on the demands and capabilities of the other aircraft systems. The RAT is also used to drive a standby electrical generator for emergency use with all of the aircraft considered since it is not a time-limited source, and it usually can power the control surfaces sufficiently well for flight.

The distribution of hydraulic systems among the control surfaces is very similar for the two aircraft. For the elevators and horizontal stabiliser, one system powers both elevators, while the other two systems each power an elevator and one of the trimmable horizontal stabiliser motors. All of the Airbus aircraft have the same hydraulic and actuator arrangement for the tail surfaces. The arrangement for the hydraulic systems on the wing is different though. The Airbus aircraft have a symmetrical arrangement, where the hydraulic systems which power each of the ailerons are mirrored from side to side, see Figures C2 and D3, while they are not the same on the Boeing 777 since the two ailerons and flaperons (high speed ailerons which also droop at low speed to act like a flap) are driven by different hydraulic systems on each side, see Figure E2. In all cases however, the spoilers in each pair are both powered by the same system. The two ailerons and flaperons are driven from two of the four actuator control electronics (ACE) so that each ACE drives one flaperon and one aileron. Therefore the hydraulics are arranged so that the No. 1 left ACE, the centre ACE and the right ACE use the left, centre and right hydraulics to power the surface, with the No. 2 left ACE using the left system for the aileron, and right system for the flaperon, which gives the dissimilarity. A similar logic is used for the elevators.

All of the aircraft are fitted with hydraulic fuses, which limit the fluid flow in the event of a pipe breakage to prevent the complete hydraulic system being drained. In addition, no more than two of the three systems enter into an area of non-critical structure so that in the event of loss of that structure, at least one system is preserved.

5.2.2 Electrical

The electrical system will be described with respect to the flight control computers only. The A320 has three independent sources, ELAC1 is powered from the DC emergency bus, ELAC2 and SEC1 are powered from the DC shed emergency, and SEC2 and 3 are powered from the No. 2 DC bus, see Figure C1. Therefore in the event of power failure, the system could degrade as low as ELAC1 alone, which is sufficient to fly the aircraft until power is restored. The A330 / A340 have PRIM1 and SEC1 powered by battery buses 1 and 2 respectively. This leaves the rest of the computers to be powered from No. 2 DC Bus, see Figures D1 and D2. Therefore there are three

independent sources of power, either of the battery buses, which can be powered from any of the DC buses, or the No. 2 DC bus, which is primarily powered from the AC system via a transformer/rectifier.

The Boeing 777 has a system which has three individual electrical buses for each of the flight control computers, see Figure E1. Three of the ACEs are powered from these buses, with the fourth being powered from the Left 28V DC bus. Hence each computer can have its own source of DC power since there are dedicated batteries for the flight control buses, and also dedicated generators on the engines for two of the buses, as well as being powered from the main aircraft DC power system.

The Boeing 777 is very redundant, more so than the Airbus aircraft. It is not necessarily the case of the Airbus aircraft being under-redundant, rather the 777 being highly redundant, as most Boeing aircraft are. The general requirements for electrical power systems require more work than presented here, but essentially the flight control system should have at least three independent sources of power, with the system being capable of being run from the aircraft batteries as well as a renewable source, such as a RAT generator.

5.3 Fly-By-Wire Control System Architecture

5.3.1 Data Communication

There are obvious differences between the flight control systems of the different aircraft. Most significant is the use of different technology, the 777 having an ARINC 629 databus as the primary form of information interchange while the Airbus has more direct links and the more simple ARINC 429 point to point databus, or datalink. These differences reflect partly the different choices available, but more importantly they represent the limit of available technology at the time. The Airbus A320 was the first fly-by-wire civil aircraft of its type, and therefore the certification authorities had to be sure that it was sufficiently safe. Therefore it used a large amount of conventional technology, such as ARINC 429 and direct links since both were proven.

This trend was carried through into the A330 / A340, which followed the A320, although their systems were modified to make them simpler while still meeting the requirements as a result of the lessons learned from the A320. The Boeing 777 used new technology and concepts to a greater degree than the Airbus aircraft. Boeing have traditionally been the first to implement new technology, the ARINC 429 system was first used on the Boeing 757 / 767. The databus technology has made the aircraft more reliable, and in some cases cheaper to build, but required a vast amount of development resource. Some of the systems, such as ARINC 629 had been under constant development since 1977. The 777 also has a high degree of redundancy and availability, primarily to help it through certification, but also because of the sectors that it was planned to be flying, for example up to 10,000 miles at a time over the oceans. The different aircraft considered here therefore reflect how the state of the art has progressed.

ARINC 629 has a benefit for large aircraft, though this is probably not true for small aircraft. This is because there is a significant weight reduction from electrical wire savings, that does not occur with smaller aircraft. Even so, the databus does not extend to the extremities of the aircraft and the bus connectors are expensive. Therefore the number of connections on the bus are minimised, and therefore remote data concentrators need to be used to connect a number of components onto the bus. See Appendix B for more detail concerning current databus formats.

Military databuses, such as MIL-STD-1553B are not deemed suitable for civil transports since they have bus controllers, which could constitute a single point failure, and they are expensive. However, they are widely used in most modern military aircraft, especially those of American origin.

5.3.2 Sensors

In all of the Airbus aircraft described, the pilot's inceptor sensors are hard wired to more than one flight control computer. Inter-computer communication is done using ARINC 429 broadcast buses, and other systems, such as the air data and inertial reference systems are also connected to the flight control computers using ARINC 429 links. However, the individual inceptors are connected directly to the flight control computers.

On the Boeing 777, the inceptor sensors are hard wired to the Actuator Control Electronics boxes (ACEs). All of the inceptor sensor output signals are available to all of the flight control computers through the ARINC 629 databus. The signal for the computers is selected using a routine based on the mid-value selection principle. A similar procedure is carried out for the trim inputs and the speed brake.

The difference in the two systems reflects the ability of the ARINC 629 buses to transmit information around the system rapidly. However, the Airbus system is adequate for the task, as long as there is sufficient isolation between the individual computers so that a failure from a faulty sensor will not propagate through the system.

The differences also reflect certification requirements. The Airbus aircraft can be flown with none of the databuses operating if required. The ACEs enable the Boeing 777 to be flown without any of the ARINC 629 databuses operational since the ACEs are connected directly to the actuators and inceptors. This is to enable the system to cope with a generic ARINC 629 failure, which would result in all of the databuses failing at the same time.

For the Boeing 777, other information required by the flight control system, such as aircraft configuration data is collected by the Airplane Information Management System (AIMS) for transmission on the ARINC 629 flight control buses. This enables information to be provided by non-critical systems, and transmitted onto a critical flight control databus. Therefore the AIMS acts like a bridge between systems of differing

integrity requirements. The Electronic Central Aircraft Monitor on the Airbus aircraft performs a similar function.

All of the aircraft have a federated air data and internal reference system (ADIRS). This enables all of the systems which require the information to access it without having to have a direct link between the ADIRS and the individual users. The ADIRS systems which transmit on databuses often have multiple transmitters for a single bus in order to reduce the impact on the system of a transmitter failure. The federated nature of this system is good since it removes the processing of raw data to provide air and inertial reference data from the FCCs as it is performed within the air data computer, where there are sufficient internal channels to provide a redundant source, which can trap faults as they occur.

5.3.3 Flight Control Computers

There are different schools of thought between the different implementations. The Flight Control hardware with the Airbus aircraft does not have databuses for the primary means of communication for the majority of the data transfer, as the connections between the flight control computers, and the actuator electronics and sensors are hardwired. In theory, this should not affect the system architecture since the databuses can be replaced with hardwired links, requiring only a change in the interface hardware / software. The actual function of the "black boxes" can be left unchanged. However, the Airbus aircraft have one computer which is nominated the execution computer, and instructs all of the other flight control computers in the normal situations with the required control surface demands via a dedicated ARINC 429 link. Boeing have adopted a different approach since all of the three flight control computers are performing both the control law computation and individual actuator commands. Any differences between the computers is noted, and fault-finding algorithms can isolate the required subsystem. This gives the Boeing aircraft a more distributed processing system, at the expense of an increase in data communication whereas the Airbus aircraft have a more centralised processing system, without some of the advantages of a distributed system, such as ease of upgradeability (see section 2.4.2). However, the benefits of these features to flight control systems are doubtful.

The number of lanes in each computer is different too. With the Airbus aircraft, the redundancy is in the number of flight control computers (FCC). Each computer has two lanes, and failure of one lane will result in that computer shutting down, or at least being removed from the execution task. The redundancy comes from the fact that each control surface can be driven by up to four computers. Boeing have adopted three primary flight control (PFC), each with three lanes. The individual actuators are driven effectively from the flight control computers, with one PFC having the ability to drive another PFCs actuators / control surfaces. In the same way as the Airbus aircraft, each control surface is driven by two or more actuators, and hence by two or more PFCs. With the Boeing aircraft, loosing a lane in one of the computers does not mean that the flight computer will shut down since the computers can function with only two lanes

out of the three operating. Therefore the redundancy is within the computers as opposed to being in the number of computers.

There is dissimilarity within the individual systems. There are two different types of FCC within the Airbus flight control systems. Each type has identical hardware, but dissimilar software to prevent common mode faults within the computer. The two different computer types have dissimilar hardware and software, which prevents common mode faults within the complete system. The Boeing 777 has only one type of PFC, but it has both dissimilar hardware and software. Therefore both types of aircraft have dissimilar hardware and software within a system.

Each aircraft also has two dissimilar forms of control. With the Airbus aircraft, the two different types of computer make up the dissimilar form of control, with the secondary computers being a very sophisticated direct link since they can only fly the aircraft in direct law. The Boeing 777 has the three PFCs as the primary form of control, with the direct link as the secondary form of control.

5.3.4 Control Surfaces and Actuation

The number of actuators for each surface is governed by the control force, flutter and redundancy requirements and is approximately the same for each of the aircraft. The elevators, ailerons (and flaperons) each have two actuators per surface, although the Airbus system allows more than one computer to drive a single jack. Two actuators result in the surfaces being fail operational / fail passive, which is suitable for them since several control surfaces can do the same job. The rudders in all of the aircraft each have three actuators. This is to meet a greater redundancy requirement since the surface must reliably cope with the engine-out case, and with the possible exception of asymmetric spoiler deployment, it is difficult to reconfigure control surfaces to cater for yaw control. One solution would be to have split rudders, where the loss of one surface would not be critical. However a better solution to have a force summing arrangement, where hydraulic servos powered by the three hydraulic systems in parallel, which then power the three primary actuators. Therefore only one servo is needed to power all of the jacks, and either of the two pairs of rudder pedals could also be used to power the jack in the event of failure of the three servos or the computers driving them. The spoilers are all driven by one computer channel since they are not critical for flight control.

The actuation systems on the two aircraft is different. The Boeing 777 uses force summed actuators, where both actuators are active at the same time, with any one servo-valve being able to control the power actuators on one particular control surface. The Airbus aircraft use active / standby actuation, where one actuator is controlling the surface while the second is in standby or damping mode, i.e. not controlling, but ready to take over if the first actuator fails. Active / standby is simple to implement, but does not give as good failure transient performance as a force-summed system, and can be heavier. The Airbus actuators are slightly more complex in the sense that one actuator

can be driven by two different FCCs in some cases, whereas the Boeing servo-valves are driven by a single FCC.

The actuator monitoring is done in the ACE computers for the Boeing 777, while it is done by the actual flight control computers themselves for the Airbus aircraft. This again highlights the difference between the distributed approach by Boeing and the centralised Airbus method. There is no equivalent of the Boeing 777's direct analogue link between the pilot's inceptors and the actuators on the Airbus aircraft. This is because the analogue link is classed as a dissimilar form of control. Airbus do have a dissimilar method of control, which is the SEC computers since they are classed as being dissimilar to the PRIM computers on the A330/A340 and the ELAC computers on the A320. The SEC computers on the Airbus aircraft are primarily used for spoiler actuation, although they have the reserve capability of actuating the primary surfaces, and they can only fly the aircraft in direct law, i.e with the sidestick giving control surface position demands. Therefore they are essentially a separate means of commanding the actuators external to the PRIM or ELACs, coupled with direct command facility.

The other differences between the Airbus and Boeing systems are due to the system arrangement. The probabilities of a 777 loosing a FCC are less than an Airbus since the Boeing can tolerate a lane failure in any given FCC before the systems fails, while the Airbus cannot. However, with the Airbus, primary control surface actuators can be driven by a PRIM and a SEC, therefore a combined hydraulic and computer failure, which could disable a conventional system is not critical on an Airbus since the individual surfaces are inherently tolerant to computer failure, and therefore it would require a large number of failures for the system to fail. This capability is not present in the Boeing system, but the Boeing aircraft have the redundancy in the flight control computers themselves instead of in the actuation system.

All of the aircraft considered have sufficient control power to fly the aircraft, albeit with reduced manoeuvrability with one hydraulic system alone. In the case of the 777, one working flight control computer / actuator control electronics combination has approximately the same control authority as one working hydraulic system.

Computer Failures

The Airbus aircraft have an active-standby system, i.e. one control surface actuator is on standby, and the other actuator is commanding the surface. A failure with active / standby actuation are slower to cope with the transient due to the active bypass valves having to operate to isolate the failed actuator and energise the standby one, whereas a force summed system does not have this problem, therefore there is less of a transient.

The Boeing aircraft also have an approximate computer / hydraulic combination, i.e. the right PFC drives the right ACE box, which in turn controls the majority of its surfaces with the right hydraulic system. This is duplicated, more or less, for the centre and left systems, although there is some crossover between the ACE boxes, see Table E1. This

seems to have been a philosophy adopted by Boeing - it makes the failure analysis much easier, but has no other obvious benefits. The 777 can be dispatched with one PFC failed for a short period, but this is effectively like dispatching with one hydraulic system failed. However, the chances of having to dispatch with a PFC failed are remote, even if repairs to the PFC are left to the scheduled servicing periods.

The Boeing aircraft have a total of four ACE boxes, each of which drives one actuator on either of the two elevators, ailerons and flaperons. These then have to be driven by three primary flight computers. Therefore in normal operation, one PFC drives two ACEs, while the other two PFCs each drive a single ACE. There were initially four PFCs in the initial study, therefore each PFC would have driven one ACE, but the fourth PFC was removed since the three PFC arrangement was sufficiently reliable, and removed the need for the associated quadruplex sensors (and the fourth ARINC 629 bus). Any ACE can be driven by any PFC. It would have been difficult to allocate four elevator outputs to three ACEs or PFCs and still retain a degree of similarity between the ACE boxes. Therefore having four ACE boxes circumvents this problems, and the amount of similarity between the ACE boxes is preserved to a high level, although the fourth box has very few outputs since it only controls the 'fourth' surfaces, where they are present, see Table E1.

5.3.5 Dispatchability

The aircraft considered can be dispatched with up to 1 FCC (Airbus) or 1 PFC (Boeing) failed. With the Airbus aircraft, the actuation functions of the failed computer can be taken over by one of the other computers for the working surfaces. Therefore the system can tolerate at least an additional two failures, with subsequent failures gradually reducing the system functionality. The 777 can tolerate one flight computer failed for a short period, or one lane indefinitely, or two lanes for a period, as long as the two lanes are not of the same type. This ensures that the probabilities of retaining at least one working PFC are high. The Boeing 777 can be flown on one PFC since any PFC can drive all of the control actuators, while no single Airbus computer can do this. The presence of the direct links on the 777 means that any one hydraulic system can control the aircraft in all axes, even with FCC failure since the analogue links should still permit the 'working' control surface actuators to be driven, therefore the requirement that the direct link is reliable is a necessity.

5.3.6 Certification

The aircraft have a common theme when certification is involved. The two different computers on the Airbus A320 (ELACs and SECs) are considered as two different methods for control due to the dissimilar hardware and software, and therefore this assists with the certification process. This is because the two types have different processors within them, and different software. This has also been carried over into the FCPC and FCSC on the A330/A340. The Boeing 777 has adopted a similar stance, as the FCCs are the primary means for control, and the analogue link which is contained

within the ACEs is considered to be the secondary form of dissimilar control. It is reasonably straightforward to demonstrate that the reliability of this link is high, therefore the certification process is eased. Hence if the flight control computers in the proposed system are identical, then it is recommended that an analogue link is used to bypass them and provide the required reliability.

Both aircraft have included a mechanical backup which will enable the aircraft to be flown in the event of total electrical and hydraulic power failure. In each case, this is only intended as a short term measure while normal power is restored, although Field [4] demonstrated that it is possible to land an Airbus A320 using the manual reversion alone.

5.4 Handling Qualities

There are different alternatives for the handling which require a different approach. With a conventional control approach the pilot is effectively controlling the aircraft longitudinally through direct connections to the control surfaces. This corresponds to a short term pitch rate response with a long term angle of attack response, hence the reference often made that a conventional aircraft is angle of attack command. This also means the aircraft is speed stable, and can therefore can be flown without an autothrottle. With a non-conventional approach, the aircraft has either a form of attitude or flight path command. Either can be used to good effect, for example, the aircraft's flight path can be controlled directly, and these artificial responses are better suited to a small displacement inceptor, such as a sidestick. However, there are disadvantages. The aircraft is no longer typically speed stable, which can present speed control problems unless an autothrottle is fitted. An autothrottle can be used to good effect though, and in the case of the Boeing 777, speed feedback has been built in so that the aircraft remains speed stable. Autothrottle can modify the effect of the command variable [28]. For example, adding an autothrottle to a pitch rate command system causes the system to behave like flightpath demand with constant speed. Hence the pilot can fly the flightpath with the control wheel after having dialled-in the desired speed on the autothrottle. However, systems whose dissimilar forms of control have a very different handling characteristic to the primary form of control could have certification problems since it is an airworthiness requirement that the first system failure does not produce a marked change in the aircraft handling characteristic.

For the lateral handling qualities, the Airbus and Boeing aircraft have similar implementations. They all have augmented roll command so that for angles of bank below approximately 35°, the aircraft has neutral roll stability, i.e. the roll command inceptor is acting like a rate command unit, with roll attitude hold. Above 35°, they all have positive roll stability, hence roll commands need to be held in order to maintain the bank angle above this limit. Unlike the Boeing aircraft, the Airbus aircraft are also bank angle limited at 67°. Field [4] found that the Airbus aircraft has approximately a Cooper Harper rating 5 under the second level of degraded controls, i.e. with direct law. Using complete system failure, i.e. with mechanical rudder and elevators, it was

possible to land the aircraft, though damage would result to it. This corresponds to a Cooper Harper Rating of approximately 9 or 10.

Configuration Changes

Augmented response types have the advantage of being able to minimise attitude or flightpath changes with configuration changes. This can be of assistance to the pilots since the optimum aircraft response to, say, gear lowering, can be determined and implemented. Auto-trim functions are already implemented with current civil aircraft, especially with gear and flap deployments which have large trim changes. However, care must be taken that the pilot's cues are not misleading or lost. These cues also need to be considered for engine failures.

Protections

There are two principal options for flight envelope protections. The first is soft protection, where the aircraft alerts the pilot that he is reaching the envelope boundaries, typically with high control forces, but does not actively limit him from exceeding them. This is the system favoured by the American manufacturers. The second type of protection is hard protection, where the pilot is prevented from exceeding the envelope limits. This system is favoured by the Airbus aircraft since it gives the aircraft absolute protection from exceeding the limits as the aircraft can override the pilot, and in theory renders the aircraft 'uncrashable'. There is good reason for going no further than soft protection though, since the pilot can make a 'better' situational judgement than the 'aircraft'.

However, there are other issues that need to be considered. The Airbus aircraft are equipped with sidesticks whereas the American aircraft are equipped with conventional control inceptors, the Boeing aircraft having a control wheel. These have fundamentally different characteristics. It has been said that hard protection is suitable for sidesticks since the pilot can pull back on the stick as hard as he can, and the aircraft will respond by giving him a stabilised response, such as a maximum rate climb. However this implies a non-conventional control technique, and therefore conventional techniques and reasoning do not apply. This can be summarised by saying that protections must be considered with the whole system philosophy.

5.5 Incident Analysis

This section considers the accidents and incidents that have occurred with fly-by-wire civil aircraft. These incidents all involve Airbus aircraft, which is understandable since the A320 has been in service since 1988, and the A330/A340 since the early 1990's, whereas the Boeing 777 has only been in service for a few months at the time of writing. Therefore no conclusions should be made concerning the number of incidents with Airbus aircraft. Also, no comparison has been made with non fly-by-wire aircraft since the purpose of this section is to learn from what has happened previously and not to compare records of different aircraft.

In total, there have been thirteen incidents with A320 aircraft, and one with an A330. They have been described briefly in Table 1. Some common trends can be seen. Excluding the maintenance and structural incidents, to which all aircraft are subject, none of the aircraft has had an accident which has been a direct result of the control-law or flight control system architecture. In other words, the use of the C* law in the current aircraft flight control system in the Airbus aircraft does not seem to have directly contributed to the accidents and incidents considered here.

However there have been landing incidents where there is a possibility of the aircraft having floated in the landing flare, resulting in a slightly delayed reverse thrust deployment due to the undercarriage oleos not compressing. This tendency to float was uncovered by Field [4] as a contributory factor for a variation in touchdown performance. This would not cause a danger to the aircraft in normal circumstances since the aircraft performs acceptably as long as the operating manuals and procedures are obeyed, as there is no inherent problem with the aircraft. Additionally, human factors issues need to be considered, such as the complexity of the autothrottle, and pilot situational awareness, which must be considered in all aircraft design. With an aircraft that is different from the conventional handling response types i.e. the Airbus aircraft, crew training is also of utmost importance since the aircraft may have to be operated differently, to give the increased benefits that the unconventional system possesses. This requirement needs careful consideration, especially as an increased level of training may be expensive. However, in all of the cases, the aircraft have performed as designed, and no design faults were noted.

Sources for this incident information can be found in the references listed with each aircraft incident / accident in Table 1.

5.6 Concluding Remarks

This section will conclude the analysis for the flight control system briefly by using the criteria given in section 4.1. It is difficult to recommend improvements that could be made since the aircraft systems are task-tailored, and they all meet the necessary safety and reliability requirements. 'Improvements' could be made to the individual aircraft, but only to give an economic benefit, and only if the design was changed during initial aircraft development, such as using different technology which may not have been around at the time. However, it is useful to draw on the important design features that have been shown so that they may be incorporated into future aircraft.

Aircraft	Description	Cause(s)
A320 ref. [29]	Pilot allowed aircraft to get too slow and low with engines at idle at an airshow. Aircraft hit trees near the end of the runway. Aircraft performed properly.	Pilot error. There were many human factors points revealed during this incident.
A320 [30]	Incorrect autopilot mode selected by the crew on approach. Crew were not aware of the speed loss. Aircraft hit the ground before the runway. Aircraft performed properly.	Pilot error. Possible problem with inexperienced crew in sophisticated aircraft.
A320 [31,32]	Incorrect autothrottle mode selected by the crew on approach. Aircraft flew into mountains. Crew were not aware of the high rate of descent. Approach in mountains. No runway ILS and no GPWS, which would have probably saved the aircraft. Aircraft performed properly.	Pilot error. Very low crew experience.
A320 [33]	Engine cowls detached. Damaged Horiz. Stab. and undercarriage. Landed safely.	Structural failure.
A320 [33]	Nose gear shock absorber failed, followed by nose wheel separation. Skidded 150m before the aircraft stopped.	Structural failure.
A320 [34]	Fast landing with tailwind in rainstorm. Delayed wheel spin-up, depriving crew of reverse thrust. Aircraft overran the runway and crashed into an earthen bank.	Not known. Possible reverse thrust logic failure.
A320 [34]	Captain shut down both engines by mistake in the climb. Both were re-started. Aircraft fully serviceable.	Pilot error.
A320 [35]	Spoiler remained deployed after maintenance. Required full roll demand to counteract. Aircraft landed safely at higher approach speed than normal in the alternate control law.	Maintenance error.
A320 [34]	Aborted take-off when aircraft had pitch-up tendency. Incorrect loading resulted in aft CG.	Loading error.
A320 [36]	Severe pitch-up with aft CG during autoland on reverse thrust and lift dump deployment. #1	Not known.
A320 [36]	Severe pitch-up with aft CG during autoland on reverse thrust and lift dump deployment. #2	Not known. same airfield and operator as previous.
A320 [36]	Delayed spoiler deployment due to throttles not being at idle resulted in aircraft bouncing and landing heavily. Throttles were retarded during the bounce.	Not known.
A320 [36]	Severe turbulence caused flaps to lock in position 4. System gave incorrect advice to pilot's to select position 3, which resulted in incorrect landing gains and the aircraft sensitive in roll. Aircraft landed safely	Incorrect advice to pilots.
A330 [37,38]	Aircraft crashed on test flight. Pilot's situational awareness was low, and the crew were slow to react after simulated failures in the initial climb-out.	Not confirmed. Possible slow crew reactions and non-compliance with test procedure. Crew fatigue.

Table 1 : Fly-By-Wire Accident and Incident Summary

Capability

The Airbus and Boeing aircraft have different design philosophies, with the Airbus aircraft being unconventional in terms of aircraft handling, and using relatively 'simple' technology, whereas the Boeing aircraft have more conventional handling characteristics, but relatively 'complex' technology. Both are perfectly acceptable as long as the aircraft are operated in accordance with their operating manuals and hence in accordance with the design philosophy. However, this can result in an increased training requirement for a non-conventional system, which could be expensive. The philosophies differ most when failures and emergencies are considered. Again, without conducting evaluations, it would be difficult to say whether either flight control system is better or worse since the aircraft must be considered as a whole, i.e. with control laws, displays, inceptors all included in the evaluation, and not as a series of individual components.

According to the literature search, all aircraft perform acceptably well when operated according to normal procedures, and with 'common' failures, such as engine shut-downs. An in-depth evaluation by a test pilot was only available for the Airbus A320 [4], which showed that there could be some variation in performance when operating under increased workload, for example, variation in landing performance. More data would be required to make any firm conclusions.

Reliability

All of the aircraft meet the required standards. However, the level which they exceed it by is significant. Boeing aircraft traditionally have very redundant systems, which makes the aircraft extremely safe, but can add to the cost. The Airbus systems do not have as high a level of redundancy, but they are sufficiently safe, and meet all airworthiness requirements. This has been shown by the fact that there has been no Airbus accident in service as a result of a systems failure. Only sufficient reliability is required to meet the tough airworthiness requirements under all conceivable operation conditions, greater reliability is uneconomic.

Maintainability

All of the manufacturers work with the customer to make maintenance easier, and to reduce cost. All of the aircraft can achieve deferred maintenance on the flight control computing system, delaying maintenance to the next scheduled servicing period. It is also possible to demonstrate that the Boeing 777 has possible zero requirement for fly-by-wire computing maintenance during the aircraft life. This is achieved by the use of components with very high mean times between failures. However, this is not necessarily desirable since hardware tends to be less expensive compared to the flight control system software, and as long as the maintenance can be deferred, there is no reason to have components which are going to last the lifetime of the aircraft, but cost substantially more in the long run.

Maintenance computers are now the norm for medium to large civil aircraft, and are desirable since they assist with fault tracing, as well as keeping a log of the aircraft history. However, the requirement for them to be fitted and the required level of functionality should be very closely examined, especially for an aircraft with a low system complexity, a small number of critical systems and a 'generous' mandatory minimum equipment list.

Certification

From a flight control system point-of-view, certification is critical to the system. Therefore there are ways in which the process can be made easier. Firstly, it is important to have two forms of dissimilar flight control, plus a mechanical backup. This covers most eventualities, and it is easier to have a second dissimilar form of control than to try and prove that the first is free from faults, common mode failures, single point failures. An analogue link which connects the inceptors to the control surface actuators is a very good way of implementing this second form of control, since the analogue links are simple, and therefore it is relatively straightforward to show that they meet the requirements compared to a more complex system. Cost has a large part to play in this, it is expensive to certify components to an extremely high degree of reliability, and it is therefore cheaper to add an analogue link and certify the system to a relatively lower requirement, even though the system would probably exceed the higher reliability requirement.

All of the aircraft considered have been successfully certificated. The Airbus A320 was the first fly-by-wire aircraft, and therefore had a high degree of redundancy, and is based around proven technology. The Boeing aircraft is based around new technology, and the direct link has enabled this new technology to be certified. All of the aircraft have a mechanical backup for unforeseen circumstances. Again, this has been added since it relieves some of the testing requirement on the flight control system in a similar way to the analogue link. However, it is likely that this will not need to be designed with a new aircraft in several years, especially with large aircraft since it is not intended to be used to land the aircraft but instead as a temporary measure while power is restored, and power systems are becoming more reliable.

Cost

Cost is an important component of any aircraft design. Therefore new technology may only be installed if it gives a significant cost benefit. The Boeing aircraft has technology such as ARINC 629 installed because for that particular application it gives a cost benefit. For a smaller aircraft, it would probably not give any benefit since the cost of implementing it would outweigh the particular saving that ARINC 629 gives. Again, the golden rule is 'if it doesn't give a cost saving then don't install it.' ARINC 629 could probably be used successfully on the A330 / A340 aircraft, though it would probably not be beneficial on the smaller A320. However, to install it on the A330 / A340 would be expensive in terms of re-design since these aircraft were never designed

to have it installed from the outset. Therefore it is not appropriate for these aircraft, though it may be for a future large aircraft.

Technical Risk

The Boeing approach has historically made use of more new technology than the Airbus aircraft. Boeing were also the first manufacturer to use ARINC 429, and therefore they have a track record of using new technology on aircraft. Airbus have not implemented new technology to as high a degree, although they were the first company to produce a full fly-by-wire civil aircraft (with existing technology). Therefore if new technology gives substantial savings then it should be used. But too much new technology in one go is too risky, and can be expensive to certify and get right, especially if there are problems. Therefore the use of technology demonstrators is useful in situations like this, since they allow the technology to be introduced one step at a time. They have been used successfully by Airbus and Boeing by modifying a conventional civil airliner to accept full fly-by-wire, with the aircraft's own system remaining to take over in the event of an emergency.

6. Recommendations for the Generic Regional Aircraft

This section of the report describes the proposed flight control system for the Generic Regional Aircraft. The proposed system is derived from the conclusions drawn during the previous sections of this report. The assumption that fly-by-wire is required has been made, and is not in dispute. However, it has not yet been established to what extent fly-by-wire needs to be implemented, i.e. is electrical signalling of the control surfaces or full fly-by-wire required ? Therefore the assumption has been made that a full fly-by-wire system is required, with its associated control laws and protections, since more work would need to be done in the field of aircraft handling and operating costs for this decision to be made.

6.1 Power Generation Systems

This section considers the hydraulic and electrical systems for the Generic Regional Aircraft.

6.1.1 Hydraulics

It is recommended that three hydraulic systems are fitted since they will be used as the primary form of power for actuating the control surfaces. Any one hydraulic system must be able to control the aircraft in order to meet the requirement for control with two hydraulic system failures. The systems shall be called yellow, green and blue. The yellow and green systems are for normal flight control, and the major / high volume users such as the undercarriage and flaps. See Figure 2 and Table 2.

The yellow system will be powered by an Engine Driven pump on the left engine for normal use, with an AC driven pump from right AC bus for high demand situations. The green system will be driven by an Engine Driven Pump on the right engine, with an AC motor pump driven from the left AC bus. Therefore, in the event of an engine failure, the yellow or green system will be able to be driven by the opposite AC main bus so that loosing an engine will not result in the loss of a complete hydraulic system, although the flap or gear deployment may be at a reduced rate, depending on the overall demand on the system.

The blue system will be driven by an AC electrical pump, which should be powered from one the emergency AC electrical bus since it is one of the flight critical supplies and will enable the system to be powered from the remaining AC source in the event of an almost complete power loss. The blue system will also have the Ram Air Turbine (RAT) for emergency power. The RAT should be sufficient to power the flight controls, although control may be degraded due to lower actuator rates, and possibly supply the flight critical avionics via a hydraulic powered electrical generator.

Control Surface	Flight Control Computer	Hydraulic System
Left Elevator 1 (outboard)	FCC 4	Y
Left Elevator 2	FCC 3	B
Right Elevator 2	FCC 2	B
Right Elevator 1 (outboard)	FCC 1	G
Trimmable Horizontal Stab. 1	FCC 1 & 2	Y
Trimmable Horizontal Stab. 2	FCC 3 & 4	G
Left Aileron 1 (out)	FCC 3	Y
Left Aileron 2	FCC 4	B
Right Aileron 2	FCC 1	B
Right Aileron 1 (out)	FCC 2	G
Rudder Servo-Actuator 1	FCC 1	B
Rudder Servo-Actuator 2	FCC 2	G
Rudder Servo-Actuator 3	FCC 3	Y
Spoiler 1 (inboard)	FCC 4	B
Spoiler 2	FCC 2	B
Spoiler 3	FCC 1	Y
Spoiler 4 (outboard)	FCC 3	G

Table 2 : Proposed Control surface and flight control computer actuation

6.1.2 Electrics

The electrical system design should ensure that there are sufficient dissimilar sources of power available to the flight control system so that it does not fail through a small number of faults. With reference to the flight control system, each of the flight control computers (FCC) should be powered from a separate DC source, but in practice at least three sources in total should be used so that two independent power failures can be tolerated before power loss to all of the FCCs. Two FCCs should therefore be powered from the two main battery buses, with the remaining computers being powered from the emergency DC bus.

The electrical system should have at least one main generator on each engine with another generator on the APU. Any one generator should be able to power all of the critical flight loads in normal service. This may also probably give a dispatch possibility with one main generator failed, but this would require further analysis to confirm. There should also be an emergency generator on the blue hydraulic system for use when all conventional sources of power are unavailable.

6.2 *Flight Control System Interface with Other Aircraft Systems*

It is important to consider the interface of the flight control system with the other aircraft systems. Therefore the interface of the system proposed was considered with the Honeywell digital flight guidance system (DFGS) on the Avro RJ aircraft [39]. This system integrates the autoland, steep approach, elevator trim, yaw damper, attitude alerting and envelope protection, automatic throttle control, windshear detection and guidance and some maintenance functions. Therefore it is recommended that the proposed flight control system should be able to be interfaced with this DFGS system.

The two systems would remain separate since the DFGS is not a flight critical system whereas the flight control system is. However the interface between them would be essentially straightforward since the same communication media are used by both systems, and the majority of the information required by the flight control system, such as air data, is already available in the DFGS. Some modification of the DFGS functions are required, but these are generally simplifications of the system. For example, for autoflight, the flight control system (FCS) could be considered as an extension of the autopilot. By removing the specific autopilot actuators and substituting the FBW FCS, autopilot commands could be executed by the FCS. The proposed flight control system architecture can be seen on Figure 3, showing the interfaces with the other systems.

6.2.1 Control Surface Recommendations

The following section outlines the proposed methods of control for each of the flight control surfaces.

Aileron and Elevator

It is proposed that there are two ailerons and two elevators, being divided into left and right sides, with each side being unconnected to the other. Therefore with fail operational / fail passive on each control surface, a double failure will ensure that at least one surface is still functioning, therefore control will be maintained in that particular axis.

Faults will be detected by the individual flight control computers through duplex monitoring, and will isolate the failed system by removing its hydraulic supply and engaging the hydraulic supply of the standby system. The flight control computer driving the standby system will have been calculating the control surface demands, and effectively signalling the actuator, although the hydraulics to the actuator being driven by that computer would have been disabled, therefore it should be able to take over straight away. The standby system will automatically take over, unless there is a fault in that system, when the direct link will automatically be engaged by reconfiguring the flight control computers, and supplying hydraulic pressure to both actuators.

In the event of the direct link being engaged, both actuators will drive the surface. It has been assumed that there will be no synchronisation between the two actuators, therefore the stresses in the control surface may be greater. Therefore pressure reducing valves have been incorporated when the backup system is engaged, which allows the actuators to work at reduced pressure, and therefore minimise the control surface stresses.

Rudder

It is proposed that the single rudder should be driven by three actuators in order to achieve a similar overall reliability to the combined ailerons or elevators, where either aileron (or elevator) is sufficient to control the aircraft. The requirement for a rudder tab has not been considered since it is not considered necessary with a hydraulically driven surface.

In order to cope with flutter and also the high forces envisaged during engine failure, it is proposed that all three rudder actuators are active at once. This is likely to cause some problems since the actuators must all be commanding the same values so that the internal forces within the control surface are reduced. Two different ways have therefore been considered for doing this. A force-summing system has not been proposed due to its complexity.

The first way of achieving the same displacements is to introduce voting at the output plane of the flight control computers. This would involve the values computed by the three computers being distributed amongst all of the flight control computers so that each one that controls a rudder actuator can carry out a vote to determine which value they should select. It is suggested that if this type of system is implemented, the mid value should then be selected. The command and monitoring lanes within each computer could be used to determine if the signal from that particular computer is valid or not, and therefore this system should still ensure that two flight control computer failures can be tolerated since voting is only present to ensure synchronisation, and not to determine if failures have occurred. Algorithms should be incorporated within the individual flight control computers to detect failures.

The second way of achieving synchronisation is to adopt a system like that used by Airbus, where one computer is nominated the controller, and the others are used solely to process the actuator demands generated by that controlling computer. In the event of failure in the controlling computer, it will declare itself failed, and another computer will take over. This system has the advantage over the first that no voting is required, other than the usual failure monitoring within the computers as usual. In both cases, the amount of information passing along the databus is very similar, i.e. computer status information or whether the computer is healthy or failed in that particular channel, and the commands from the controlling computer. The choice of system would require further work to accomplish.

Spoilers

With the individual spoiler pairs, failures are detected by comparing demanded position to actual position, which can therefore determine if a given spoiler has failed. Failure on one particular spoiler should result in that particular spoiler pair being disabled to ensure that 'symmetrical handling' results, e.g. the roll rate is the same in both directions. This is a fail passive system. Reconfiguration of spoiler surfaces may also be required, therefore information concerning the current failure status of the spoiler pairs may need to be transmitted along the databus.

Trimmable Horizontal Stabiliser

The trimmable horizontal stabiliser (THS) is normally used to trim the aircraft for efficient flight. However, it has been shown that it can be used as a primary means for backup pitch control, as long as the rate at which it moves is sufficiently fast. Hence it is proposed to use this as a means for mechanical reversion, and the rate at which it needs to move will need to be considered during a handling qualities evaluation for the proposed aircraft.

Mechanical Backup

It is proposed to implement a mechanical backup for temporary use under failure conditions. This will control the THS for pitch control, with lateral control provided by either the rudder pedals under mechanical control, or a single pair of spoilers. The choice between these two is determined by the choice of main pilot inceptor. Rudder pedals have been used with the Airbus FBW aircraft, all being fitted with sidesticks, primarily because the pilot cannot put enough force into the sidestick to actively drive a pair of spoilers by hand. The Boeing 777, which has a conventional control wheel, does not have this limitation, and has adopted for the lateral backup to control the spoilers. However, the best solution for the Generic Regional Aircraft will need to be evaluated in a simulator.

Flap and Slat Actuation

It has been assumed that the flap and slats will be controlled by a conventional flap and slat control system. The flight control computers will need to know what the current aircraft configuration is, and this can be an output from the flap and slat control system. It is proposed that two flap and slat control computers be fitted, in line with current civil aircraft.

The flap and slat system can be linked to the primary flight control system in a number of ways. Each flight control computer could be wired directly to each flap and slat computer. However this would introduce the possibility for Byzantine faults [16]. Therefore some sort of broadcast bus should be fitted, such as a dedicated ARINC 429 link.

The flap and slat system could be driven by the flight control computers if necessary, since there is no reason why the flight control computers should not control these surfaces. However, the flaps and slats tend to be controlled with dedicated computers, firstly to preserve the integrity requirements of the flight control system, and secondly because they tend to be driven using a different form of actuation to the primary control surfaces. Therefore it is suggested that the flaps and slats should be driven by a conventional flap and slat controller, which has the benefit of being proven technology.

6.2.2 Flight Control Computer Architecture

This section will consider the layout for the lanes and channels in the flight control system. This is discussed in section 2.3.2. The design is based on ideas and comments from the available literature and from industry.

There are four pairs of spoilers, and since it has been determined that each can fail passively, only one actuator is required per spoiler. It is possible to drive all of the spoiler pairs by three flight control computers. However, since it is proposed that there are four elevator actuators, four aileron actuators and four pairs of spoiler actuators, it would be much neater to have four flight control computers. Using this arrangement, the computers would be essentially identical, with minor differences within each computer to account for the appropriate surfaces being controlled (i.e. a left or a right aileron). The rudder only requires three channels, therefore one computer would not be needed for rudder signalling. It would be a relatively straightforward matter to program these differences into the software, and to use a coded plug to tell the flight control computer which position they are located in. This gives a cost benefit since the flight control computers therefore have essentially similar hardware, and it also has a maintenance benefit due to the reduced parts count.

Since there are four computers, it would seem appropriate to have two lanes per computer, making an overall total of eight lanes. This should therefore meet the required reliability requirements. It also has the advantage that one computer within the lane can be permanently configured as a command computer, and the other as the monitor. Using one processor type for the command, and one for the monitor would remove the greatest likelihood of a common mode fault. It would also enable dissimilar software to be used, one type for the command software and another for the monitor. Since the computational overheads are approximately the same for the each of the lane types, two processors of a similar capability could be used, such as a Motorola 68030 and Intel 386, which are used on the Airbus A340 computers. It would also enable the computers to be synchronised internally, which would reduce the required fault thresholds between the command and monitor lanes. The system will not be synchronised for normal operation between the individual flight control computers since it is envisaged that it will not be required, and synchronism would tie the individual flight control computers in too closely so that they could drag each other down in the event of failure. Even though the computers will be synchronised internally, it is assumed that they will be using a Byzantine fault-tolerant routine. The

distribution of control surfaces among the computers can be seen in Table 2, and the proposed computer architecture can be seen on Figure 3.

This is a relatively simple system since it does not have distributed processing as all of the flight control computations are carried out in the individual FCCs only. It does not require reconfigurable hardware since the command and monitor lanes are dedicated to their task. Therefore it is not envisaged that ARINC 629 databuses will be required since the requirement for information to be passed around the system is relatively low compared to a typical distributed architecture. The system has therefore been designed with a deliberate low requirement for information interchange between the individual components, and to make the most of the available ARINC 429 buses. Therefore it is proposed that ARINC 429 be the primary standard on this aircraft.

It is proposed that the flight control system is an extension to the Airbus A340 system. The overall Airbus system could be simplified by removing the SEC computers, and adding an additional PRIM computer to increase the availability, and to ease the problems of allocating the actuators. This would only give one form of control, therefore a second dissimilar link would be required. This could be implemented by using a reliable analogue backup within the modified PRIM computers which would simplify the certification process since it would probably be easier to demonstrate that this link is reliable compared to a second set of flight control computers.

6.2.3 Required failure monitoring

There is a requirement for an overall failure monitoring and fault management system. This will enable the failures to be logged and subsequently reported for maintenance action, as well as carrying out the overall system monitoring. Functions that are required, for the purpose of this study, are listed briefly as follows.

1. Monitoring to determine if the flight control computers controlling one elevator have both entered the analogue backup mode so that the other computer pair controlling the second elevator may do the same. This is needed so that both elevators are always being controlled by the same control law.
2. Same as 1, but for the ailerons.
3. Failure to determine if a given spoiler pair has failed, so that reconfiguration of spoiler function can take place. This reconfiguration requirement will need to be determined by the handling study.
4. Active actuator switching for the surfaces controlled by the active-standby system so that the active actuators are alternated from flight to flight in order to ensure that actuator wear is even.
5. Monitoring for the flap failures, so that this may be communicated to the control surfaces.
6. Monitoring of the sensor values through the individual flight control computers so that sensor faults may be detected and isolated. Recovery from sensor failure is not envisaged; if a sensor connected to a computer fails then it is assumed that the complete computer / sensor, and possibly actuator system will be lost.

Since maintenance is not a flight critical function, it is suggested that two maintenance computers are fitted, with dispatch being possible with one computer failed. These computers are not flight critical - if they fail then the only functions that are lost are the maintenance recording ones. However since the flight control computers require computers to be operative to detect failure, the flight control computers should revert to direct law in the event of their failure since this is the most reliable state for them to be in, and would mean that the computers were all controlling the aircraft in the same way, as opposed to one computer having failed and reverted to direct law while the others are still in normal or an alternate law. The reconfiguration information can be easily made available to the other flight control computers by giving each one its own dedicated ARINC 429 link, which would be used to broadcast any status information required. The control surface reconfigurations could be carried out independently of the maintenance system by having a lookup table within each computer which instructs a given computer what to do for a give failure state.

6.2.4 System Reliability

This section will consider the reliability of the flight control system. The following assumptions have therefore been made;

- A system will require maintenance when the probability of it being available is less than 0.95.
- A system will fail when the probability of it being available is less than 0.5.

The predicted time before maintenance merely indicates when the system may require maintenance. The system will still be functional, and will remain so until the time to failure has elapsed.

The overall reliability values have been obtained using the reliability figures in Table 3 and Table 4. The reliability values calculated will be given here, but the methodology behind them will only be given in the complete report. The values for the component reliabilities tend to be conservatively estimated. Therefore, it is often found that the components turn out to be more reliable than predicted, with systems having MTBFs of three or four times the figures initially given. Therefore it is likely that the system will be substantially more reliable than the figures suggest.

Component	Mean Time Between Failures (hours)
Hydraulic system	23,000
Actuator	51,400
ADIRS	40,000
Computing Lane (in normal mode)	35,000
Inceptor Sensor	200,000

Table 3 : Reliabilities for the Components in Normal Law

Component	Mean Time Between Failures (hours)
Hydraulic system	23,000
Actuator	51,400
ADIRS	40,000
Computing Lane (in direct mode)	100,000
Inceptor Sensor	200,000

Table 4 : Reliabilities for the Components in Direct Law.

The projected time to first maintenance action, for the flight control computers alone, is predicted at 1370 hours with the first computing failure which results in one aileron or elevator surface predicted at 5840 hours. This implies that maintenance can be deferred to scheduled maintenance periods since the elapsed time between the first failure and the system failing completely is substantial (over 4400 hours), and it can be demonstrated that the likelihood of the system failing per flight hour is sufficiently low to be able to dispatch with one computer failed. This deferral provides a significant benefit to the operator. This section will be explained in more detail in Appendix A.

Table 5 and Table 6 give the probabilities of the control surfaces failing per flight hour. The term 'Complete System' means that the reliabilities of the computers, sensors, hydraulics and actuators have been considered. The term 'Computing Only' refers to the probability of the computers and sensors alone failing. The figures for the system reliabilities have been given in Table 3 and Table 4. 'Direct law' assumes that only one control surface is required for the ailerons and elevators. 'Normal law' requires that both aileron and elevator surfaces are working. A working rudder is also required for normal law, but it can be seen that the rudder failure rate is much smaller than the aileron or elevator failure rate.

	Normal Law Failure Rate (per hour)		Direct Law Failure Rate (per hour)	
	Computing Only	Complete System	Computing Only	Complete System
Aileron and Elevator Combined	4.1×10^{-8}	1.2×10^{-7}	better than 10^{-16}	3.3×10^{-16}
Rudder Only	1.2×10^{-12}	1.2×10^{-12}	2.8×10^{-14}	4.7×10^{-13}

Table 5 : Failure rates - all computers working

	Normal Law Failure Rate (per hour)		Direct Law Failure Rate (per hour)	
	Computing Only	Complete System	Computing Only	Complete System
Aileron and Elevator Combined	1.7×10^{-4}	3.0×10^{-4}	5.6×10^{-14}	2.4×10^{-12}
Rudder Only	1.0×10^{-8}	1.6×10^{-8}	8.3×10^{-10}	8.3×10^{-10}

Table 6 : Failure rates - one computer failed

These figures show that it should be possible for the aircraft to be dispatched with one flight control computer inoperative since the requirement for failure rates of 10^{-10} per hour are met in most of the cases. The one problem is with the rudder availability when dispatching with one computer failed (Table 6) since the failure rate of the complete system does not meet the 10^{-10} per hour requirement for computing. Therefore it may be necessary to have a form of mechanical backup which would be able to control the aircraft in yaw. However, before requirement is determined, it would be necessary to perform a more detailed study.

This brief study has demonstrated that the proposed system architecture should meet the required reliability requirements. However, the handling of the aircraft with an engine failed and mechanical control must be investigated by a simulator evaluation. In practice, it is likely that a mechanical rudder will be fitted since the possible use of sidesticks would require it for the lateral mechanical backup. Therefore the dispatch with failure case would not be critical since the rudder would be able to be powered manually.

6.3 Handling Qualities

Though the handling issue is not an important part of this report, it has a major role in the choice of aircraft flight control system architecture. The handling of the aircraft will need to be evaluated with components of the system failed. Therefore the system has been designed with this requirement in mind, so that any one computer should be able to control the aircraft reasonably well in pitch, roll and yaw.

The programme will need to identify the required level of handling for a given failure case. Work done by McDonnell Douglas in this field [24,25] should help to identify the required levels required for given failures. Knowing the probabilities of the aircraft entering a certain failed condition can therefore be used to determine the required handling level. The following guidelines have therefore been suggested. The handling should be level 1 for normal flight, level 2 for landing with a degraded system, and may sometimes be level 3 under failure conditions in up-and-away flight.

A further handling requirement is that a single failure should not give a large transient, therefore there is a need to consider graceful degradation of handling under failures. Ideally, an intermediate step is required between full fly-by-wire and the mechanical backup. No single failure, no matter how remote should give a significant change in handling qualities.

7. References

1. Stanislaw, David L. *General Aviation Data Bus Update.* Cessna Aircraft Company. AIAA 84-2637. 6th Digital Avionics Systems Conference. Baltimore, Maryland. 3-6 December 1984.
2. *Flight International.* Reed Business Publications. 14 Feb. 1987.
3. Bleeg, Robert J. *Commercial Jet Fly-By-Wire Architecture Considerations.* Boeing Commercial Airplanes. AIAA 88-3900-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988.
4. Field, E.J. *Flying Qualities of Transport Aircraft: Precognitive or Compensatory?* College of Aeronautics PhD Thesis, Cranfield University. January 1996.
5. Rushby, John. *Formal Methods and Digital Systems Validation for Airborne Systems.* NASA Contractor Report 4551. December 1993.
6. *Joint Airworthiness Requirements,* Civil Aviation Authority. Large Aeroplanes; JAR-25
7. Swern, Frederic L; Bavuso, Salvatore J; Martensen, Anna L; Miner, Paul S. *A latent Fault Markov Model for a Highly Reliable Triplex Computer System.* AIAA GNC Conference 87, Monterey, CA. AIAA 87-2605. 17-19th August 1987.
8. Rushby, John. *Formal Specification and Verification of a Fault-Masking and Transient-Recovery Model for Digital Flight-Control Systems.* NASA Contractor Report 4384. July 1991.
9. Goddard, Peter L. *Convergence as a Trade-Off in System Architectural Design.* Hughes Aircraft, Fullerton, CA. AIAA 89-3083-CP. AIAA Computers in Aerospace 7 Conference. Monterey, CA. 3-5 Oct. 1989.
10. Bavuso, Salvatore J. *Impact of Coverage on the Reliability of a Fault tolerant Computer.* Langley Research Centre. NASA TN D-7938.
11. Johnson, Sally C; Butler, Ricky W. *Design for Validation.* NASA Langley. IEEE/AIAA 10th Digital Avionics Systems Conference. Los Angeles, CA. 14-17 Oct. 1991.
12. Butler, Ricky W. *The SURE Reliability Analysis Program.* NASA Technical Memorandum 87593. February 1986.
13. Butler, Ricky W; White, Allan L. *SURE Reliability Analysis.* NASA Technical Paper 2764. March 1988.
14. Mackall, Dale A. *Development and Flight Test Experiences With a Flight-Crucial Digital Control System.* NASA Technical Paper 2857. November 1988.
15. Goddard, Peter L. *Convergence as a Trade-Off in System Architectural Design.* Hughes Aircraft, Fullerton, CA. AIAA 89-3083-CP. AIAA Computers in Aerospace 7 Conference. Monterey, CA. 3-5 Oct. 1989.

16. McGough, J. *The Byzantine Generals Problem in Flight Control Systems.* Allied Signal. AIAA-90-5210. AIAA Second Aerospace Planes Conference. Orlando, Florida. 29-31 Oct. 90.

17. Walter, Chris J. *MAFT: An Architecture for reliable Fly-By-Wire Flight Control.* Allied-Signal Aerospace Company. AIAA 88-3902-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988.

18. Hills, Andy D. Mirza, Nisar A. *Fault Tolerant Avionics.* GEC Rochester, Kent. AIAA 88-3901-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988

19. Chang, Larry K. *Flight Deck and Avionic System Design for the F-93A Aircraft Project.*

20. Prahoro, Djoko. *F-93A/B Military General Purpose Large Aircraft Reliability and Maintainability Design.* College of Aeronautics, Cranfield University. May 1994.

21. Tzu-Cheng, Liang. *F93A Fly-By-Wire Flight Control System.* College of Aeronautics, Cranfield University. May 1994.

22. Lala, Jaynarayan H; Adams, Stuart J. *Inter-Computer Communication Architecture for a Mixed Redundancy Distributed System.* AIAA 87-2607. AIAA GNC Conference 87, Monterey, CA. 17-19th August 1987.

23. Sankrithi, Mirtha M K V; Bryant, W F. *7J7 Manual Flight Control Functions.* Boeing Commercial Airplane Company. AIAA GNC Conference 87, Monterey, CA. 17-19th August 1987.

24. Gillette, Darrell E; Page, MA; Hodgkinson J. *Flying Qualities Criteria for Adverse Weather.* McDonnell Douglas Corporation. AIAA-93-1191.

25. Page Mark A; Gillette, Darrell E, Hodgkinson John; Preston Jeff D. *Quantifying the Pilot's Contribution to Flight Safety.* McDonnell Douglas. MDC 92K0337. International Air Safety Seminar, Long Beach, CA. 1-5 Nov. 1992.

26. Glashagen, Claus. *Airline Requirements on Aircraft Electrical Power Generation & Distribution.* Lufthansa German Airlines. Proceedings, Aircraft Generation and Distribution Systems Conference. RAeS. 14 October 1992.

27. SPITZER, Cary R. Digital Avionic Systems: Principles and Practices. McGraw-Hill. 2nd Edition. 1993.

28. Moorhouse, David J; Leggett, David B; Feeser, Kenneth A. *Flying Qualities Criteria for Precise Landing of a STOL Fighter.* AF Wright Research and Development Center, WPAFB. AIAA-89-3390-CP. AIAA Atmospheric Flight Mechanics Conference. Boston, MA. 14-16 August 1989.

29. *Flight International.* Reed Business Publications. 11-17 April 1990.

30. *Flight International.* Reed Business Publications. 25 Apr. - 1 May 1990.

31. *Flight International.* Reed Business Publications. 29 Jan. - 4 Feb. 1992.

32. *Flight International.* Reed Business Publications. 22 Dec. 1993 - 4 Jan. 1994.

33. *Flight International*. Reed Business Publications. 27 Jan. - 2 Feb. 1993.

34. *Flight International*. Reed Business Publications. 19 - 25 Jan. 1994.

35. *Aerospace*. Magazine of the Royal Aeronautical Society. April 1995.

36. *Flight International*. Reed Business Publications. 18 - 24 Jan. 1995.

37. *Flight International*. Reed Business Publications. 13 - 19 Jul. 1994.

38. *Flight International*. Reed Business Publications. 10- 16 Aug. 1994.

39. Beale, James; Jackson, Joseph W. *British Aerospace Regional Jetliner Digital Flight Guidance Certification.* IEEE/AIAA 11th Digital Avionics Systems Conference, Seattle, WA. 5-8 Oct. 1992.

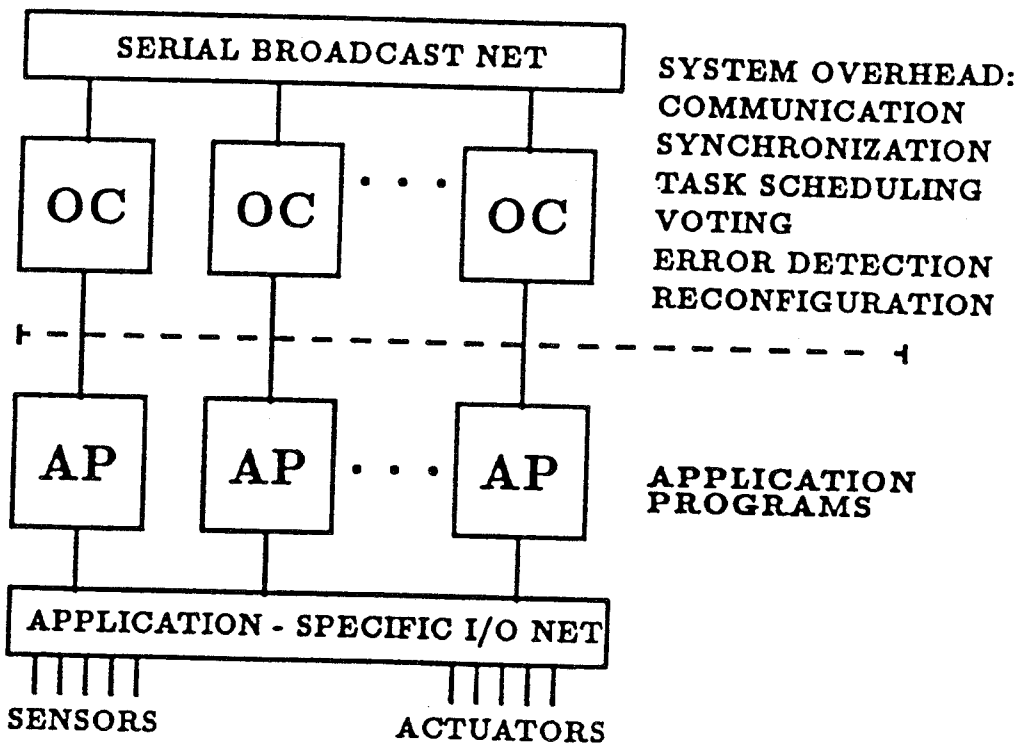
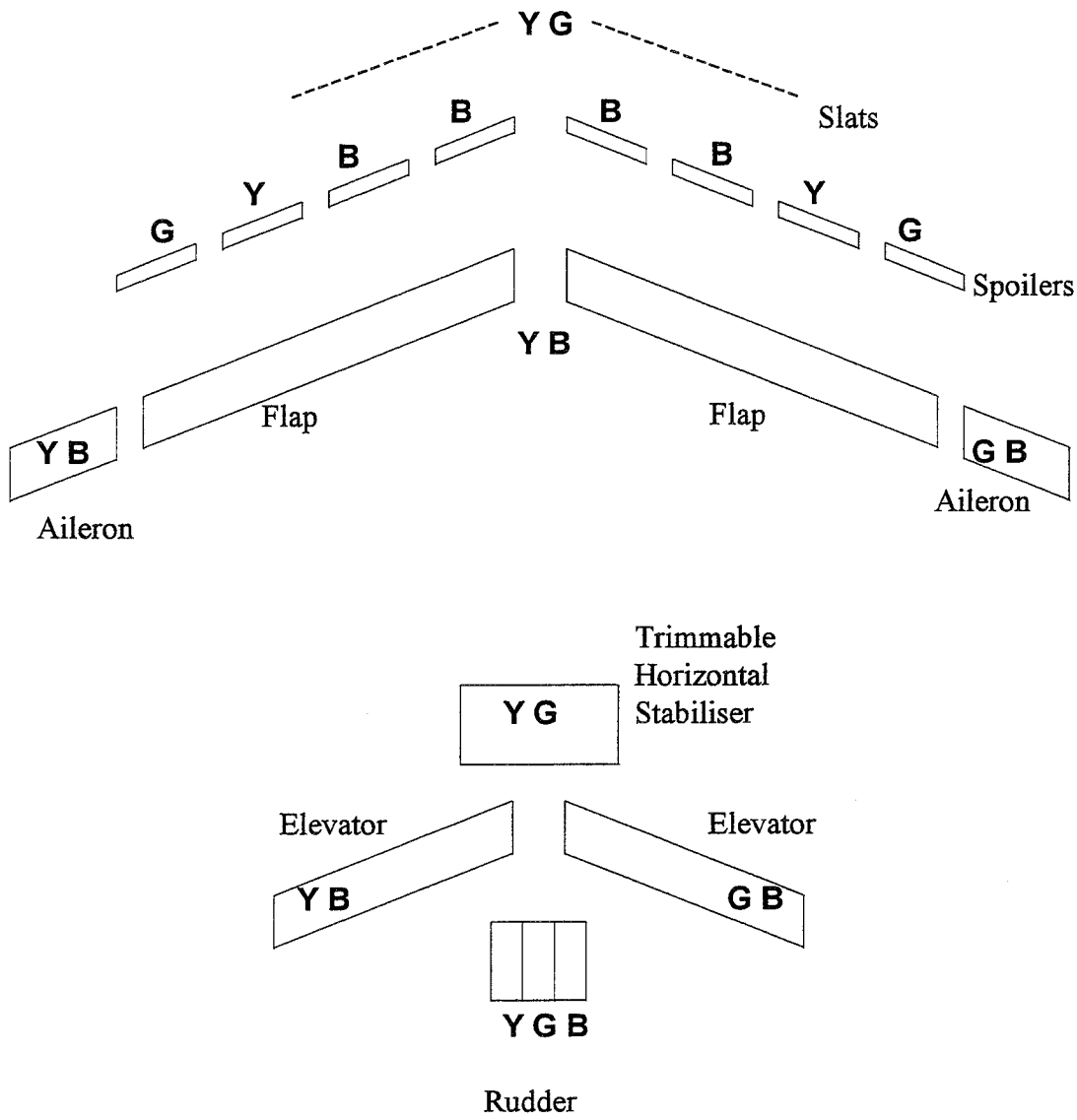


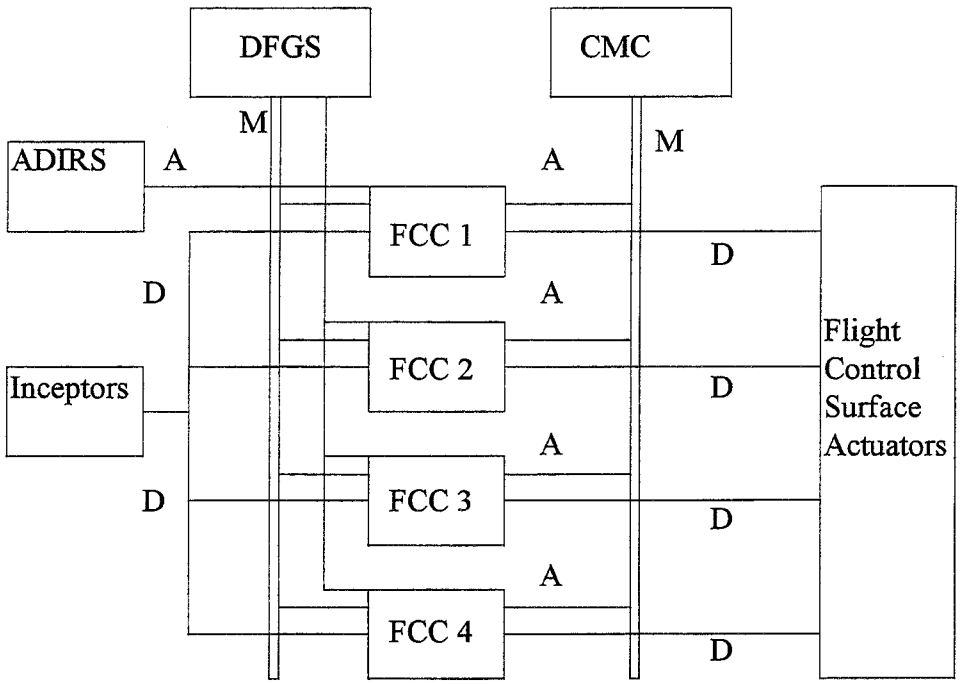
Figure 1 : MAFT System Partitioning. See Ref. [17].



Key :

G	:	Green Hydraulic System
Y	:	Yellow Hydraulic System
B	:	Blue Hydraulic System

Figure 2 : Proposed Control Surfaces and Hydraulic System Distribution



Key :

A	:	Single ARINC 429 Link
ADIRS	:	Air Data & Internal Reference System
CMC	:	Central Maintenance Computer
D	:	Direct Connection
DFGS	:	Digital Flight Guidance System
FCC	:	Flight Control Computer
M	:	Multiple ARINC 429 Link

The only direct connections are between the inceptors and FCCs, and between the FCCs and the Actuators. The rest of the connections are dedicated ARINC 429 datalinks. Individual 429 links have not been shown for clarity.

Figure 3 : Proposed Flight Control System Architecture

Appendix A. Reliability Analysis

This appendix will cover the theory that has been used to calculate the failure probabilities for the proposed flight control system, and then detail the preliminary calculations which have been performed.

A.1 Theory

In order to calculate the failure probability for a system, it is necessary to know the reliability of the system. Therefore, the mean time between failures (MTBF) is assumed to be known.

$$MTBF = \frac{1}{\lambda} \tag{A1}$$

where λ is assumed to be the number of operational defects per hour, or failure rate. Hence the failure probability can be calculated, assuming that there is an exponential relationship between the failure rate and functional probability.

$$P(Functional) = R = e^{-\lambda t} \tag{A2}$$

Assuming that the failure rate (λ) is known for a single component, the probability of survival can therefore be calculated for any time period, using equation A2. Conversely, the time to failure can be calculated, given the probability of survival, nominally 0.5 for time to failure, and a value for the failure rate.

This method can be expanded to cope with a network of failures. A reliability block diagram can be drawn which represents the network. Blocks in series represent components which must all be working for the overall system to be working. Blocks in parallel represent a number of components, of which at least one must be working for the system to be working. Therefore the diagram could be considered to be a chain, with blocks that are complete being functional, and blocks that are incomplete being non-functional. An unbroken path through the network is required for the represented system to be operational.

The overall probability for n components in series can be found by multiplying all of the individual probability figures for the individual components (R_i) together by using equation A3.

$$R(Total) = \prod_{i=1}^{n} R_i \tag{A3}$$

Similarly, for n components in parallel, the overall reliability can be found by using equation A4.

$$R(Total) = 1 - \prod_{i=1}^{n} (1 - R_i) \qquad \text{(A4)}$$

This assumes that all of the components are active at the same time, and that any switching for reconfiguration purposes has a coverage of unity, or will be 100% reliable. In a real-life situation this may seen contrived since there may be non-perfect switching involved, i.e. the coverage is not equal to 1, but it is suitable for the purposes of this analysis.

Some parallel systems (or channels) require more than one lane to be functional for the complete system to be functional. An example of this is a Boeing 777 flight control computer which requires two out of three lanes to be functional. Therefore the following formulae may be derived which will give the probability of the channel being operational, given that the probabilities for the individual lanes being operational are identical.

Number required for success	Quadruplex	Triplex	Duplex	Single
4 out of	R^4			
3 out of	$4R^3-3R^4$	R^3		
2 out of	$6R^2-8R^3+3R^4$	$3R^2-2R^3$	R^2	
1 out of	$4R-6R^2+4R^3-R^4$	$3R-3R^2+R^3$	$2R-R^2$	R

Table A1 : Reliability Probabilities for System Networks

A single channel within the flight control system may be represented as follows. The command path between the pilot is assumed to be through the inceptor sensor to the flight control computers, and thence into the actuator. The ADIRS has been included since it is required for the system to be operative in the normal mode, and the hydraulic system has been included since the actuator requires the hydraulics to be functional to drive the system. This reliability block diagram can be seen on Figure A1.

Therefore the values for the probability of a system component being functional (R) can be calculated from the mean times before failure and the sector time by using equations A1 and A2. The sector time has assumed to be 80 minutes, and the MTBF values can be found in Table A2 for the system in normal mode. The probability for the complete system can then be found by using equation A3.

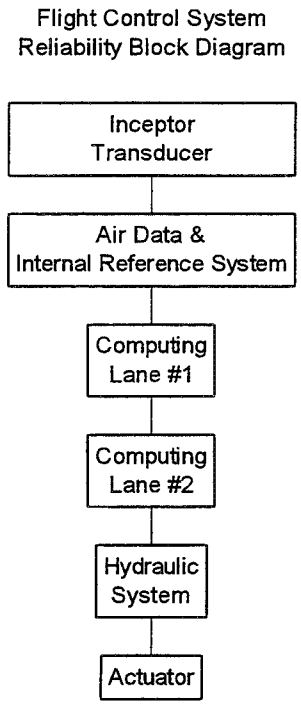


Figure A1 : Single Channel RBD

The system considered in Figure A1 only represents one flight control computer / actuator combination. In practice, each control surface will be controlled by two of these in parallel. Equation A4 can then be used to calculate the overall reliability. The reliabilities of the computing components will change as the system enters direct law from normal law. The direct law reliabilities can be found in Table A3. Note that the MTBF for the ADIRS is infinite, i.e. it will not fail. This is because it is not required for the aircraft system to be functional in normal law, and therefore has an effective MTBF of infinity, or a probability of survival of 1, and does not therefore affect the calculation.

Component	Mean Time Between Failures (hours)
Hydraulic system	23,000
Actuator	51,400
ADIRS	40,000
Computing Lane (in normal law)	35,000
Inceptor Sensor	200,000

Table A2 : Reliabilities for the Components in Normal Law

Component	Mean Time Between Failures (hours)
Hydraulic system	23,000
Actuator	51,400
ADIRS	infinite - i.e. will never fail
Computing Lane (in direct law)	100,000
Inceptor Sensor	200,000

Table A3 : Reliabilities for the Components in Direct Law.

A.2 Actual Failure Rates

Single Ail.
and Elev. RBD

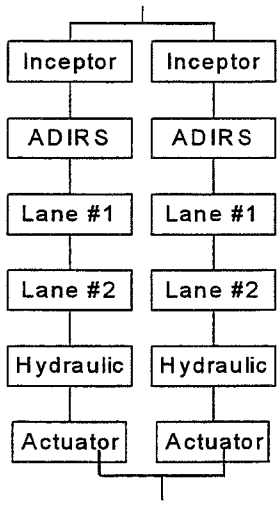


Figure A2 : Ail. & Elev. RBD

Rudder RBD
Three Channels

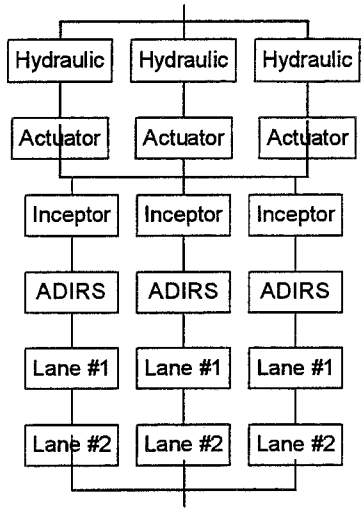


Figure A3 : Rudder RBD

The analysis above assumes a very simple system, which is only driven by one control system. In practice, there will be two of the arrangements of Figure A1 in parallel, driving the aileron and elevator surfaces in the proposed system, therefore a RBD of the form of Figure A2 is required.

For the rudder, the RBD is different because the individual flight control computers control the servo-valves, whose outputs are summed before driving the actuators. Therefore the RBD in Figure A3 has been used. This assumes that the servo-valves are 100% reliable, which is not sufficient for an in-depth calculation, but is sufficient here since the probability due to failure of the servo-valve is included with the actuator reliability, and therefore has been accounted for in the system.

A.3 One Computer Failed

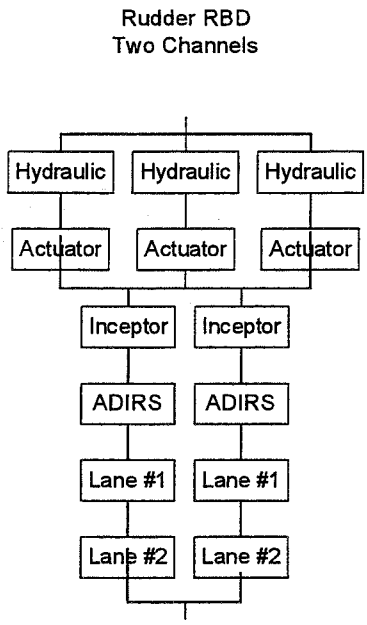


Figure A4 : Rudder RBD - One FCC Failed

With one flight control computer failed, the RBD for the different control surfaces change. The RBD for the aileron with the failed FCC in normal mode will have a RBD identical to Figure A1 since the second lane is failed. The RBD for the control surface which has not been affected by the FCC failure will be unchanged. For direct law, the RBD is assumed to be equivalent to that in Figure A2 since dispatch with failure still implies that the analogue link is still intact.

For the rudder, all of the actuators will still be available, but the servo-valve driven by the failed computer will not. Therefore the RBD will be like that in Figure A4. Again, the component of the failure probability for the servovalve has been included with the actuators.

A.4 Complete Aircraft Analysis

The probability of an aircraft being in different control modes during flight is of importance. Therefore the following assumptions will be made. For the system to be in the normal flight control law, i.e. where all of the nominal augmentation and protections are active, both of the elevator surfaces, both of the aileron surfaces and the rudder must be active. Alternate law is active while there is at least one elevator, one aileron and the rudder are active, and uses the component reliability values in Table A2. Direct law is similar to alternate law but the reliabilities in Table A3 are used.

A.4.1 Normal Law

With all FCCs working, the RBD for the normal control law can be seen on Figure A5. With one FCC failed, the RBD on Figure A6 needs to be used. The results of the calculations can be seen in Table A4. They show that the system should meet the deferred maintenance requirement since the probability of the aircraft not being in normal law is greater than 0.5 at 300 hours.

	Failure Rate per sector	P(available @ 300 hours)
All FCC working	1.2×10^{-7}	0.992
One FCC Failed	3.0×10^{-4}	0.910

Table A4 : Normal Law Reliabilities

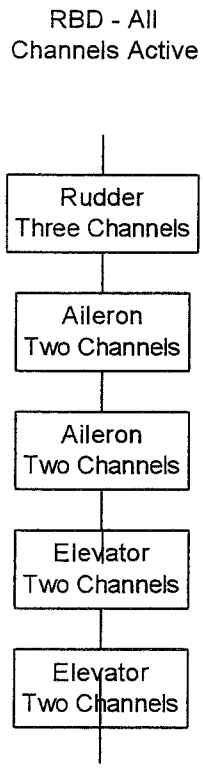


Figure A5 : Normal Law RBD

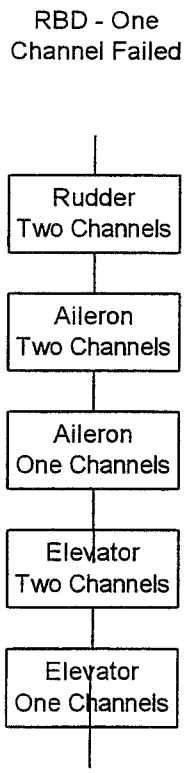


Figure A6 : Normal Law, One Channel Failed RBD

A.4.2 Alternate Law

The probability of the aircraft being in the alternate control law can be found by using the RBD in Figure A7. This assumes that one of the two elevators, one of the two rudders and the rudder are required to be working for the aircraft to be flyable.

With one FCC failed, the probability of alternate law being active can be found by using the RBD in Figure A8, and the results of these calculations can be found in Table A5.

	Failure Rate per sector	P(available @ 300 hours)
All FCC working	1.6×10^{-12}	$\cong 1$
One FCC Failed	1.0×10^{-8}	$\cong 1$

Table A5 : Alternate Law Failure Rates

Direct Law

Table A6 shows that the aircraft meets the overall reliability requirement, which is a failure rate of 10^{-9} per hour by using the component failure rates given in Table A3. The 10^{-9} requirement is met with one flight control computer failed, therefore this aircraft should be able to be dispatched with one computer failed.

	Failure Rate per sector	P(available @ 300 hours)
All FCC working	1.0×10^{-13}	$\cong 1$
One FCC Failed	4.7×10^{-10}	$\cong 1$

Table A6 : Direct Law Failure Rates

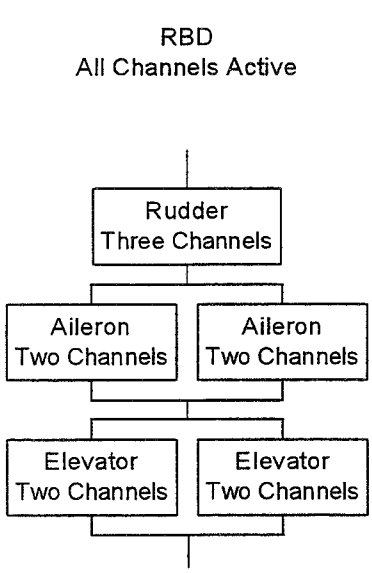


Figure A7 : Alternate / Direct Law RBD

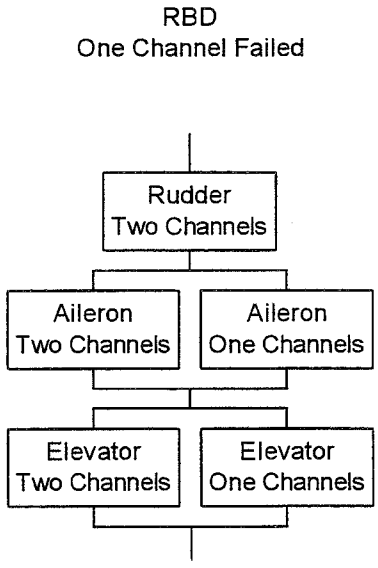


Figure A8 : Alternate / Direct Law, One Channel Failed RBD

Appendix B. Databus Technology

This section considers the databus technology available and relevant to this study, since this is an evolving technology, and can have a large effect on the system architecture. Therefore each of the relevant items will be listed, and a brief summary of its generic characteristics.

B.1 Databus Background

The choice of method of data transfer around the aircraft has an important influence on the system architecture and therefore warrants mention. Broadly, the choice is between using conventional direct connections, where one box is connected directly to another, and a databus, where a number of boxes are connected to a databus, what acts essentially like a omnibus, with people (messages) boarding the given bus route (databus) at one location (bus user), and getting off at another. The databus can reduce component weights, and facilitate the data communication within a system, but can be much more complex, and protocols are required to ensure that chaos does not arise, i.e. people getting on and off the bus at the wrong destination, and a number of people all trying to board the bus simultaneously, thus blocking the door.

For a desired multiple transmitter data bus, there are several requirements which must be guaranteed ideally for an aircraft operation, several of which are ideally suited to a commercial aircraft. First, the transmit / receive terminal, which provides the access interface to the bus, must isolate the global bus side from the local user side. Therefore a failure in a local Line Replaceable Unit (LRU) must not propagate onto the bus, therefore denying access by the other bus users. In essence, each terminal is autonomous, and separate from the others. A sample of principal requirements are;

- A terminal must not be jammed in the transmit mode,
- Error detection is required to account for noise and interference effects on the bus,
- The transmission protocol must be foolproof,
- Transit times for information transfer must be bounded, deterministic and acceptable.

B.2 Databuses Described

This section describes the common databus formats that are currently in use. A good general reference to databuses is [B1]

B.2.1 ARINC 429

In the mid 1970s, with the rapid growth in digital avionics and the need for efficient data transfer between LRUs, a new commercial digital avionics communications standard was being developed, namely ARINC 429 [B2]. This databus was first approved in 1977. The first application of the ARINC 429 system was on the Boeing 757 and 767 aircraft. It was thought, however, that the ARINC 429 single transmitter/

multiple receiver concept would be unable to handle the required amount of inter-system data transfer required for evolving commercial aircraft and would quickly be outgrown. The need for a multiple transmitter access data bus was recognised, just as it had been for military aircraft a decade earlier.

The ARINC 429 is a simplex, slow bus that is relatively easy to certify. However, it does not offer the savings in wiring that are being looked for.

B.2.2 ARINC 629

A small group at Boeing started working on the concept of a multi-transmitter data bus in 1977. This emerged 16 years later as ARINC 629 [B3], and is the primary communications standard on the Boeing 777.

The ARINC 629 digital data bus is a new system of databuses which use two way, multi-transmitter autonomous terminal controllers. Major components are the Data Bus Terminator, the Data Bus Cable Assembly and the Coupler and LRU (up to a maximum of 120). Each LRU has a ARINC 629 terminal controller and a Serial Interface Module. The ARINC 629 on the 777 has taken Boeing and its suppliers 16 years to develop.

The ARINC 629 guarantees isolation in several ways. Firstly, the access protocol logic guarantees that every connected terminal will get access in turn. There is no central bus controller. Also, the local system cannot access the bus, it is the job of the terminal to do this, and hence the local system cannot interfere with global bus operation.

Secondly, the system must have the ability to provide data at some minimum update rate. The ARINC 629 protocol logic operates in a periodic mode that guarantees periodic transmission and receipt of data. It is also designed to operate in an aperiodic mode which, in the event of a temporary or sustained bus overload condition guarantees access to every terminal in turn to the bus.

Thirdly, the data bus should be viewed as a shared resource. Every transmitters data is available to every receiver for use if required. This is supported by each terminal having a unique number, and each item of data having a label. A terminal can receive none or all of the labels and associated data on the bus.

Fourthly, the system must be able to support intra-system between both complex, e.g. a flight control computer, and a simple system, e.g. a sensor, with a user system interface flexible enough to accommodate the needs of both. The approach used in ARINC 629 is a parallel, sixteen bit word scheme, where the transmitter and receiver can be considered as memory addresses.

Once the decision was taken to incorporate the ARINC 629 onto the 777, two development paths emerged. One was for the development and production of flight quality ARINC 629 components, and one for the development of an aircraft system

application. Guaranteeing the inter-operability of the components has been the most difficult requirement to meet

B.2.3 ARINC 659

The ARINC 659 [B4] bus or SAFEbus™ [B5] is essentially similar to the ARINC 629. However, it is a backplate bus, and is destined to become the industry standard. Honeywell submitted the SAFEbus as a candidate standard for the ARINC 659 subcommittee after their receiving the Boeing 777 AIMS contract, and SAFEbus has subsequently become the draft standard.

There is no bus controller. It is a unique form of a dual-dual redundant bus. Each unit connected to the bus has a memory chip that contains details of the duration and sequence of individual frames on the bus, which correspond to individual data transmissions. For each frame, the unit therefore knows whether to transmit, receive or be idle. There are two timing bits at the end of each frame, and data rates of up to 30 Mbit/sec can be achieved. Backplates up to 1 meter long, containing 10 to 15 LRUs have operated at speeds near 50 MHz.

B.2.4 MIL-STD-1553B

This bus [B4] was first approved in September 1976, and is used virtually in all American military aircraft for avionics and electrical systems. It has many good features, but its protocol is extremely complex, making it too costly for general aviation use. No commercial integration units were planned, hence its cost is likely to remain high.

This has three main types of unit which can be attached to the bus. The first is a bus controller, which initiates information transfers and controls the bus. The second type is the bus monitor. This does not transmit, but can receive and store selected data which is being transmitted on the bus. This can be used for flight test or maintenance applications. The third type of unit is the remote terminal. This is the unit which actually receives and transmits data on the bus, under the command of the bus controller. Up to 31 of these remote terminals can be connected at any one time.

B.2.5 References

B1 Aplin, John A; Newton, I W; Warburton, I G. *A Brief Overview of Databus Technology.* Flight Controls Group, GEC Marconi Avionics. RAeS Conference, The Design and Maintenance of Complex Systems on Modern Aircraft. 6 April 1995.

B2 Stanislaw, David L. *General Aviation Data Bus Update.* 6th Digital Avionics Systems Conference. Baltimore, Maryland. 3-6 December 1984.

B3 Pottenger, Simone. *Boeing 777 629 Data Bus - Principles, Development and Application.* Boeing Commercial Aircraft Group. Advanced Avionics on the Airbus A330/A340 and The Boeing 777 Aircraft. RAeS London. 17 November 1993.

B4 SPITZER, Cary R. Digital Avionic Systems: Principles and Practices. McGraw-Hill. 2nd Edition. 1993.

B5 Hoyme, Kenneth; Driscoll, Kevin. *SAFEbus™.* Honeywell. IEEE/AIAA 11th Digital Avionics Systems Conference. Seattle, WA. 5-8 Oct. 1992.

Appendix C. Airbus A320

The Airbus A320 is a twin-engined short to medium range airliner. It was the first aircraft of its type with a flight critical, fly-by-wire flight control system. Airbus operates with the philosophy that pilots should be prevented absolutely from getting into extreme situations by the aircraft. The amount of new technology used on this aircraft is not as significant as its implementation. It presents a move away from what is generally taken to be 'conventional', which has caused some comment.

The flight control system on the A320 is essentially a derivative of the flight control system of the conventionally controlled Airbus A310. The A310 has an electrical signalling system which controls the wing spoilers, and a flight augmentation unit which provides yaw damping functions. The A320 system was developed from the A310 system. Two computers were installed which control the elevators and ailerons (ELAC computers). The three spoiler computers was upgraded so that it could control the elevators as a backup mode (SEC computers), and finally the functions of the two flight augmentation computer were enhanced.

In normal operation, all of the control surface position commands are calculated by one computer, which is nominally an ELAC, before being transmitted to all of the other computers, which then actuate the control surfaces to which they are connected. This is because no one computer is connected to all of the control surfaces. In the event of the computer in the computation task failing, control transfers to the other computers in turn, with the failed computer still actuating its surfaces if it is able to. Any one control surface (apart from the individual spoiler panels on the wing) are capable of being actuated by more than one computer, so in the event of one or more computers failing completely (i.e. in both the computation and actuation task), all of the control surfaces can still be actuated through a combination of the other computers.

The final level of backup in the event of total electrical failure for the Airbus aircraft is a direct mechanical link to the trimmable horizontal stabiliser (THS) and the rudder pedals. Although it is possible to land the aircraft with these two controls alone, it is difficult, and this mechanical backup is only intended to be used as a temporary measure while the flight control system is restored.

C.1 Power Supply Systems

C.1.1 Electrical

There are three main electrical generators on the A320. The primary electrical system is powered by two 90 kVA constant frequency generators, one on each engine. A similar generator is also fitted to the APU for use in emergencies. There are also two batteries for use when all other power sources fail. An electrical system schematic is given on Figure C1.

C.1.2 Hydraulic

The Airbus A320 has three independent hydraulic systems

1. Green system. This has a EDP on the No. 1 Engine plus a power transfer from the Yellow system. The Green system powers the rudder, yaw damper, left elevator, THS, ailerons, slats, spoilers 5 and 1 (ground spoiler), the main brakes, the landing gear and the nosewheel steering.
2. Yellow system. This is powered by an engine driven pump (EDP) on No. 2 Engine plus a power transfer from the Green system. The Yellow system powers the rudder, yaw damper, right elevator, THS, slats, the flaps, spoilers 4 and 2 (ground spoiler), the auxiliary brakes and the cargo doors.
3. Blue System. This is powered by an electrical pump, and in the case of an emergency, the ram-air turbine. This system drives both elevators, both ailerons, the rudder, the flaps and spoiler 3 (ground spoiler). It also drives an AC/DC generator for emergency power generation.

Any one hydraulic system is sufficiently to retain flight control of the aircraft.

C.2 Electronic Centralised Aircraft Monitor

The ECAM has been developed from the ECAM installed on the A-300 and A-310. It is used to indicate aircraft and engine performance, and also warning and system synoptics on two displays in the cockpit.

C.3 Centralised Fault Display System (CFDS)

This is a man-machine interface for maintenance purposes which allows the display of fault messages in plain English, the interrogation of the Built-In Test Equipment (BITE) of various electronic systems and the initialisation of system tests from a central point located in the cockpit, the Multipurpose Control and Display Unit (MCDU). The architecture of the A320 Central Fault Display System (CFDS) is the distributed type (compared with the centralised type permitted in ARINC 604. ARINC 604 is a report for the guidelines for the design of a central maintenance system (Guidelines for Design and Use of Built-In Test Equipment). This distributed architecture means that the intelligence required for formatting and processing the maintenance data is included in the BITE of each of the individual avionics components. The main advantage of this architecture is that the conditions for generating the message depend on one system only, the originator of the message. Hence information is more reliable and easier to manage. This approach does not prevent the Centralised Fault Display Interface Unit (CFIDU) from automatically correlating events, thereby minimising the number of messages, which could have been the advantage of a centralised architecture.

C.4 Flight Control System

C.4.1 Sidesticks

The sidesticks are orientated a little inboard. Travel is important. The limits are ± 16° with ± 22 lbs in pitch. Roll forces are 9 lbs inboard and 7 lbs outboard, with a stick throw of ± 20°. The roll forces are not symmetrical due to the strength of the forearm, and pilots do not notice this which suggests that it is about right.

The reason put forward for no mechanical link between the sticks is it could introduce failures that could disable both sticks, not to mention backlash, inertia and friction which is what is trying to be removed. The autopilot disengage button on the stick is used as a take-over button whereby he can disconnect the other pilot. An indicator on the glareshield shows when the stick has been disconnected but is still displaced.

Some problems that have been raised are the lack of ability to see what the other pilot is doing. Airbus state that the pilots react to the observed changes in flight path rather than the stick displacements. This is probably not true. Also you cannot feel what the other pilot is doing. Answer- having two sets of hands on the controls is a no-no, and hence this is not a problem. You cannot see what the control input is for a crosswind take-off. This is recognised by the flying control position on the PFD when the aircraft is on the ground only.

The sidestick controllers save over 56 kg on the A320.

C.4.2 Flight Control Surfaces

The primary flight controls use the following control surfaces.

a one piece rudder
A trimmable horizontal stabiliser
two independent elevators
two ailerons
four single slotted fowler flaps
5 spoilers per wing
5 slats per wing

The A320 has fairly conventional aerodynamics and therefore the control surfaces and stabilisers are conventional in size. These surfaces are driven by the different flight control computers, as shown on Figure C2.

Each elevator is driven by two electrically controlled hydraulic servo jacks. One servo is in the active control mode, i.e. is actually controlling the surface while the other is in damping mode, or doing no work, and offering little resistance to the surface movement. In the event of failure of the active servojack, the failed jack reverts to damping mode while the other servojack assumes the active mode. Some flight manoeuvers requiring high load factors may result in both servojacks momentarily being in the active mode due to the higher control surface forces. In the

case of electrical supply failure to both servojacks, they both assume the centring mode, i.e. command a 0° deflection. In normal flight, the elevators are driven from ELAC 2, in which case the left and right elevators are driven by the green and yellow hydraulic systems respectively. If a failure occurs in ELAC 2, or its associated hydraulic systems or hydraulic jacks then control automatically transfers to ELAC 1. ELAC 1 then controls the elevators via the blue hydraulic jacks. If a failure occurs in ELAC 2 or its associated systems or hydraulic jacks then control passes to SEC 1 or SEC 2 depending on the state of its associated systems.

The Trimmable Horizontal Stabiliser (THS) is driven by two hydraulic motors supplied by the green and yellow systems. These motors are commanded by either 3 electric motors or by direct command from the mechanical trim wheel located in the Cockpit. The THS is normally driven by No. 1 motor via ELAC 2. If a failure occurs in ELAC 2 then control passes to ELAC 1, and control is maintained via the No. 2 THS motor. IF neither ELAC 1 or ELAC 2 are available then control passes to either SEC 1 or SEC 2, depending on their associated systems, and to THS motor No. 2 or 3.

Each aileron is driven by two electrically controlled servo jacks. As with the elevator, one servo is in damping mode, while the other is in active mode. When the Load Alleviation Function (LAF) function is required, both jacks assume the active role to achieve the high surface deflection rates. The ailerons are normally controlled from ELAC 1, in which case the left and right ailerons are driven by the green and blue servo jacks respectively. IF a failure occurs in ELAC 1, the aileron control is automatically transferred to ELAC 2. The left and right ailerons are driven by the blue and green servo jacks respectively. In the normal mode, in the event of Blue or Green system low pressure, ELAC 2 takes over control of the affected aileron. In the case of double ELAC failure, or Blue and Green hydraulic system low pressure, all aileron servo jacks revert to damping mode, i.e. zero hinge moment.

Each spoiler is driven by one servo control which is connected to one of the three SEC computer and one hydraulic system. Surfaces are automatically retracted when a fault is detected by the appropriate SEC, or the electrical supply fails. In the case of loss of hydraulic supply, the surfaces remain at their current position, or closed if pushed in by the aerodynamic forces. If a spoiler fails, the corresponding spoiler on the opposite side will also be disabled.

The roll control surface maximum displacements for the different roll functions is shown in Table C1. The ailerons are also drooped by 5° when the flaps are extended.

	Roll	Speed Brake	Load Alleviation Function	Ground Spoiler
Spoiler 1 (inner)	-	-	-	45°
Spoiler 2	35°	20°	-	45°
Spoiler 3	35°	40°	-	45°
Spoiler 4	35°	40°	10° (35°)	45°
Spoiler 5 (outer)	35°	-	10° (35°)	45°
Ailerons	± 25°	-	25° up (15°)	25° up

Table C1 : A320 Roll Control Surface Displacements

The Load Alleviation Function (LAF) is used to relieve large structural wing loads in turbulence, and pilot authority is not modified. The LAF becomes active at a load greater than 0.3g, in which case the appropriate control surfaces are deflected. LAF is inhibited when the flaps or slats are deployed, the speed is below 200 knots or above V_{MO} + 10 knots, the slats or flaps brake is engaged (i.e. there is a problem, and they have locked in their current position) or the aircraft is in pitch alternate law without protections, or in pitch direct. If the aircraft is in alternate law with protections, the maximum deflections are increased to the figures in parenthesis. The LAF may require large control surface deflection rates, of the order of 100°/sec for the ailerons, and 250°/sec for the spoilers.

The speed brake is inhibited when in configuration FULL (i.e. full flap and slat deployment), or the angle of attack protections are active. The surfaces are always deployed symmetrically, and the roll and LAF have priority over the speed brake function. The ground spoiler is activated when the thrust levers are at idle and ground spoiler has been armed, or reverse thrust is active on either engine. The surfaces are deployed when the main landing gear oleos are compressed, and wheel spin-up has occurred.

Yaw control is provided by one rudder surface. The rudder is operated by three independently supplied hydraulic jacks, which operate in parallel, with a common mechanical input. The mechanical input receives three commands. The first is the rudder pedal input, which comes directly from the pilot's pedals. The second is the rudder trim actuator trim electrical input, from the FACs which controls the zero load position on the rudder pedals. The third is the yaw damper electrical input, computed by the two FACs. The yaw damper actuator is controlled by either the green or yellow hydraulic system. Autoflight commands and turn co-ordination commands received from the ELACs are also computed by the FACs, and transmitted via the yaw damper actuators. There is no feedback to the rudder pedals from the turn co-ordination or yaw damper functions. In normal operation the three hydraulic servo jacks are driven by the green hydraulic servo actuator controlled by FAC 1. A yellow servo actuator controlled by FAC 2 remains synchronised, and will take over in the event of failure. The rudder and pedal deflection is limited as a function of speed. Each limiter channel is monitored by its associated FAC. In the event of double FAC

failure, specified circuitry in each FAC selects the 'low speed' position when the slats are extended. Rudder trim is achieved by two electric motors acting at the artificial feel unit. In normal operation, FAC 1 and motor 1 are driving, with FAC 2 and motor 2 remaining synchronised as a back-up.

The schematic for the Slat and Flap system is shown on Figure C3. The slats and flaps are driven by two Slat and Flap Control Computers (SFCC). There are five leading edge slats, two trailing edge flaps and the aileron droop is achieved by signals directed from the SFCC through the ELAC computers. The slats and flaps are driven through similar hydromechanical systems consisting of power control units, differential gearboxes / torque shafts and rotary actuators. Each SFCC then controls one hydraulic motor in both of the flap and slat PCUs. The SFCC monitor the surface positions through Position Pick-off Units (PPU) located at the PCU and at the outer end of the transmission torque shafts. Brakes installed within the torque shaft system and controlled by the SFCC prevent asymmetric operation. There is also a pressure off brake, located between the PCU and the gearboxes which lock the position when no input is being applied to the PCUs. Slat and flap position information is fed back to the ECAM. If one SFCC is inactive, both slats and flaps will operate at half speed. If one hydraulic system is lost, then the appropriate slats or flaps will operate at half speed. The slats are also inhibited from retracting at low speed or high angle of attack.

C.4.3 Flight Control Computers

The A-310 and A-300-600 have partial FBW systems, and hence the A320 system was an extension from these. The A320 is full fly-by-wire in pitch and roll. Pitch trim and rudder remain mechanical to ensure survivability in the event of a total electrical failure. Three distinct types of computer are used, each with different software. A table with the flight control computers and the control surfaces that they control is given on Table C2. The overall system architecture can be seen on Figure C4. There are 7 computers :

2 Elevator and Aileron Computers (ELAC)
2 Spoiler and Elevator Computers (SEC)
2 Flight Augmentation Computers (FAC)

The ELACs and SECs are manufactured by separate divisions of Sextant Avionique to ensure maximum dissimilarity. All of the computers are DC powered, and are fed by four sensitive accelerometers near the CG, and three ADIRS (ADC + IRS). The ELACs are the primary computers with the SECs as the secondary ones. The function of the ELAC and SEC computers are identical, except in roll the ELACs control the spoilers via the SECs. The ELACs control the aircraft in pitch in the normal control law by sending commands to the left hand and right hand elevators, and long term commands to the Trimmable Horizontal Stabiliser (THS). The normal law is a C* command. In roll, the ELACs control the ailerons, and also send spoiler demands to the SECs, which control the spoilers. The ELACs cannot drive the spoilers directly. Under failure conditions, either with the ELACs or SECs failed, a different roll law is used.

Control Surface	Primary Computer	Backup Computer	Hydraulic
Left Elevator 1 (outboard)	ELAC 1	SEC 1	B
Left Elevator 2	**ELAC 2**	SEC 2	G
Right Elevator 2	**ELAC 2**	SEC 2	Y
Right Elevator 1 (outboard)	ELAC 1	SEC 1	B
Trimmable Horizontal Stab 1	**ELAC 2**	-	G & Y
Trimmable Horizontal Stab 2	ELAC 1	SEC 1	G & Y
Trimmable Horizontal Stab 3	SEC 2	-	G & Y
Left Aileron 1 (outboard)	ELAC 2	-	B
Left Aileron 2	**ELAC 1**	-	G
Right Aileron 2	ELAC 2	-	G
Right Aileron 1 (outboard)	**ELAC 1**	-	B
Rudder Servo-Actuator 1	FAC 1	-	G
Rudder Servo-Actuator 2	FAC 2	-	Y
Spoiler 1 & 10 (outboard)	SEC 2	-	G
Spoiler 2 & 9	SEC 1	-	Y
Spoiler 3 & 8	SEC 1	-	B
Spoiler 4 & 7	SEC 3	-	Y
Spoiler 5 & 6 (inboard)	SEC 3	-	G

Computers in **BOLD** are the nominal controllers

Table C2 : Airbus A320 Flight Control Computer and Control Surface Distributions

Elevator and Aileron Computer (ELAC)

On the A320, the two ELAC computers were independent. Within each primary computer there are two control units for self-monitoring, which use different software. If P1 suffered a failure from, say, loss of feedback then P2 would take over in the master role. P1 would remain in the execution environment unless it suffered a computer fault, when it would be relieved of the execution task.

Each ELAC contains a pair of MC 68000 processors. One is the command unit, and the other is used as a monitoring unit to check the performance of the command unit. Dissimilar software is used in the pair of processors as a fault tolerance technique. Each ELAC fits a standard ARINC 600 6 Modular Concept Unit (MCU) LRU.

Spoiler Elevator Computer (SEC)

In the pitch channel, the ELACs and SECs perform exactly the same function with the same control laws. If both of the ELACs are inoperative then the aircraft is controlled solely by two of the three SECs which will take over the pitch control of the aircraft in the alternate control law. The aircraft should handle exactly as with the normal control law, but many of the envelope protection features will be unavailable, including alpha protection and pitch attitude protection. All of the computers are self-monitored.

The SECs contain a pair of Intel 80186 processors. As with the ELAC, one processor is the command unit, and the other is the monitoring unit. Dissimilar software is used in the pair of processors as a fault tolerance technique. Each SEC fits a standard ARINC 600 8 MCU LRU.

Flight Augmentation Computer (FAC)

Yaw control is achieved through the use of the FACs signalling the rudder actuators, although the FACs receive their signals from the ELACs and the SECs. In the event of a total EFCS failure, a mechanical connection between the rudder pedals and the rudders is maintained in order to allow for lateral control.

C.4.4 Databuses

A fully equipped ARINC 700 digital databus is installed, which includes advanced digital automatic flight control and flight management systems. The Automatic Flight Control System (AFCS) integrates functions from the autopilot and the Flight Management System (FMS). There are several ARINC 429 databuses for each of the ELACs, SECs and FACs. These are used to interface with the other flight control computers, plus the air data and internal reference systems. The pilot's inceptors and actuators are connected directly (i.e. hardwired) to the appropriate flight control computer.

The engines are fully digitally controlled through the FADEC system (Full Authority Digital Engine Control), which comprises the electrical signalling from the inceptors and flight management system to the engines, and also the associated sensors and control units on the engine itself. The databuses for each engine's FADEC is a dual system since there is no mechanical backup.

C.5 Handling and Control Laws

The A320 control laws are based on the C* concept. On the ground, the feedback systems cannot be used, and therefore the stick is connected directly to the controls. Pitch rate feedback is an exception to this, and may be used in the derotation phase after landing.

Take-off

The aircraft commences he ground roll in direct law, i.e. with the control surfaces commanded directly by the stick. The C* law is phased in 1 second after takeoff over 1½ seconds. During landing it is phased out when the aircraft descends below 100 ft. In the event of a radio-altimeter failure the C* law may exist down to the ground. The only disadvantage to this is an extended landing flare. The sidestick also directly commands the ailerons and spoilers in roll when the aircraft is on the ground. The ground is sensed when the undercarriage oleos are compressed.

Up and Away

Away from the ground at low speed, pitch rate and normal acceleration have equal power over the control law. Above 210 kts, the pitch rate feedback is linearly reduced until it is zero. Above this speed it is solely used as a loop stabilisation term. Hence the pilot will demand acceleration, and thus flight path. To the pilot, the aircraft will appear neutrally stable. There is also an automatic trimming system that allows the sidestick to recentre over the short term. This results in a constant elevator deflection, that is then neutralised over the long term by trimming the horizontal stabiliser. Both of these functions are carried out automatically. The autotrim function is disabled when the aircraft is below 100 ft.

The lateral sidestick movement commands roll rate up to a roll angle of 33°. The spiral stability is zero up to a roll angle of 33°, and then positive spiral stability is introduced up to the maximum roll angle of 67°. The maximum roll rate available to the pilot is limited at 15°/sec, though greater power is available to the aircraft systems. These limits are 40°/sec, and at times 70°/sec and are available to the system to resist atmospheric disturbances etc. Also, single or multiple surface failures will have no apparent effect on the roll command as the computer will increase the deflections on the other surfaces to compensate. The maximum roll angle is also reduced at high angle of attack, i.e. when the angle of attack protection is operating to 45°. If the high speed protection is operative, then positive spiral stability is induced for all roll angles, and the maximum roll angle is limited to 40°. This ensures there is some performance margin left for recovery.

The rudder is operated in parallel by the FAC and also via the ELAC to provide yaw damping, turn co-ordination, rudder travel limiting and engine failure compensation. The last one of these is of interest, above 100 ft on takeoff an engine may be stopped with the pilot taking no corrective action at all. During this scenario, the aircraft banks 7 or 8°, and then turns at about 1°/sec in heading in a stable pitch attitude. Conventional cues remain to identify the failed engine.

Landing

The landing control law is phased in when the aircraft is passing 50 feet on the radar altimeter. The pitch attitude is memorised, and as the aircraft passes through 30 feet, a 2° pitch down is introduced over 8 seconds. This means that the pilot must continue to pull back on the sidestick to hold the pitch attitude, and subsequently flare the

aircraft. This ensures that pilot is out of the centre dead-band on the stick, and a monotonic stick force is continually present. In the event of the pilot having to land the aircraft in the normal C* law, the handling is marginally modified, with the pilot possibly having to push forwards on the stick as well as pulling back, and the landing flare may also be extended.

C.5.1 Protections

As previously mentioned, this aircraft has a hard protection system. The attitude limits are +35° -15° in pitch, ± 65° in roll reduced to 30° at high angle of attack and reduced to 40° above the high speed warning. Above a certain angle of attack specified for each configuration, the C* law will give way to an angle of attack command. This will produce a slight flight path discontinuity which is the first warning of entry to the high alpha region. In order to continuing the alpha increase, a continuous full back stick movement must be made requiring a high force. As alpha continues to increase, alpha floor will operate and Take-Off/Go-Around (TOGA) thrust will be applied, at a point 2° beyond the onset of alpha protection. Autothrottle is always active in the A320. Alpha will stabilise at the limit, in a steep pitch attitude at this point. Alpha max. is chosen to give stability at the limit and the aircraft will never enter a clean aerodynamic stall. For dynamic entries, alpha floor can be phased advanced, i.e. if the pilot's demand is more than 50%, the alpha floor will operate at entry into the alpha range.

The overspeed protection is employed to stop the aircraft going too fast. In practice it means that the flutter and divergence speeds can be reduced, and hence the structure can be made lighter. The overspeed protection is operative at V_{MO} + 6 knots or M_{MO} + 0.01. Overspeed is guarded against by reducing the effect of the trim, and the system demanding up to 1.75g to ensure recovery. Finally, the A320 has the first active gust and manoeuvre load alleviation function on a large civil transport.

C.5.2 Failures and Alternate Modes

The loss of the three internal reference systems (IRSs) would cause the selection of the pitch direct law, where the elevator is directly coupled to the stick. Here, the total elevator available is determined by the CG position, and also the flap position. A complete failure of the EFCS in pitch, requiring failure of both ELACs and SEC 1 and 2 would require the aircraft to be flown using the pitch trim wheel as manual backup. The autopilot only controls the aircraft through the ELACs.

Laterally, the aircraft remains in roll normal law for most of the flight, the only exception being when the aircraft is on the ground when it is in roll direct. Under the following conditions, it will revert to roll direct.

Failure of :

1. 2 Air Data Reference or 2 Internal Reference or Pitch Normal Loss - Ailerons and Spoilers Roll direct.
2. 2 ELAC or B and G hydraulic systems or 2 Ailerons - Spoilers Direct Only.
3. All Spoilers - Ailerons Only.
4. 2 FAC or G & Y Hydraulic Low Press or 3 Air Data Reference or 3 Internal Reference - Ailerons + Spoilers

Yaw alternate only becomes active if roll normal fails. Yaw alternate is when only the yaw damping function is available, and its authority is reduced to ±5° rudder.

Under an engine failure condition, the optimal sideslip angle is shown on the pilot's PFD. This is not necessarily zero, being a function of the throttle setting, aircraft configuration etc., and is calculated to achieve optimum climb.

C.6 Bibliography

Anon. *A320 Flight Crew Operating Manual.* Airbus Industrie.

Chatrenet, D. *Flight Simulation and Digital Flight Controls.* Handling Qualities Department. Aerospatiale, Toulouse. ICAS-90-0.2. Published by AIAA.

Corps S.G. *Airbus A320 Side Stick and Fly-by-Wire - An update.* Airbus Industrie. SAE Paper 861801.

Flight International. Reed Business Publications. Page 29. 14 Feb. 1987.

Field, E.J. *Flying Qualities of Transport Aircraft: Precognitive or Compensatory?* College of Aeronautics PhD Thesis, Cranfield University, January 1996.

Grossin, Jean; Schuster, Patrick. *A330/A340 Central Maintenance System: Philosophy, Implementation and In-Service Use.* Advanced Avionics on the Airbus A330/A340 and The Boeing 777 Aircraft. RAeS London. 17 November 1993.

PALLETT, E H J, COLYLE S. Automatic flight control. 4th edition. Blackwell, 1993.

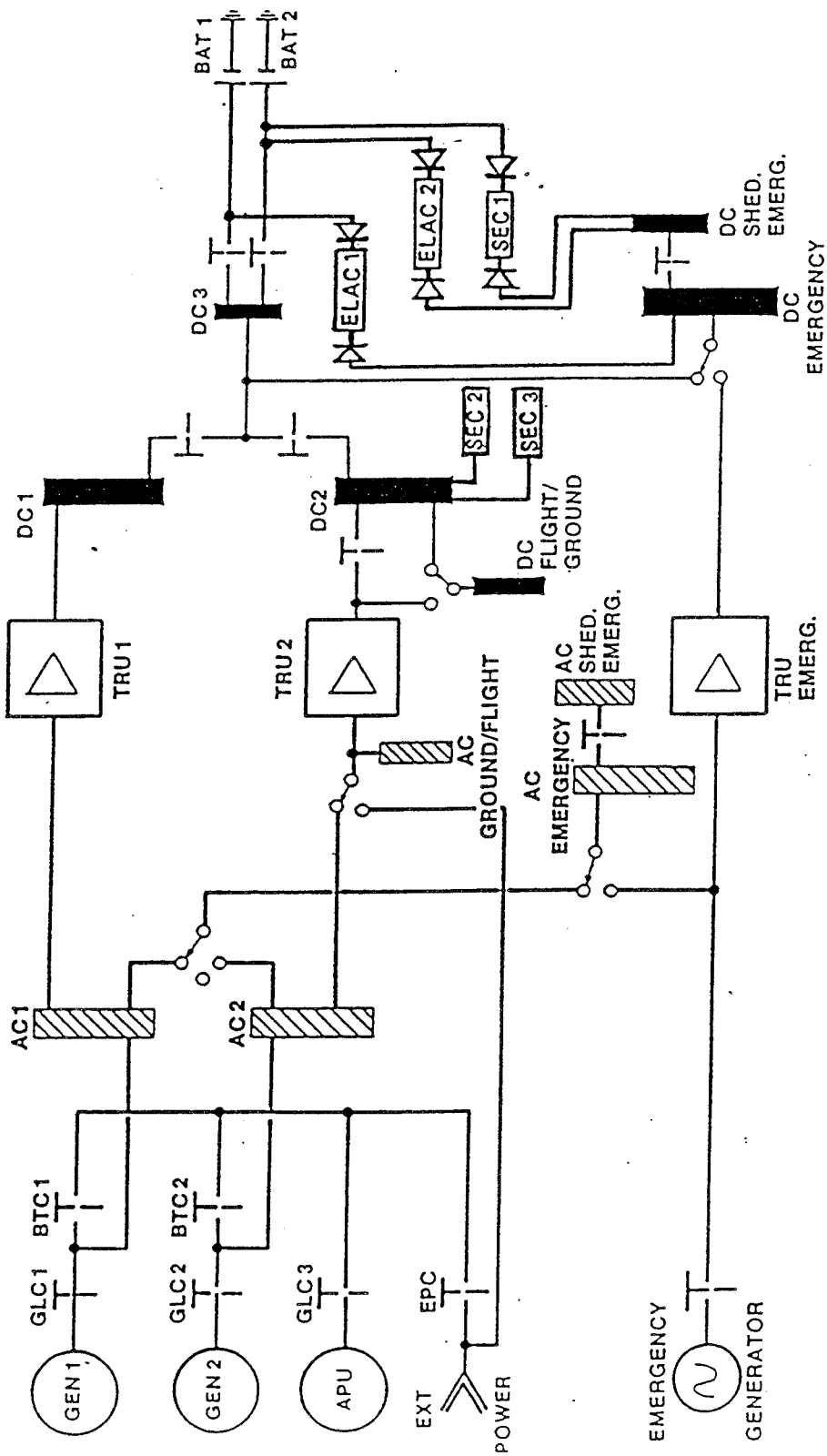
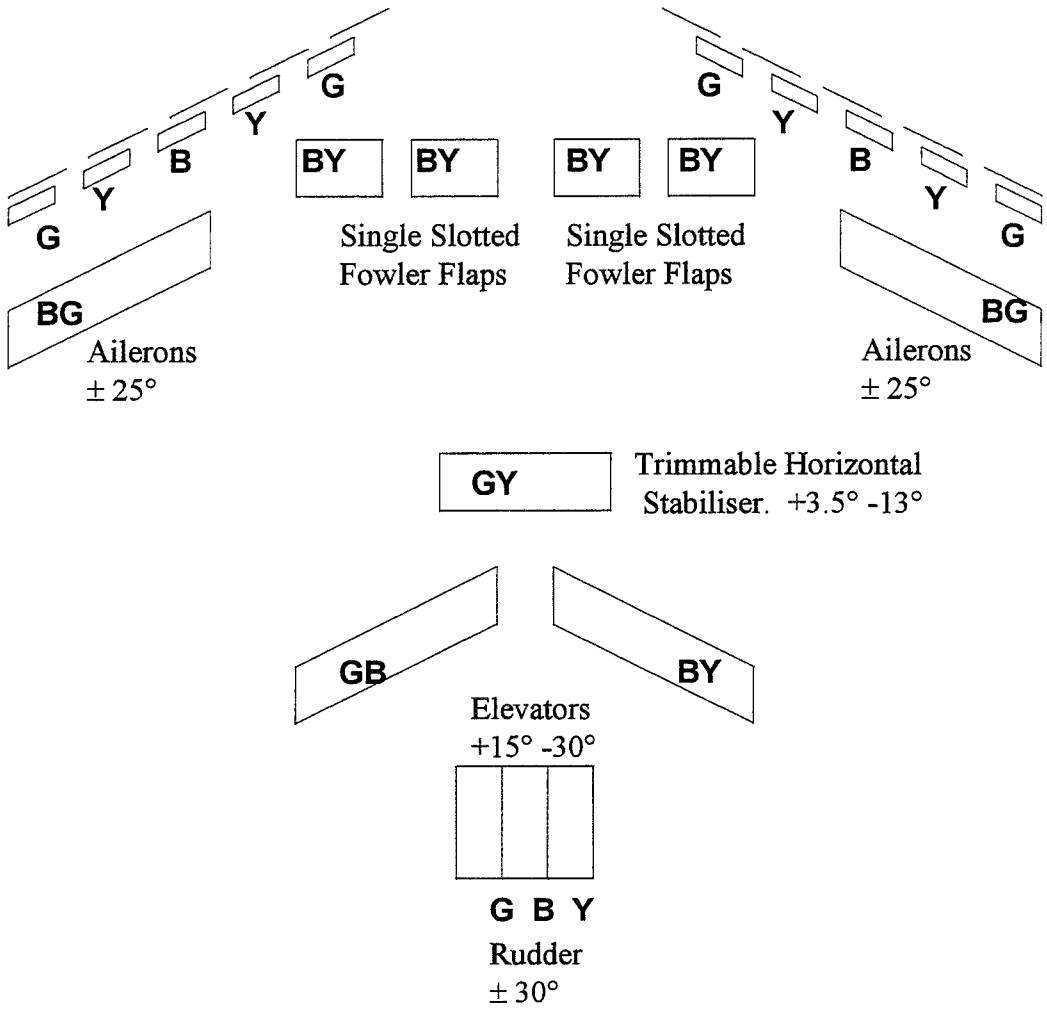


Figure C1 : Airbus A320 Electrical System



Key :

G	:	Green Hydraulic System
B	:	Blue Hydraulic System
Y	:	Yellow Hydraulic System

Figure C2 : Airbus A320 Control Surfaces and Hydraulic System Architecture

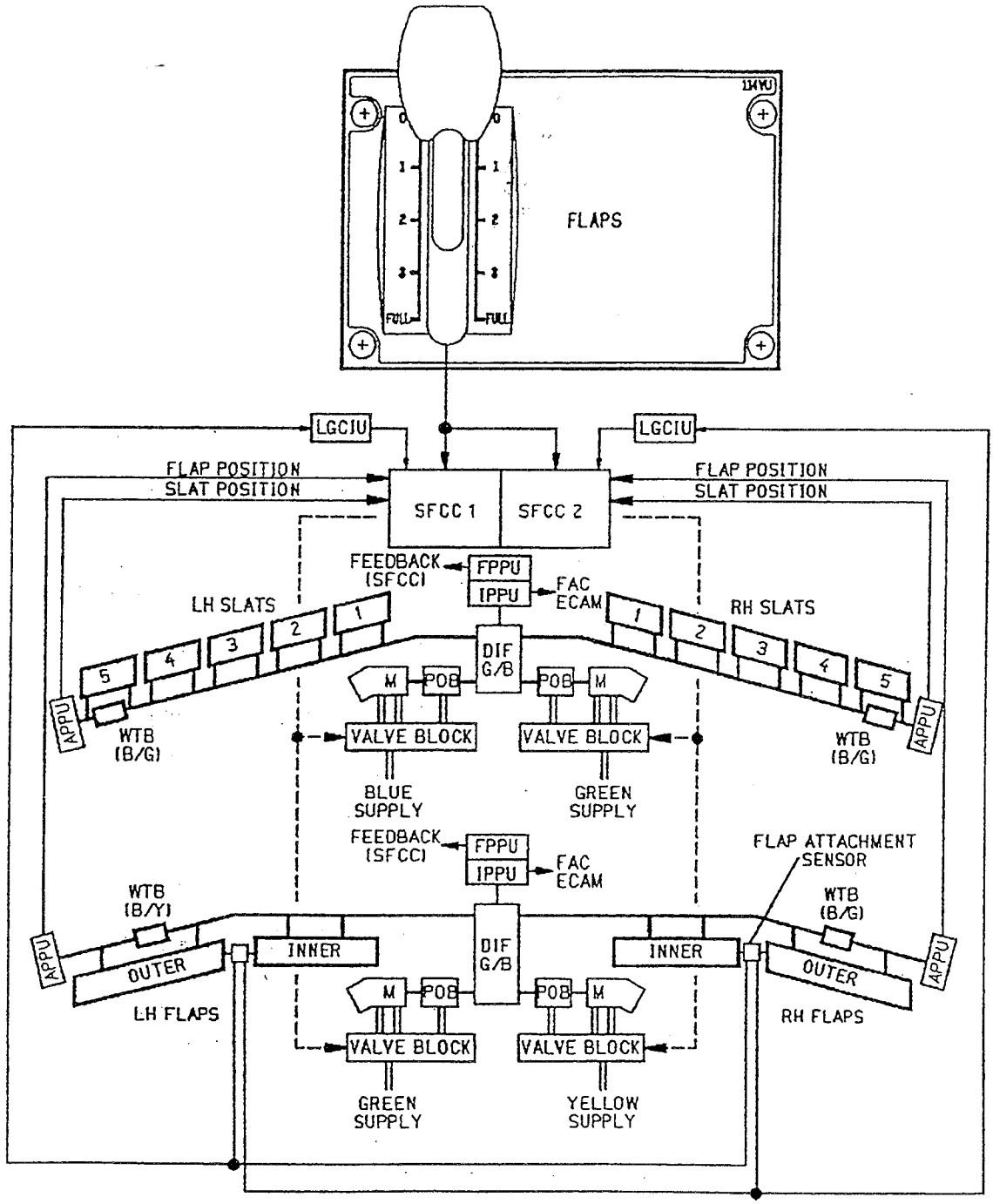
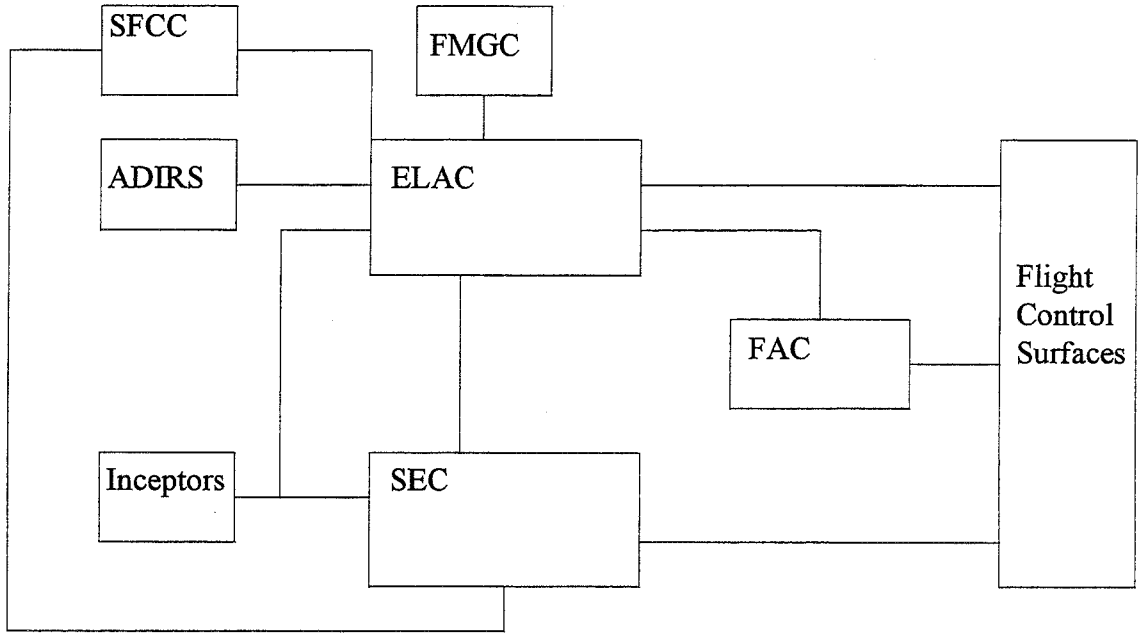


Figure C3 : Airbus A320 Flap and Slat System Schematic



Key :

ADIRS	:	Air Data & Internal Reference System
ELAC	:	Elevator & Aileron Computers
FAC	:	Flight Augmentation Computers
FMGC	:	Flight Management Guidance Computers
SEC	:	Spoiler & Elevator Computers
SFCC	:	Slat & Flap Control Computers

Figure C4 : Airbus A320 Flight Control System Architecture

Appendix D. Airbus A330 and A340

The Airbus A330 and A340 are a twin programme, and it is the first time that an aircraft has been produced with both two and four engines respectively. Both aircraft have essentially the same passenger and freight capacity. The four-engined A340 is optimised for long range missions and is also effective at shorter ranges, while the A330 offers better airline operating costs where the long ranges are not required.

The aircraft are very similar, and many of the features are engineered in the same way on the two aircraft, without suffering a penalty. As a result, the two aircraft use the same spare parts (except the engine related parts), the same aircrew and airports, and have cost almost the same to develop as a single aircraft.

The flight control systems of the A330 and A340, which are essentially identical, were a derivation of the A320 system. The ELACs, which are now known as flight control primary computers (FCPC) were modified slightly to enable them to control some of the spoiler panels and the rudder as well as the ailerons and elevators. The number of SEC computers, now known as flight control secondary computers (FCSC), was reduced from three to two since they were being little used, and their function was also enhanced to enable them to control the ailerons, as well as the elevators and some of the spoilers. The flight augmentation computers could therefore be removed since their function was now covered by the new primary and secondary computers. The principal behind the computation remained the same as the A320 however, with one computer performing all the calculations, and driving the actuators through all of the other computers.

D.1 Power Supply Systems

The A330 is designed to land safety under full systems control with no engine driven generators by using the drop down ram air turbine. For ETOPS reasons there are also two generators per engine, an electrically powered standby hydraulic pump, a quick start auxiliary power unit and a 30 minute reserve battery. Otherwise this aircraft is very similar to the A340 in terms of systems structure.

The pneumatic systems have not been covered since they play no part in power generation of flight control, although they are used for engine starting, de-icing, pressurisation of the cabin and hydraulic systems etc.

D.1.1 Electrical

A schematic of the A330 / A340 electrical systems can be found on Figure D1 and Figure D2. There are four electrical generators, one on each engine, with a nominal power of 75 kVA. If they are all unavailable during flight, the APU or the RAT could be used for electrical power generation. The APU generator is rated at 115 kVA. The emergency hydraulically-powered generator is rated at 5.5 kVA (with the Green hydraulic system being engine powered), or 3.5 kVA (with the green system being RAT powered), and has a Constant Speed Motor Generator. The battery may be phased in for slat extension for this latter case. The A340 electrical system retains

the integrity advantage of having a split-bus system, which is usually only found on twin-engined aircraft. It also has the load transfer capability allowing similar flexibility to the parallel-bus system of other four-engined aircraft. The A340 has a Garrett APU which is capable of starting two engines at once.

If the A340 looses a generator, another will automatically take-over. If the APU is operative, this will be the generator phased in. If it is not operative then the generator on the same side of the aircraft will take over. If this generator is not available then the opposite side external generator will take over, which covers the double failure case.

The A330 AC system has two larger generators on each engine (115 kVA IDG), supplying the same split-bus system as the A340 and a higher-powered generator to supply the added ETOPS loads on a twin-engined aircraft. In addition, there is an APU generator (also 115 kVA) and an emergency hydraulic driven generator, supplying about 8 kVA. Finally there is a static inverter to supply AC power from the batteries. The DC system has three Transformer Rectifiers (TR) which are all used to supply a DC split system. In addition, one TR is dedicated to the APU battery. There are an additional two batteries which provide an autonomous source for some DC powered equipment during transient phases during emergency generator activation.

In normal flight, each engine driven generator supplies its own busbar on the A330, or split bus on the A340. In addition, the essential busbars are normally supplied by No. 1 AC busbar. AC busbar No. 1 also supplies DC bus No. 1 and similarly with AC bus 2 and DC bus 2. The battery DC bus is supplied from DC 1 bus or alternatively DC 2 bus. The DC essential busbar is supplied from AC 1 bus via the Essential TR or from the DC BAT bus. see fig AL. With the DC system, a failure to supply one of the DC buses results in DC 1 and DC 2 being tied and supplied through the same TR. The failure to supply the BAT BUS from the batteries can be rectified by supplying it from DC 1 or DC 2. In the event of complete loss of main generation, the DC Essential busbar is supplied automatically from the emergency generator via the essential TR.

The aircraft can be dispatched with one AC generator failed, as the remaining generator will supply both busbars. With a complete loss of AC generation, an emergency generator will supply the ESS busbars and the AC STAT INV busbar.

A maximum of 75 kVA is allocated for the galley services in flight. In flight, maximum galley power is available providing all main generators are operating. Automatic galley shedding is provided though to ensure overload conditions do not occur. A standard option is available to increase galley power to 90 kVA.

Both electrical systems have been designed for smooth operation in series, with strict attention paid to proper fault transient behaviour in user systems, and a no-break power transfer capability to eliminate the normal transients due to the generator switching that occurs when the APU and engines are started up and shut down at the gate.

D.1.2 Hydraulic

The A330 and A340 control surface and hydraulic system distribution can be seen on Figure D3. The aircraft hydraulic systems are the same, with minor adjustment for engine-related features. For example, there is one pump per engine on the A340, and two pumps per engine on the A330. The ram air turbine used on the A330 as a back-up power source is used on the A340 to improve the engine-out flight envelope. The Airbus A340 has three independent hydraulic systems :

1. Green system. This has a EDP on the No. 1 and No. 4 engines. There is also an electrical pump, plus the Ram Air Turbine (RAT) for emergency use.
2. Yellow system. This is powered by an engine driven pump (EDP) on No. 3 Engine, plus an electrically driven pump for emergency use, and a hand pump for operating the cargo doors on the ground.
3. Blue System. This system has an EDP on the No. 2 engine, plus an auxiliary electrically driven pump.

The A330 has the same hydraulic users, but has a slightly modified power generation system. The systems use the following forms of generation.

1. Green system. This has a EDP on No. 1 and No. 2 Engines plus a RAT driven pump. There is also an auxiliary electrical pump.
2. Yellow system. This is powered by an engine driven pump (EDP) on No. 2 Engine, plus an electrical pump. There is also a hand pump for operating the cargo doors on the ground
3. Blue System. This system has an EDP on the No. 1 engine, plus an auxiliary electrically driven pump.

In flight, the engine driven pumps normally operate continuously, with the electrical pumps being switched off. On the ground, the electrical pumps are used to pressurise the systems, and to top-up the systems if required during flight. The RAT extension is automatic in the case of shut down of both engines.

D.2 Electronic Centralised Aircraft Monitor

System information is provided by the Electronic Centralised Aircraft Monitor (ECAM) consisting of the engine/warning and systems displays on the two central display screens in the cockpit. Sensors throughout the aircraft continuously monitor the systems, and if a parameter moves out of range, they warn the pilot. During normal flight, the ECAM presents system displays according to the flight phase, showing the systems in which the pilot is interested. The pilot can, by manual selection, interrogate any system at any time. Should a fault occur which results in the cascading of other systems, ECAM identifies the originating fault and presents the needed checklists without any need for additional crew actions.

D.3 Cabin Intercommunication Data System

This is a flexible system which allows the cabin to be changed without rewiring the aircraft. It also offers opportunities in operating and testing the cabin systems, with lower maintenance costs and weight than previous systems.

D.4 Central Maintenance System

This enables troubleshooting and return-to-service testing to be carried out rapidly, with a high degree of confidence from the cockpit. Much of the information available can be accessed remotely, giving the aircraft the ability to be greeted on arrival by a maintenance engineer that has information concerning the defect, and with the knowledge of the LRU which is likely to require replacement.

The CMS includes fully redundant Central Maintenance Computers (CMCs), with number 2 being a hot spare. Four user interfaces are provided, the three MCDUs, an A4 printer, the ACARS management unit (MU) and the Multipurpose Disk Drive Unit (MDDU). The ACARS MU is used for preparation of the work during the next transit. Both CMCs are connected to 48 systems, with 11 optimal systems, which represent 102 reporting units. The systems have been divided into three types and each member system, via their BITE detects, memorises and transmits to the CMC, the failure message in clear English.

To cope with increased complexity, the CMCs have been split into three modes of operation.

1. The reporting mode, active in flight, records all events linked to maintenance actions to be performed on the ground. Reports are provided at the end of each flight, but the system can also be interrogated by the crew during flight.
2. The interactive mode, active on the ground, offers help to the maintenance crew. Various reports, status and LRU identification are provided, as well as troubleshooting tests.
3. The servicing report is provided to monitor servicing options.

The CMS bring the system to a level of definition stated as an objective by the ARINC 624 report, On-Board Maintenance System (OMS). The system is based around an English language user interface. It allows storage of system BITE data within each LRU, provides ground test capabilities for LRU replacement, it is integrated with BITE fault isolation procedures and it takes a step forward to On-Board Maintenance Documentation (OMD).

D.5 Auto-Flight System

This system comprises the following elements. There are two Flight Management Guidance and Envelope Computers (FMGEC). These perform flight planning and navigation functions and also performance and prediction calculations. The data is displayed on the MCDUs. The flight guidance functions are Autopilot, flight Director and Autothrust. These computers also compute the speed envelope, the wind

shear and alpha floor detection and consolidate the flight phase and aircraft configuration computations. Various flight guidance modes are available, both vertically and laterally, which interface with the autopilots/ flight directors and autothrust.

The three Multipurpose Control and Display Units (MCDU) are used to create the flight plans, perform the required navigation interface and sequence the waypoints and flightpath deviations.

The Flight Control Unit (FCU) is used for flight mode selection, and is positioned on the pilot's glareshield. It also allows control of the autopilots and autothrust, and displays the selected data for the thrust and vertical/ lateral modes.

The two FMGECs are interfaced with the FCU and two MCDUs. The FCU is installed in the glareshield and has three independent processors used for AFS and EIS control. The two FMGEC are installed in the avionics compartment. They acquire signals from associated systems sensors and provide output commands to the control surfaces via the Electronic Flight Control System and to the engines via the FADEC. The systems which interface with the FMGECs are

Two full authority FADECs. These are used to limit the available thrust depending on ambient conditions and prevent engine abuse and mishandling. The thrust levers are non-moving when in autothrust, and have the following detents, which the lever can be moved into. These are (from the front rearwards) Take-Off/Go-Around (TOGA), Maximum Continuos Thrust /Flex Take-off (MCT FLX TO) and Climb (CL).

There are also two Fuel Control and Management Computers (FCMC), three Air Data Internal Reference Systems, plus other navigation and database units.

D.6 Flight Control System

Those aircraft systems that are liable to in-service change now have facilities for updates to be included in situ on the aircraft.

D.6.1 Flight Control Computers

The FBW architecture is identical in the A330 and A340, though different to the A320. There are three primary computers (PRIM) and two secondary computers (SEC) replacing the ELACs, SECs and FACs. The software functions are very similar. As with the A320, only switches in the cockpit with white captions require re-setting during checks, those with amber captions clear when all systems are powered up. The minimum equipment list allows dispatch with one PRIM or SEC unserviceable. This will reduce the chance of crews having to land in alternate or direct law, which is important since the crews will probably not be landing this aircraft very often. The flight control system architecture can be seen on Figure D4.

The A-310 and A-300-600 have partial FBW systems, and learning from its' A320 experience, Airbus have made several changes to the A340 flight control architecture system. From the A320 experience it was found that the secondary computers were not being used frequently, therefore they went for a simpler secondary computer on the A340. Using three rather than two primary computers also provides more flexibility and redundancy. This allows the system to remain for longer within the normal control law envelope before having to revert to another law.

The digital flight control system has two main tasks: computing the control laws and execution which is calculating the electrical signals required by the actuators. There are three primary computers and two secondary computers in total. The flight control system is a derivative from the A320, with detailed changes having been introduced reflecting the longer mission times, especially for the A340, to provide better system availability, and the opportunity has been taken to reduce the backup modes that the crew need to use, making the aircraft easier to fly.

Primary Computers

The flight control primary computers (FCPCs) are based on Intel 386s and the three different computers are designed by different teams to minimise software errors. They are designed to provide the normal, alternate and direct control laws. In the event of a FCPC developing a fault, the next computer takes over the computation, and the computer with the failure carries out the execution task alone. In a failure-free environment, computer P1 has priority. P1 computes the surface deflection orders which the other computers operate on. P1, P2 and P3 communicate, providing for graceful degradation and the greater availability of normal law. The FCPCs are the only computers capable of controlling the aircraft through the autopilot. In normal flight, the primary computers control the Horizontal Stabiliser, the elevators, some spoilers, ailerons and the rudder yaw damper.

Secondary Computers

The flight control secondary computers (FCSCs) are both of the same design, based on Intel 186s. In the event of all the primary computers failing in the execution task, they can take over, although they can only control the aircraft in the direct control law. In normal operation they control the spoilers and limit the rudder travel. In the event of failure of the primary computers, the secondary computers take over the actuation of the elevators, ailerons and rudder yaw damper in addition to their normal functions. The autopilot cannot fly the aircraft through them.

Other Systems

Dual Flight Management Systems (FMS), integrated with the Flight Guidance and Flight Envelope computing functions combine the information from the aircraft navigational sensors. The FMS allows the pilots to select an optimal flight plan from a selection in the airline navigational database, and allows the aircraft to fly the sector automatically, though the flight director or the autopilot.

D.6.2 Databuses

The avionics are highly integrated for optimal crew use and optimal maintenance. As with all new and derivative Airbus aircraft since 1981, the primary bus standard is ARINC 429, with ARINC 600 packaging. Other industry bus standards are used in specific applications where ARINC 429 is not suitable. As with the A320, the inter-computer communications are via the databuses, as are the air data and internal reference systems. The actuator electronics and inceptor sensors are hard-wired to the appropriate sensors.

D.6.3 Flight Control Surfaces

This aircraft has drooping ailerons that also function as flaps for takeoff and landing, with spoiler panels used as ground lift dumpers. It was found that gust load alleviation not necessary due to the larger aircraft. However manoeuvre load alleviation has been employed. This moves the centre of lift inboard and hence reduces the wing bending moment.

There are the following control surfaces

2 ailerons per wing
6 spoilers per wing
trimmable horizontal stabiliser
two elevators
one rudder
seven slats per wing

These surfaces are driven by the different flight control computers, as shown on Table D1.

Each elevator is driven by two independent hydraulic servo control units. One servo is in the active control mode, i.e. is actually controlling the surface while the other is in damping mode, or doing no work, and offering little resistance to the surface movement. In the event of failure of the active servojack, the failed jack reverts to damping mode while the other servojack assumes the active mode. In the case of electrical supply failure to both servojacks, they both assume the centring mode, i.e. command a 0° deflection. In normal flight, the commands are processed by PRIM 1 or 2, or SEC 1 or 2 in the event of failure of both PRIMs.

The Trimmable Horizontal Stabiliser (THS) is driven by two hydraulic motors supplied by the blue and yellow systems. These motors are commanded by either 3 electric motors, one commanded by each PRIM, or by direct command from the mechanical trim wheel located in the Cockpit. Direct law or mechanical backup has priority over any other command.

Control Surface	Primary Computer	Backup Computer	Hydraulic
Left Elevator 1 (outboard)	PRIM 2	SEC 2	B
Left Elevator 2	**PRIM 1**	SEC 1	G
Right Elevator 2	**PRIM 1**	SEC 1	G
Right Elevator 1 (outboard)	PRIM 2	SEC 2	Y
Trimmable Horizontal Stab 1	**PRIM 1**	-	B & Y
Trimmable Horizontal Stab 2	PRIM 2	-	B & Y
Trimmable Horizontal Stab 3	PRIM 3	-	B & Y
Left Out. Aileron 1 (out)	**PRIM 3**	-	Y
Left Out. Aileron 2	SEC 1	-	G
Left Inner Aileron 1	**PRIM 1**	SEC 1	G
Left Inner Aileron 2	PRIM 2	SEC 2	B
Right Inner Aileron 2	**PRIM 2**	SEC 2	G
Right Inner Aileron 1	PRIM 1	SEC 1	B
Right Out. Aileron 2	**PRIM 3**	-	Y
Right Out. Aileron 1 (out)	SEC 2	-	G
Rudder Servo-Actuator 1	**PRIM 1**	SEC 1	G
Rudder Servo-Actuator 2	PRIM 3	SEC 2	Y
Spoiler 1 & 12 (outboard)	SEC 2	-	Y
Spoiler 2 & 11	SEC 1	-	G
Spoiler 3 & 10	SEC 1	-	Y
Spoiler 4 & 9	SEC 3	-	B
Spoiler 5 & 8	SEC 3	-	B
Spoiler 6 & 7 (inboard)	SEC 3	-	G

Controls in **BOLD** indicate the priority servocontrols

Table D1 : Airbus A330 / A340 Fight Control Computer and Control Surface Distribution

Each aileron is driven by two electrically signalled servocontrols which are connected to two computers for the inboard aileron (PRIM 1/2 and SEC 1/2) or one computer for the outboard aileron (PRIM 3 or SEC 1/2). As with the elevator, one servo is in damping mode, while the other is in active mode. In the event of the RAT providing all the Green Hydraulic power, the outboard aileron servo controls are in damping to minimise hydraulic demands. Above 300 kts, the outboard ailerons are centred to prevent any inversion problems.

Each spoiler is driven by one electro hydraulic servo control which is connected to one specific computer and one hydraulic system. The roll control surface maximum displacements for the different roll functions is shown in Table D2.

	Roll	Speed Brake	Manoeuvre Load Alleviation	Ground Spoiler
Spoiler 1 (inner)	-	35°	-	35°
Spoiler 2	35°	20°	-	50°
Spoiler 3	35°	20°	-	50°
Spoiler 4	35°	20°		50°
Spoiler 5	35°	20°		50°
Spoiler 6 (outer)	35°	20°		50°
Inner Ailerons	± 25°	15° up	-	25° up
Outer Ailerons	± 25° not above 300 kts	15° up not above 300 kts	-	25° up

Table D2 : Airbus A330 / A340 Roll Control Surface Displacements

The roll demand has priority over the speed brake function. If one spoiler surface fails to extend, the corresponding surface on the other wing is also inhibited. The lift augmenting function, which is where the ailerons droop to increase lift when the flaps are extended has priority over the speed brake function.

Yaw control is provided by one rudder surface. The rudder is operated by three independently supplied hydraulic servo control units, with a common mechanical input. The mechanical input receives three commands. The first is the rudder pedal input, which comes directly from the pilot's pedals. The second is the rudder trim actuator trim electrical input, from the SECs which controls the zero load position on the rudder pedals, since artificial feel is provided. The third is the yaw damper electrical input, computed by either the PRIMs, or in the event of their failure, the SECs. Autoflight commands are computed by the PRIMs, and are transmitted to the rudder by the yaw damper servo actuator and the rudder trim actuator. In the case of loss of both yaw damper actuators, the yaw damping function is provided by the spoilers, in which case at least one working spoiler pair is required.

The schematic for the Slat and Flap system is shown on Figure D5. The slats and flaps are driven by two Slat and Flap Control Computers (SFCC). There are seven leading edge slats, two trailing edge flaps and the aileron droop is achieved by signals directed from the SFCC through the PRIM computers. The slats and flaps are driven through similar hydromechanical systems consisting of power control units, differential gearboxes / torque shafts and rotary actuators. The control lever position is obtained from the Command Sensor Unit (CSU) by the two SFCC. Each SFCC then controls one hydraulic motor in both of the flap and slat PCUs. The SFCC monitor the surface positions through Position Pick-off Units (PPU) located at the PCU and at the outer end of the transmission torque shafts. Brakes installed within the torque shaft system and controlled by the SFCC prevent asymmetric operation.

There is also a pressure off brake, located between the PCU and the gearboxes which lock the position when no input is being applied to the PCUs. Slat and flap position information is fed back to the ECAM.

D.7 Handling and Control Laws

Take-off

There is a direct connection between the stick, and elevator and aileron input while the aircraft is on the ground. Several seconds after the aircraft has rotated, the longitudinal C* normal law is blended in, and the roll law assumes roll rate. The aircraft has neutral roll stability up to a roll angle of 33°, hence no constant inputs need to be held. Up to the maximum roll angle of 67°, a constant input must be held. Releasing the sidestick at a roll angle of greater than 33° will result in the roll angle reducing until this value is reached.

Up-and-Away

In the normal control law, the aircraft is flight path stable, using a modified C* law. The stick demand corresponds to normal acceleration, i.e. flight path rate when the speed is above 250 knots. When the speed is below this value, the control law is a combination of normal acceleration and pitch rate. Trimming is carried out automatically, hence requiring no pilot action. However, the trimwheel moves in response to the demands commanded by the flight control system. The lateral normal control law is pitch rate, with neutral spiral stability up to 33°, and positive spiral stability from this value up to the maximum demandable roll angle of 67°. There is automatic yaw compensation, hence requiring no action by the pilot. No pilot elevator input is required with turns up to 33° either, though back stick is required for bank angles greater than this value. The rudder pedals command a combination of sideslip and bank angle. A pedal input with no sidestick lateral input results in a stabilised sideslip and bank angle, for use when de-crabbing in a crosswind. The aircraft handling is also virtually unaffected by the CG position.

The normal control law provides neutral static stability and short-term attitude stability, automatic longitudinal trimming, automatic elevator in turn, dutch roll damping and turn co-ordination. The aircraft will also hold pitch attitude as long as it is within the limits of 30° nose-up and 15° nose-down and within the normal speed envelope. The alpha protection mechanism is the same as for the A320. The direct control law is the same as in the A320 for both pitch and roll. In the alternate law, the response in both pitch and roll is the same as the normal law, with rate demand in roll. The A320 reverts to direct command for the alternate roll law. With the direct law, protections are lost, and trimming is carried out with a manual control wheel.

Landing

In order to allow a conventional flare, the landing law is phased in at a given radio height. At this height, the aircraft pitch attitude is memorised, and the sidestick is used to control the pitch attitude with reference to this value in the longitudinal axis. This allows a conventional flare which takes account of ground effect.

D.7.1 Protections

The A340 has hard protection, i.e. the pilot can be restrained from exceeding the flight envelope. This is done by limiting the load factor to prevent structural overstressing, limiting the speed and mach number, both at the stall and at the high speed end of the envelope, and finally preventing the aircraft from entering extreme attitudes, both in pitch and roll.

The FBW system has a maximum pitch rate limitation to prevent a tail strike at take-off. It also has a maximum mach number and a maximum speed limitation in the control laws. The A320 only has a maximum speed limitation. This is done by reducing pilot authority as the speed increases past the critical value.

The protection at low speed is the same as the A320. The A340 normal control laws also provide alpha protection in much the same way as they did for the A320. This eliminates the risk of stall in high dynamic manoeuvres or wind shear conditions. When V_{MO} + 6 knots, or M_{MO} + 0.04 is reached, automatic up elevator is introduced, with a reduced pitch down authority being applied. The maximum roll angle is also limited to 40°, and spiral stability introduced regardless of the bank angle. The maximum stabilised speed attainable with full forward stick is V_{MO} + 16 knots or M_{MO} + 0.04.

A high lift coefficient can be maintained by holding the stick fully back without exceeding the stall angle of attack. The maximum angle of attack is set so that there is no buffeting even in an extreme dynamic manoeuvre. The maximum angle of attack permitted is approximately 3 to 5° below the stall alpha. This allows good roll manoeuvrability to be retained. This function is active from take-off to landing. There is also a load protection limitation which is +2.5/-1g without spoilers deployed or +2/0g with the spoilers deployed. This still enables a rapid pull-up to 2.5g to be made.

The angle of attack limiting system works as follows. When $alpha_{prot}$ is reached, the sidestick reverts from C* to angle of attack demand. The maximum bank angle is limited to 45° under this condition. Alpha max is obtained if the sidestick is pulled fully back, but when released, the aircraft returns to $alpha_{prot}$. If the sidestick is pushed further forward in this condition, the aircraft returns to conventional C*. If alpha -floor is reached, which is an angle of attack between alpha prot and alpha max, TOGA power is applied.

The pitch attitude is limited to 15° nose down and 30° nose up (25° under low speed conditions). This is to enhance the effectiveness of AOA and high speed protection in extreme conditions and in windshear encounter by reducing pilot authority at extreme attitudes.

D.7.2 Failures and Alternate Modes

The control law is normal law under nominal operating conditions, and with up to a single failure of sensors, electrical system, hydraulic system or flight control computer. According to the nature of subsequent failures, it automatically reverts to alternate law, direct law or the mechanical backup. Mechanical backup is intended to sustain aircraft control during a temporary complete loss of electrical power, and comprises longitudinal control through the elevator trimwheel, and lateral control through the rudder pedals.

A revision to the alternate control law requires 2 failures in the flight control which gives the aircraft handling qualities similar to a conventional aircraft. The probability of this occurring is 10^{-5} per flight hour, or 10^{-3} with the aircraft operating at its minimum dispatch equipment list. This law has identical ground and take-off modes to the normal law. The landing mode is a reversion to direct law under gear extension. The sidestick pitch command is the same as the normal law, but the roll demand is a direct stick-to-aileron coupling, the gearing of which is configuration dependent. Yaw damping is still available, and is also configuration dependent. The protections are lost except for load factor limitation. However, conventional aural stall and overspeed warnings are provided. Automatic pitch trim is still available. In the alternate law, high static stability is induced at the stall warning as in a conventional aircraft with a full forward centre of gravity. As the speed increases, the pitch law reverts. In the alternate law, high speed is also unprotected, but warned.

Further FCS failures, which have a probability of 10^{-7} (or 10^{-5} under the minimum dispatch list) would revert the A340 to direct laws. The ground and take-off modes are identical to normal law. However, there is a direct stick to surface gearing in all three axes, which is CG and configuration dependent. All hard protections are lost, though aural speed warnings are provided as with the alternate law. Trimming is possible through the manual trim wheel. This law is equivalent to flying an aircraft without the stability augmentation system engaged.

To sustain the aircraft under temporary complete electrical power loss, a mechanical backup is provided on the elevator trim and rudder pedals.

The speed tape display on the PFD will show the appropriate speeds and speeds at which the warnings will occur in the appropriate flight conditions. These displays depend on the flight law being used. If the automatic pitch trim is not available, this is also warned.

Under engine failure conditions, the handling characteristics are non-conventional. With no corrective action, the aircraft becomes stabilised in roll and sideslip angle, with a slowly diverging heading in a safe flight condition. This will provide the pilot with the necessary cues to identify the failed engine. Then trimming with the rudder

will remove the sideslip, and then the heading can be stabilised with a sidestick input. Steady flight will then be possible with no pilot control inputs. The EFCS will display a sideslip target on the pilot's PFD, which may not necessarily be zero, for example in the case of a high asymmetric thrust on one side.

D.8 Bibliography

Aerospace. The Royal Aeronautical Society. Oct. 1992.

Aerospace. The Royal Aeronautical Society. June 1993.

Aerospace. The Royal Aeronautical Society. Aug. 1994.

Anon. *A330 Technical description. Volume 3A Systems.* Airbus Industrie. Issue 1. January 1990.

Anon. *A340 Flight deck and systems briefing for pilots.* Airbus Industrie. Issue 1. May 1990

Anon. *Airbus A340-200. Standard Specification.* Airbus Industrie. Issue 2. June 1990

Aviation Week and Space Technology. McGraw-Hill. 13 July 1992

Flight International. Reed Business Publications. 15 June 1991

Flight International. Reed Business Publications. 8-14 July 1992.

Flight International. Reed Business Publications. 2-8 September 1992.

Flight International. Reed Business Publications. 13-19 Oct. 1993. P.49 - 53.

Potocki de Montalk, P. *The Avionics of the A330/A340.* Cockpit Avionics Engineering, Airbus Industrie. Proceedings; Advanced Avionicvs on the A330/A340 and the Boeing 777 Aircraft. RAeS, London. 17 November 1993.

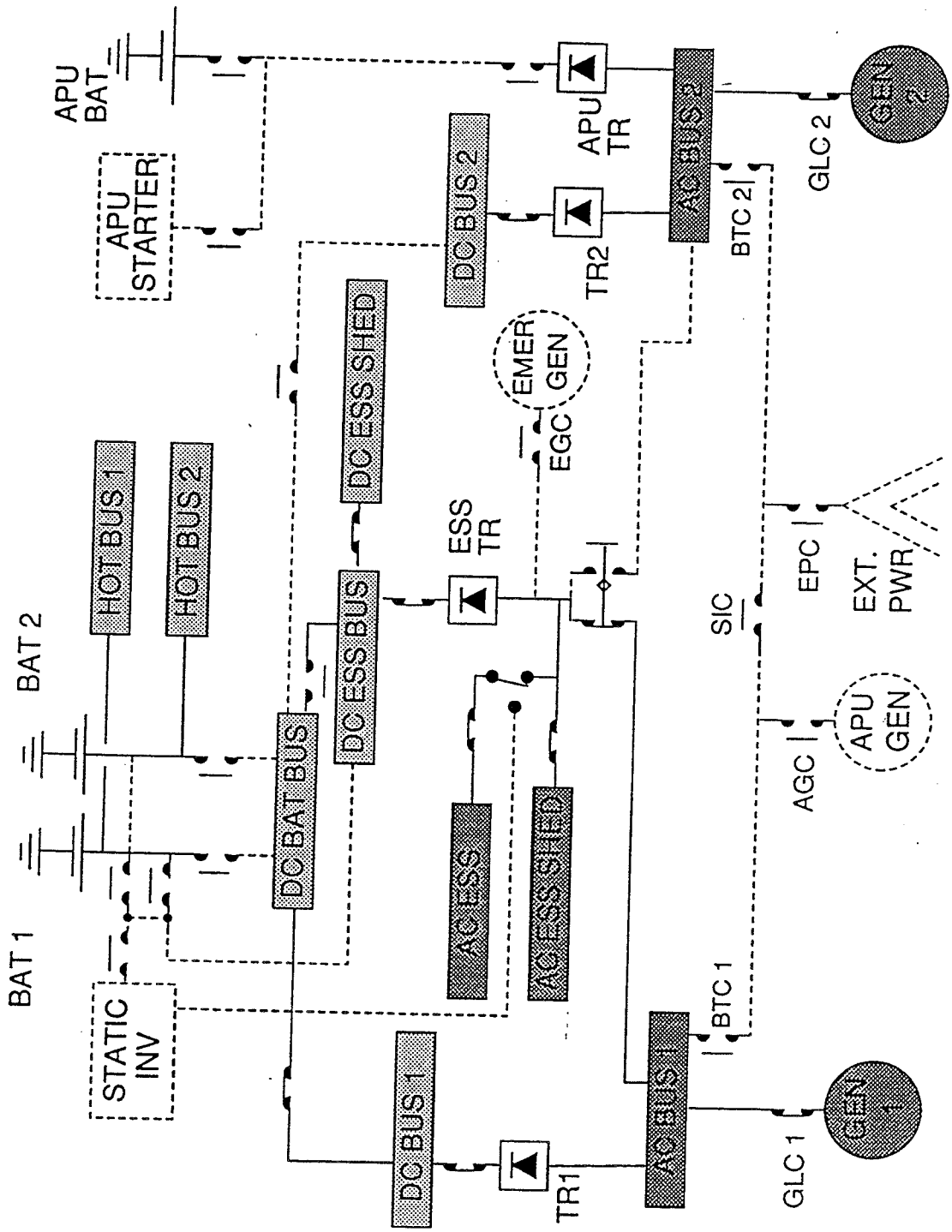


Figure D1 : Airbus A330 Electrical System

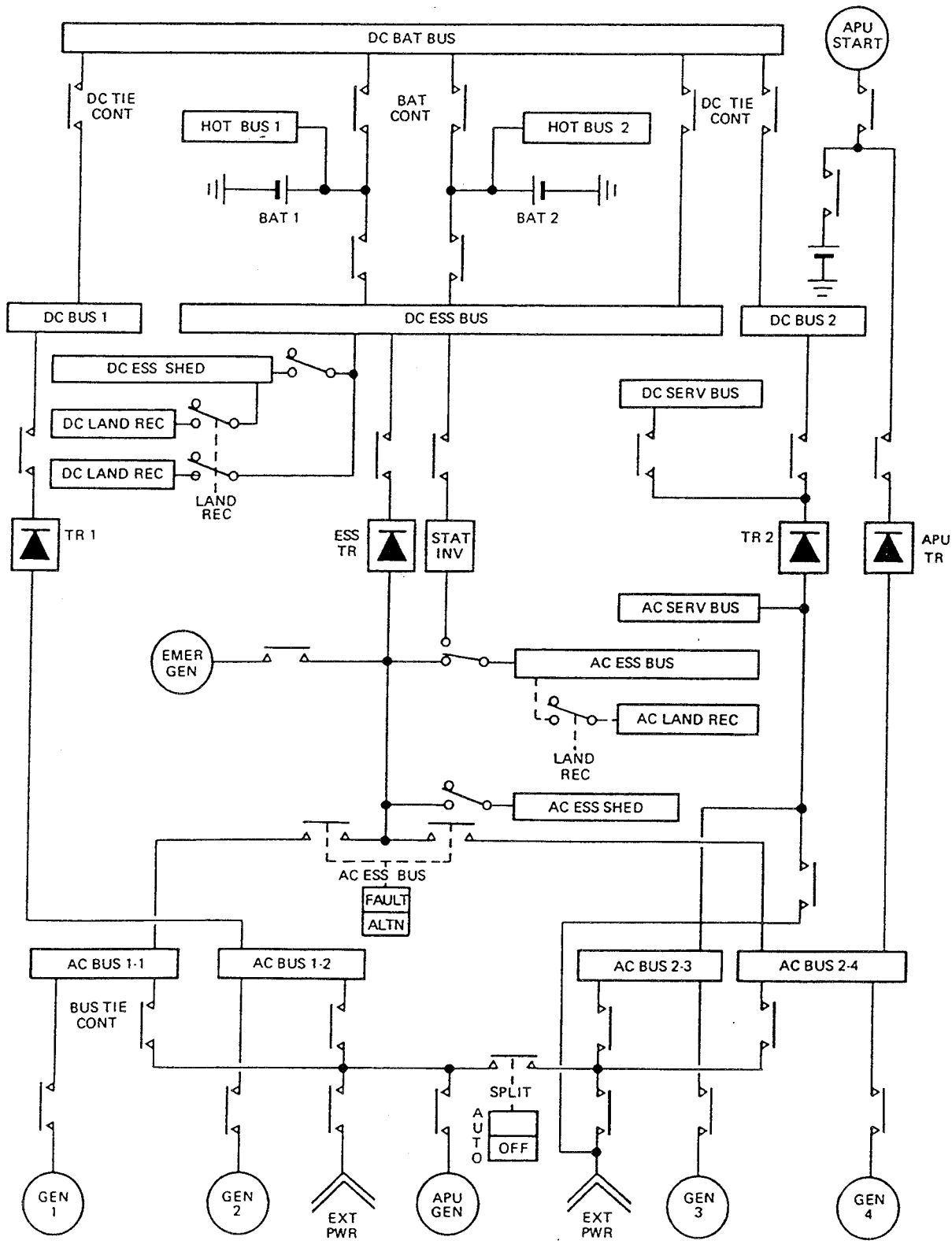
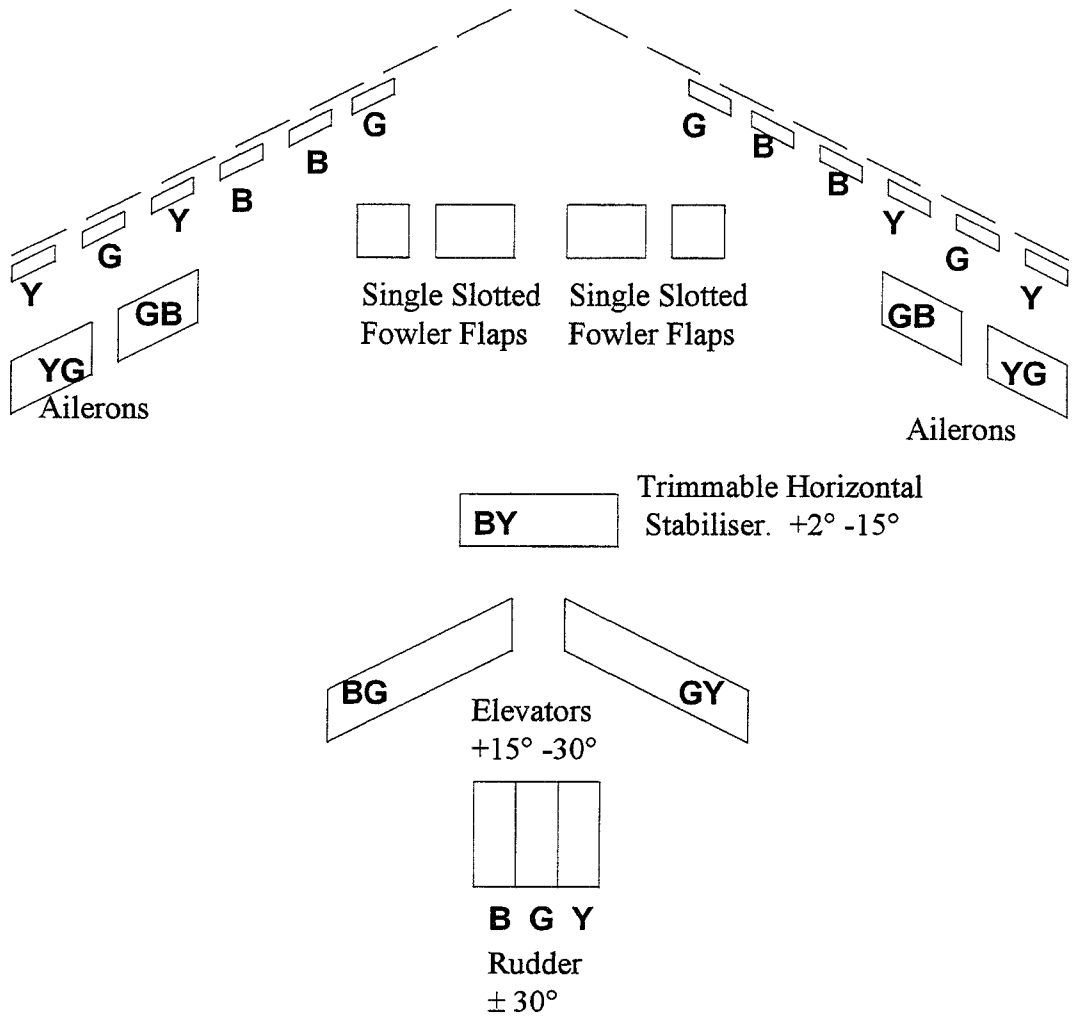


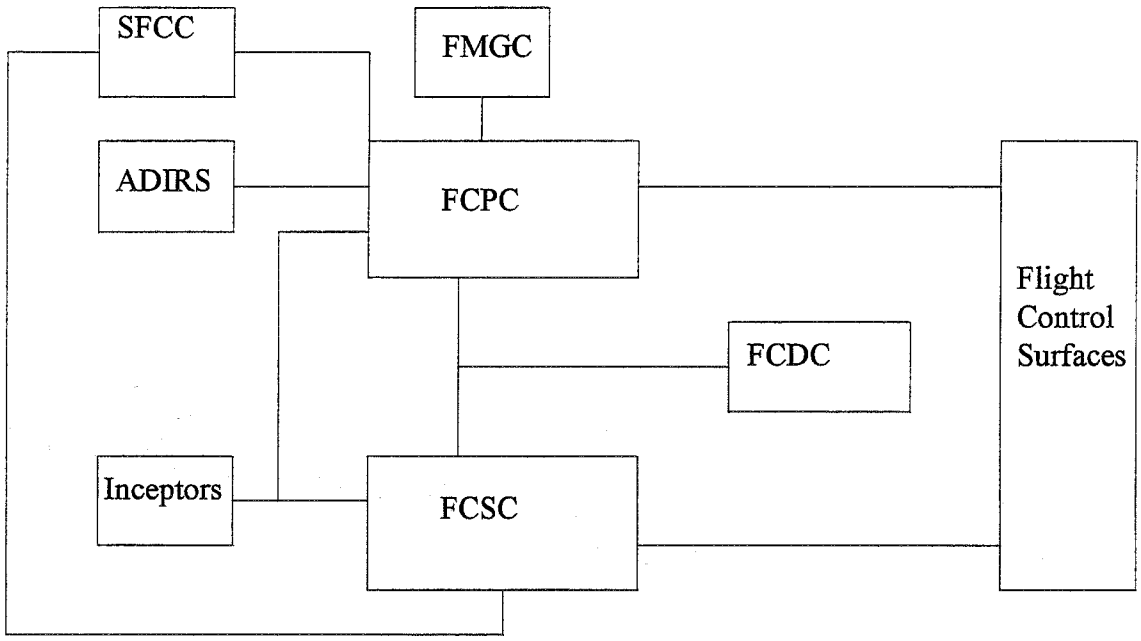
Figure D2 : Airbus A340 Electrical System



Key :

B	:	Blue Hydraulic System
G	:	Green Hydraulic System
Y	:	Yellow Hydraulic System

Figure D3 : Airbus A330 / A340 Control Surface and Hydraulic System Architecture



Key :

ADIRS	:	Air Data & Internal Reference System
FCPC	:	Flight Control Primary Computers (PRIM)
FCSC	:	Flight Control Secondary Computers (SEC)
FCDC	:	Flight Control Data Concentrators
FMGEC	:	Flight Management Guidance & Envelope Computers
SFCC	:	Spoiler & Flap Control Computers

Figure D4 : Airbus A330 / A340 Flight Computer System Architecture

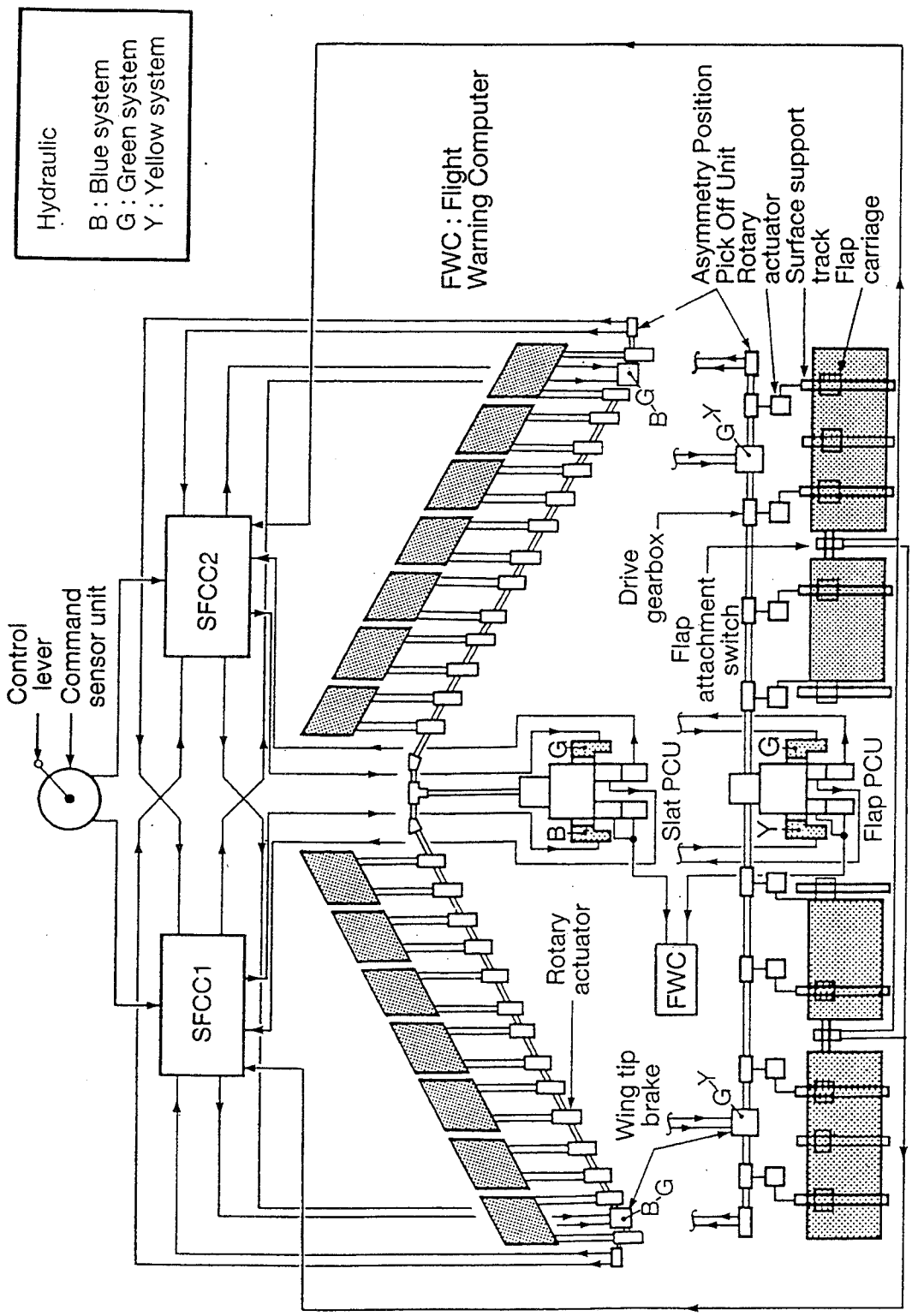


Figure D5 : Airbus A330 / A340 Flap and Slat System Schematic

Appendix E. Boeing 777

The 777 will fill the gap between the 767 and 747 models, and will be capable of being used on ETOPS routes up to 180 minutes. The 777 will be certified with three different engine types within its first year. The 777 incorporates a mix of proven equipment, some new technology, and some new features. The design philosophy adopted was to use new technology and design only where it could be shown to be cost effective, and where it would result in improved reliability and maintainability. In Boeing, the key consideration on incorporating any new technology is adding value for the customers. This is especially true of the 777, where one major initiative is the service-readiness and ETOPS capability at initial certification.

Some of the new features to be presented are ARINC 629 databuses, the Aircraft Information Management System (AIMS) and the Primary Flight Computers (PFCs). Other features included are the Air Data Internal Reference System (ADIRS), the Cabin Management System (CMS) and the Electrical Load Management System (ELMS). The new technologies have been selected from several technologies which were developed and evaluated as part of the 7J7 programme in the 1980s.

E.1 Philosophy

The philosophy of using advanced technologies such as ARINC 629 on the 777 is for one reason, to meet customer requirement by achieving higher levels of passenger comfort, unsurpassed operating economies and simplified maintenance procedures. This philosophy was developed in the 1980s from the need to rely on proven control strategies. Operation and response should be familiar to the pilots, and they should also retain full control at all times. The control functions should help the pilots in recovering from excursions in operational boundaries and traditional tactile and visual cues should be provided to help the flight crew monitor the operation of the autopilot and throttles. Finally, simple, reliable and alternate control paths should be provided.

Boeing's philosophy states that it is important that a crew may override any protection function since not every eventuality can be predicted. for example, the 777 flight control system protects the pilot at envelope boundaries such as stall, overspeed and bank angle, and it also provides variable feel in pitch.

The main reason for the selection of fly-by-wire flight control technologies on the 777 are:

- The aircraft is easier to build, due to reduction in the number of cables, pulleys, brackets, linkages and actuators.
- Weight is reduced because fly-by-wire computers provide stabilising functions, which permit lighter wings and tail.
- Reliability and maintainability are improved.
- Aircraft handling characteristics are improved through automatic compensation functions for gear, flap and thrust changes.
- Additional protection is available against inadvertent manoeuvers.

After extensive analysis, Boeing decided to rely as much as possible on control strategies developed and proven over many years. Hence the following design philosophy was chosen for the 777 control system design:

- The pilot shall retain ultimate control authority over the aircraft at all times.
- Operation and response of the aircraft shall be familiar to pilots, based on their past experience and training.
- Control functions shall assist the pilot in avoiding or recovering from exceedances of operational boundaries.
- Traditional tactile and visual cues shall be provided to assist the flight crew in monitoring the operation of the autopilot and autothrottle systems.
- Simple, reliable, alternate control paths shall be provided.

This allowed Boeing to make the following significant design decisions :

- Conventional flight controls
- Soft flight envelope protection
- Backdriven controls
- Dissimilar alternate control

This is the first civil Boeing FBW aircraft, having been developed from the YC-14. The FBW system is based on three principles :

- The fly-by-wire system will operate and "feel" much the same as conventional flight control systems, allowing the pilot to fly the aeroplane intuitively and in concert with past experience and training.
- The pilot retains ultimate control authority of the 777 at all times (i.e. a soft protection system), with built in envelope protection features that provide information but do not limit pilot input. This is because pilots have recovered from supposedly "unrecoverable" situations i.e. Chinese 747.
- A high degree of redundancy is incorporated into the 777 fly-by-wire system to ensure that it continues to function properly with individual part failures.

The display philosophy might fairly be called need to show. For example, a simple combined flap display on the EICAS is removed 10s after the flaps have been retracted; an expanded display is shown only in abnormal situations.

E.2 Power Supply Systems

E.2.1 Electrical Systems

Generation

Power generation comes from 120 kVA integrated drive generators (IDG) on each engine and the Auxiliary Power Unit (APU). These generators each have an identical generator control unit (GCU) which control the position of the respective generator circuit breakers (GCB) and bus tie breakers (BTB). The operation of these is normally automatic, though it can be done manually from the cockpit. There is also a

30 kVA generator on each engine. Power transients have been largely solved with the 747-400 experience. The electrical schematic can be found on Figure E1.

Electrical Buses

A ground handling bus is included, which is automatically powered either from the APU or external power, and is used for cargo and maintenance applications on the ground only. A ground service bus is used to power cabin lighting and some serves, and can be powered from the APU or external power without energising the main electrical bus. In flight, this bus is powered from the right main AC bus.

Using the APU alone, the aircraft is electrically self-sufficient for all ground handling operations, plus approximately 40% of the galley requirements. Hence the primary external power receptacle can be used in conjunction with the APU to power all the galley needs. A second external power receptacle has been installed on the same bus as the APU so that the ground needs can be supplied with this instead of the APU. Fuelling can be accomplished on battery power alone.

There is also a backup electrical power system that is independent of the main system, and can provide one additional channel of power for the essential equipment and flight controls. The operation of this system is fully automatic. It consists of one constant speed generator on each engine, ether of which can drive a converter unit to provide the required frequency AC power. The space these generators occupy was originally intended for an additional hydraulic pump, and their small size means that they do not have a constant speed unit attached. They are rated to provide 25 kVA for 210 minutes. The converter powers either or both of the transfer buses, which then power the essential systems. These transfer buses (L and R) are usually powered by the appropriate main AC bus. The primary purpose of this backup system is to allow dispatch with one main IDG inoperative while still maintaining three independent electrical sources. There is also a hydraulically-driven backup generator which supplies 25 kVA for critical DC services. The backup system provides for the following services, including the flight control buses, which also have their own independent sources.

1. Full flight instruments
2. Communications and passenger address system
3. Complete FMS and flight director system
4. Essential avionics
5. Engine start and essential
6. Anti-ice
7. Anti-skid
8. Limited lighting
9. Limited fuel boost and crossfeed
10. Oxygen and limited environmental system

There are two battery and charging systems. One is for the APU, and the second is for standby loads. They are charged from the ground service bus, and hence can be charged from external power.

The architecture is designed so that no single power source loss of failure of a single converter will cause loss of power to a bus, except the APU battery bus, and the APU can be cranked by pneumatics in this eventuality). for a transformer rectifier unit (TRU) failure, or the loss of its source, the two DC buses can be tied, and hence the TRUs are sized to support both buses. During autoland, the power system is configured so the main battery is used as a source for the centre autoland channel, the other two channels being supplied from the left and right DC buses. There is also a second battery bus so that only the essential services required for start are powered, as opposed to all the flight instruments etc. The battery can support this bus for 60 minutes, but only 10 minutes if all the main DC services are powered. External power can also be established without turning on the main battery switch.

A three channel 28 Volt DC independent flight control power system provides an uninterruptable supply to the fight control system. Each channel has a dedicated battery plus its own power supply assembly. In flight, power sources to the three channels are isolated so that power of abnormal quality is not supplied to all the channels. The normal source of power in flight is an unregulated permanent magnet AC generator (PMG) on each engine. Dual converters are then used to provide 28 volt DC power. On the ground, or with the loss of the PMGs in flight, the flight controls DC bus (FCDC) is automatically powered from one of the main 28 Volt DC buses. With the loss of both engines, the ram-air-turbine would automatically deploy to give limited DC power. The FCDC power requires no flight crew monitoring or operation.

The Electronic Load Management System (ELMS) is used to automate the required power switching, and provides protections to the generators from overload. The load shedding occurs in a priority order until the load is within the required limits. The system can also deploy the RAT if both of the AC transfer buses are lost.

Minimum Equipment List

The aircraft can be dispatched with one engine driven IDG inoperative by running the APU to power the appropriate bus. In the event of a second IDG failure, the main buses are tied, and all non-essential services are automatically shed until the remaining generators are no longer overloaded. One IDG is sufficient to power all essential services. These are the three electrically driven hydraulic pumps, fuel boost and jettison pumps, environmental control system and lighting, ice and rain protection, communications and navigation, DC equipment and the instruments and other avionics.

The aircraft has been designed for ETOPS from the outset; for example the main AC system is served by the main engine and APU generators and also by the standby engine-driven variable-speed/frequency generators with converters. The APU can be started, unusually, with either bleed air or electrically, even after a long cold soak. The pilot has full flight and main engine instruments, even on battery power. The primary flight control system (PFCS) is powered by two dedicated 28V generators on each engine with TRUs to provide 28 Volt DC, plus it can revert to main DC power.

The 777 electrical system features multiple power sources, which are controlled by a new system. The Electrical Load Management System (ELMS) is responsible for electrical power distribution and replaces complex relay logic and circuit cards found on previous aircraft.

Power sources include a combination of engine driven generators, an auxiliary power unit generator, and backup engine-driven generators. The aircraft main batteries can also power the aircraft emergency systems for thirty minutes in the event of complete power failure. The flight control system also has its own source of power. There is also a Ram Air Turbine (RAT) generator, which is automatically deployed in the event of engine-driven generator failure. Transient protection is assured by three small, dedicated batteries.

The ELMS consists of seven panels. The three Power Panels supply loads of more than 20 amps, and the three Power Management Panels supply loads of less than 20 amps. These 3 PMPs have processors which monitor the loads and control most of the switching components in the ELMS.

Electrical Load Management System

The conception, design, development and cont. of a subsystem of this type requires a detailed understanding of the applicable technology combined with sound aircraft systems knowledge.

The system comprises a number of power panels coupled with a number of power management panels. The primary power panels contain the major circuit breakers and electrical load control units (ELCU) which are used to control the supply of power to the major utilities such as galleys, electrical hydraulic pumps etc. These high power loads are, in the main, non-essential, and can be shed in the event of a loss in the primary power source. The ELCU are under the control of the ELMS. The secondary loads are controlled directly by the ELMS.

The system has sufficient redundancy and reliability to suffer a failure, and then continue for 10 days without additional maintenance. The redundancy was therefore included for dispatch reasons. However, a large number of the small components and LRUs are replaceable in minutes at a line level. The high level of Built In Test and maintenance functions allow rapid diagnosis, which enables the technician to assess the problem before the aircraft is on the ground. Due to the high levels of integration, the system is lighter, occupies less volume, and is also cheaper to manufacture since large, pre-assembled panels may be installed in the aircraft instead of having to assemble the system completely in the aircraft.

E.2.2 Hydraulic System

The hydraulic system is based on that of the Boeing 767, and hence much of the information has been derived from that system. All the principles used on the 767 have therefore been transferred onto the 777. The control surface and hydraulic system distribution can be seen on Figure E2.

The system comprises three independent systems, each working at 3000 psi. Each system is driven from two or more pumps, which are driven from independent power sources. The focus is on safety through multiple input power sources with redundant, parallel hydraulic pumps so that all of the numerous probable single or double failures may occur without impairing continued safe flight and landing. Each of the systems is powered by engine-driven pumps, bleed air and electrical generators to minimise the effects of power-source failures on the hydraulic system.

Left System (L). The Engine Driven Pump (EDP) on the left engine is the primary source of power for this system. There is also an AC electrically driven pump (ACMP) from the right main AC bus. This is automatically selected when needed.

Centre System (C). There are two ACMPs on the left and right main AC buses which are normally used to power the central system. There is also an Air Driven Pump (ADP) from pneumatic system which is automatically selected when needed, and a Ram Air Turbine (RAT) driven pump for emergency power..

Right System (R). The Engine Driven Pump (EDP) on the right engine is the primary source of power for this system. There is also an AC electrically driven pump (ACMP) from the left main AC bus. This is automatically selected when needed

Systems L and R are basically for powering the flight controls, with system C is for primary and secondary flight controls plus the landing gear and steering utilities. The landing gear, brakes and reverse thrust actuation systems have not been considered here.

All of the surfaces, except the spoilers are driven by more than one actuator. Three actuators are installed on the rudder to meet the extreme requirements of engine failure and flutter, but a single actuator would meet normal demands, together with a spring tab. All of the control surfaces follow an integrated logic which allows gradual control degradation in the event of several failures. No two simultaneous failures should affect control. The allocation of the hydraulic systems to the flight control surfaces is based on the Boeing 767.

Hydraulic fuses are fitted in the wing boxes and in the left system at the tail; these are electronically operated valves that close if the fluid flow becomes too high so that a system fracture does not drain the entire circuit. The RAT is unlocked either by main or APU battery power, drives a generator and hydraulic pump.

E.3 Airplane Information Management System

This is the data cruncher for many of the major avionics systems. It provides the major crew interface for both flight and crew maintenance crews. The flight crew interface is through the Control Display Unit; six display units, two Flight Instrument Control Panels etc. The maintenance crew interface is through a Maintenance Access Terminal on the flight deck, with 5 additional portable terminal access points located around the aircraft.

AIMS is a collection of modules within two cabinets, each with input/output modules, core processors power supplies etc. There is also the capacity for further future expansion should the need arise.

The AIMS is designed to provide enhanced functionality and performance, coupled with a reduced life-cycle cost. This cost reduction comes through reduced spares costs, an improved removal rate through improved maintenance diagnostics, and finally flexibility through added functions, and upgrades, coupled with an enhanced airline customisation capability.

The flight management system is implemented on the AIMS. This provides navigation, flight planning, performance management, guidance and control and thrust management. Maintenance information is also stored, for later generation into a report format. Communication management includes air to ground communication, both audio and through data link.

The AIMS information management function includes a data conversion gateway that transfers information between the various aircraft busses, and also the systems that are not on the busses. Also, the flight data recorder and quick access recorder are provided for by this system.

The AIMS has taken a major step in avionics integration by implementing a broad set of avionics functions within two AIMS cabinets. Within the AIMS philosophy, high integrity shared resource coupled with robust partitioning and fault tolerance design techniques are providing the design techniques are providing the capability to use selective redundancy to enhance functional availability within the AIMS.

The AIMS maintenance philosophy is pays dividends in reduced maintenance costs for the airlines. The high reliability AIMS hardware is coupled with hardware monitoring that provides instantaneous fault detection/ confinement, hardware/software fault separation and transient fault suppression. Redundancy is added as required to provide a 10 day maintenance goal. This deferred maintenance should significantly reduce the airline costs of ownership.

The robust partitioning and modular design allows efficient system customisation and upgrades while causing only minimum certification impact on the other aircraft systems. This allows for user customisation, and upgrades during the life of the aircraft. For example, this allows airlines to modify checklists for normal or abnormal operation via a ground based workstation.

E.4 Cabin Management System

Within the passenger compartment, the Cabin Management System is an example of large-scale integration and growth of functionality. This system includes:

- Passenger Address- announcements, boarding music, safety demonstration
- Cabin Interphone - attendant to attendant or flight crew, ground crew
- Passenger service - attendant call, reading light, smoke alert
- Cabin Lighting - cabin, lavatories, entry-ways, rest areas, work areas
- Passenger entertainment - phone, audio, video (overhead and individual)
- Cabin Data Network - data link to ground, faxes, interactive video
- Monitor and Control - cabin temperature, potable water, door status, camera

The CMS has over 2050 LRUs, some selected by Boeing, some by the customer. It allows for more personalised cabin functions with a wide selection of cabin entertainment. Also, duty-free goods can be ordered in-flight

E.5 Flight Control System

This section will describe the different components of the flight control system, both the hardware and functional descriptions. The flight control system architecture can be seen on Figure E3.

E.5.1 Air Data and Internal Reference System

The Air Data Computer (ADC) and Internal Reference System (IRS) components remain a significant component of the flight system cost. With the evolution of flight control systems, the air and internal reference data has become a flight critical component. Hence a greater reliability is required, compared to what was achieved before. Also, in the ever increasing drive for economy, reductions in price, maintenance costs, weight, volume and power are required to provide the required efficiency improvements. In studies carried out by Boeing, the following factors were identified as offering the greatest potential to meet the aforementioned needs.

1. New technology sensors.
2. Remote air modules, and integration of air and inertial data.
3. Skewed axis inertial sensors. These replace traditional sensors arranged in orthogonal triads. The primary system contains 6 gyros and 6 accelerometers and provides a functional integrity in excess of that obtained with 4 conventional Internal Reference Systems containing twice as many sensors arranged orthogonally.
4. Integrated standby reference system.
5. Fault-tolerant electronics. Redundant sub-assemblies are used to provide comparison of sensor outputs and to detect and isolate failures in real time and to reconfigure the system to use only non-failed resources. This provides 100% coverage for random failures as long as the minimum number of redundant resources remain valid.

6. High reliability/ low cost packaging. New technology gyros are expected to be 5 to 10 times as reliable as current sensors. New packaging techniques offer both higher reliability and lower cost by eliminating design features facilitating rapid removal and disassembly for maintenance in favour of features facilitating high reliability and low cost.
7. ARINC 629 interfaces.
8. Deferred maintenance.
9. Certification with exact simulation.
10. Structure design and software in ADA.

The ADIRS is therefore a logical evolution from these. It consists of traditional, triple-redundant pitot and static ports, whose signals are converted to electrical signals using Air Data Modules mounted near the air data probes. This eliminates the need to run pneumatic tubes from the probes to the computers and flight instruments, and also gives a reduced weight penalty and maintenance requirement. Digital signals are sent from these sensors on the Flight Control Buses to the ADIRU (Air Data Internal Reference Unit) and SAARU (Secondary Attitude and Air Data Unit). The ADIRU and SAARU are fault-tolerant computers, with a complement of rate gyros and linear accelerometers. In the ADIRU, six of each sensor type are mounted in a skewed-axis arrangement, such that the internal and navigational signals are still provided, even after the loss of two of each. In effect, a hot spare is always available. The secondary system is designed to provide all flight critical functions, with a probability of failure of less than 10^{-9} per flight hour.

In developing the ADIRS, it was recognised that the primary/ standby architecture was attractive, firstly because the two systems are totally dissimilar, and secondary because they are supplied with independent power and sensor inputs. These two factors minimise the potential for common mode faults. This architecture has remained common in the transition from the Boeing 767 to 777. To protect the aircraft against destructive, but hopefully very rare events e.g. bird strike, sabotage etc., a dissimilar source of data is available from the SAARU, which has four of each sensor type. This unit also supplies the standby instruments on the flight deck.

The following benefits have been recognised of an ADIRS design.

1. Reduced manufacturing costs through integration of traditionally many separate units into a single primary system and a single standby system, and also a reduction of the number of parts.
2. Reduced power consumption, weight and volume, coupled with reduced complexity of inter-system avionics architecture.
3. Increased reliability with increased MTBR (mean time between removals) through redundancy and monitoring, coupled with dispatch with allowable failures, which will decrease the required maintenance requirements, plus assist with operating away from base. Hence requirements for rapid maintenance are no longer required, which gives additional significant cost savings.

E.5.2 Flight Control Surfaces

There are 31 individual control actuators which power the following control surfaces as shown.

7 Spoilers per wing (5 outboard + 2 inboard).
Single span elevator
Stabiliser
one outboard Aileron per side
two flaperons per side.
Single rudder

There is a manual backup of mechanical elevators to the elevators and one set of spoilers for get-you-home manual pitch and yaw control.

E.5.3 Flight Control Computers

There are two types of electronic computer in the flight control system: the Actuator Control Electronics (ACE), primarily an analogue device, and the Primary Flight Computer (PFC), which is digital. Each will be considered in turn.

Operation - General

The ACEs decode signals, from multiple transducers on the pilot's controls, and those on the primary surface actuators. Both positions, converted to a digital value, are sent over triplex bi-directional ARINC 629 databuses to the PFCs, to process further surface commands. These are returned over the same buses for the ACEs to convert into further analogue commands for each actuator. In normal operation, the inceptor commands are decoded by quadruplex sensors, which are then coded by the ACEs for transmission on to the flight control bus. The ACEs also transmit the current control surface positions to the PFCs. The PFCs then perform the calculations to determine the new surface positions. The PFCs also perform the envelope limiting functions. The required actuator movements are then re-transmitted onto the flight control data bus so the ACEs can decode the signals and then command the actuator movements.

Primary Flight Computers

GEC were called upon to develop a prototype primary flight control computer for a future transport aircraft in 1986. The design goals were to develop a fault tolerant architecture which exhibited improvised life-cycle costs over a conventional system and to achieve a higher mean time between maintenance. This was achieved by a novel reconfigurable architecture, coupled with Application Specific Integrated Circuits (ASICs), which is a new component packaging technique to increase hardware reliability.

The Primary Flight Computers perform the main flight control system calculations. There are three in total, i.e. three channels, and they receive data from the other aircraft systems by two different methods. Firstly, the ADIRU, SAARU and the

autopilot flight-director computers transmit directly onto the flight controls data buses and hence to the PFCs. Other systems, such as flap-slat electronics units (FSEU), proximity switch electronics unit and engine-data interface unit, transmit data on the four systems databuses. The PFCs receive data from these databuses through the dual Aiplane Information Management System (AIMS). This gateway between the two main sets of ARINC 629 buses maintains safe separation between the critical flight controls and essential systems, while allowing data to be interchanged.

The PFCs use inceptor and control surface position information to compute the required control surface deflections for the primary flying controls. Each PFC receives signals from three sensors, one directly, and two received via the other PFCs and the databus. At the channel output plane, each PFC selects the median value of the actuator commands produced by itself and the other PFCs, and transmits this onto the Flight Control data bus for the ACEs. It only transmits onto one databus in order to prevent common mode faults. The ACEs decode the PFC commands and turn them into actuator commands. The command trim function is considered to have a lower availability requirement, and consequently the associated control inputs are implemented as dual redundant discrete sensors partitioned between two PFCs. Apart from the flight deck inputs and trim drive discretes, all other data exchanges between the PFCs and other EFCS systems are accomplished via the ARINC 629 flight control system triplex data bus.

Each PFC contains three independent lanes, i.e. different sets of microprocessors, ARINC 629 interfaces and power supplies. All lanes perform identical calculations; failure of a lane will only cause that lane to be shut down. A channel can be operated normally on two lanes; another lane failure will cause that channel to be shut down. One PFC lane is called the command lane at the voting plane, and is monitored by the other two (or one in the event of failure). The command lane in each PFC is chosen to be dissimilar. The PFCs are labelled left, centre and right, as are the databuses. Each of the PFCs has three lanes, using different microprocessors. The PFCs also support maintenance functions which interface with the AIMS. The PFCs include stall and bank angle protection features within its function.

Each PFC lane comprises three printed circuit cards that contain many ASIC components which have been specifically designed for this use. The three lanes all employ 32 bit processors, with one of each type in each PFC. These processors are the AMD 29050, the Motorola 68040 and the Intel 486. In each case, specific ASIC components have been included to cater for the high data volume throughput. The input/output module consists of three ARINC 629 terminals, two configured as receivers and one as a receiver/ transmitter. The software is produced in ADA, and the source code is converted for use in the three dissimilar processors using independent compilers.

The software is divided up into approximately the following proportions :

Executive	3%
Control Laws	47%
Inter Lane Redundancy Management	12%
Intra Lane Redundancy Management	20%
External PFC Redundancy Management	18%

PFC redundancy is in the calculating element. The 777 can be operated indefinitely with one lane of nine failed. The master equipment list will allow dispatch with two lanes out of nine failed (not within the same channel) for some days, and with one PFC inoperative for a short period.

Actuator Control Electronics

There are four ACEs. The redundancy of the ACEs is in functional distribution; ACE designations match the left (two ACE units designated L1 and L2), centre and right hydraulic systems on the aircraft. Total failure of one ACE has the same effect as total hydraulic system failure.

It is assumed that each of the Left (1 and 2), Centre and Right ACE units receives signals from one of three channels on the inceptor quadruplex sensor, and also from the appropriate (i.e. L, C or R) PFC in normal operation, though each ACE can receive commands from any PFC via all three of the Flight Control 629 databuses. The fourth channel is assumed to be a direct analogue link between the inceptor and actuator, and is therefore separate from the other electronics in the ACE.

The control surfaces which are powered by the individual ACEs are shown in Table E1.

Flight Control Modes

There are three primary modes in the flight control system. The first is the normal mode, where all of the system are operating nominally, or with minor failures, such as one PFC failed. The secondary mode is selected automatically by the FCS when there are certain failures, such as air data failures, meaning that not all of the protections are in place. This mode cannot be selected by the flight crew. However, the C*U control law is the same as for the primary mode. The third mode is the direct mode, where the pilot's controls are effectively connected directly to the control surfaces. This can be selected manually by the crew with a switch on the overhead panel.

Control Surface	ACE	Hydraulic
Left Elevator 1 (outboard)	L1	L
Left Elevator 2 (inboard)	C	C
Right Elevator 2 (inboard)	R	R
Right Elevator 1 (outboard)	L2	L
Trimmable Horizontal Stab 1	L1, C	C
Trimmable Horizontal Stab 2	L2, R	R
Left Aileron 1	L2	L
Left Aileron 2	C	C
Left Flaperon 1	L1	L
Left Flaperon 2	R	R
Right Flaperon 2	L2	R
Right Flaperon 1	C	C
Right Aileron 2	R	C
Right Aileron 1	L1	L
Rudder 1	L1	L
Rudder 2	C	C
Rudder 3	R	R
Spoiler 1 & 14 (outboard)	C	C
Spoiler 2 & 13	L1	L
Spoiler 3 & 12	R	R
Spoiler 4 & 11	L1	L
Spoiler 5 & 10	L2	C
Spoiler 6 & 9	R	R
Spoiler 7 & 8 (inboard)	C	C

Table E1 : Boeing 777 Flight Control Computers and Control Surface Distribution

Other Systems

A triple channel autopilot sends signals directly to the primary flight computers. The flaps can be driven electrically if the hydraulics fail, as on the Boeing 747-400. A third control level bypasses the flap control computer with direct electrical signalling. The flaps and slats are controlled by a separate system, the schematic of which can be found on Figure E4.

Backup systems

In the event of the failure of the flight control data buses, the PFCs or the ACEs, the ACEs contain a separate function which can be used to give direct control. A separate unit within each ACE samples a fourth inceptor command sensor and computes the required actuator movement to give direct surface command. This

computation is independent of the rest of the functions within the ACE unit so that internal ACE failures do not preclude its operation.

In direct mode, the controls are still driven by analogue electric signals, rather than by rods, and cables are not generally fitted. There is a mechanical connection from the control wheel to operate spoilers No. 4 and 11, and from the standby pitch trim handles to the stabiliser. This mechanical system is only intended to be used while electrical power is being restored.

E.5.4 Other Systems

Many of the conventional systems on the 777, such as the autopilot, have their heritage on the Boeing 747-400 or 767. These existing systems proved to be a valuable experience to utilise and learn from.

E.5.5 Databuses

Three sets of ARINC 629 buses are provided on the 777. Each bus can handle up to 2 Megabit/second data rate.

- 3 for Flight Controls
- 4 for Aircraft Systems
- 4 for AIMS Intercabinet Data Communications

The three Flight Control Buses have a limited number of subscribers to protect the integrity requirements; only units directly associated with flight control have access. The four aircraft system buses provide general purpose communication between systems using two as high integrity buses, and two as general data buses. These buses replace many analogue, discrete and ARINC 429 buses used on previous aircraft, although in the interests of minimum change to some sensors, some of these signal paths are retained. ARINC 429 buses on the 777 are retained for communication with buyer-furnished equipment or with systems used on other Boeing aircraft. Much attention was paid to protection of bus integrity and definition of protocol due to the consolidation of data to a relatively small number of buses.

As the 777 system evolved, it became clear that a mixture of critical and non-critical LRUs on the system buses would impose a significant electromagnetic interference test burden and a severe reliability requirement on the non-critical (both essential and non-essential) LRUs. To guarantee that non-critical LRUs would not impose a liability on the critical LRUs, all LRUs designed to be connected to a bus on which critical information was going to be transmitted would have to withstand more severe levels. This would have caused high cost with the initial three system bus design since all of the three buses had the required level of robustness and failure tolerance for the critical systems. Hence a fourth bus was added to the system bus to support critical functions. The left and right systems buses therefore became essential (i.e. non-critical), while the two central systems buses and the flight controls bus are considered critical.

E.6 Handling and Control Laws

The flight control laws have been designed for each different stage of the flight phase. Hence there is a certain amount of control law and gain scheduling. This is most apparent during take-off and landing, as illustrated below.

Take-off

At take-off, the pilot starts the take-off roll with direct elevator command, i.e. the control wheel is effectively coupled directly to the elevator as with a conventional aircraft. Then the C* law is blended in several seconds after take-off, and the full C*U is activated several seconds after that. The landing flight phase has a linear pitch down schedule based on radio height inserted into the control law. This is to enable the aircraft to have monotonic stick forces since an aircraft with a pure C* law does not have this since it behaves in a rate-like response, and forward stick is therefore required to de-rotate the aircraft after landing, coupled with the fact that stick pumping may be required to achieve the desired pitch attitude or flightpath.

Up and away

In flight, the trim wheels command a new referenced trim speed, with the flight control system pitching the aircraft up or down to achieve it, and then the stabiliser trimming it out. As on a conventional aircraft, trimming reduces the control column forces. However, the trimmer is considered by the flight control system to be slightly different to a conventional aircraft. The trimmer is used to set the reference speed for the C*U control law.

On the ground, the pitch trim move the stabiliser directly; the alternate trim levers always move it directly, but first signal a change to the in the referenced trim speed to the PFCs. Pitch effects caused by configuration changes are fully compensated for in normal mode.

Landing

During the landing phase, compensation is included during the flare in order to compensate for the ground effect removed by the control laws ad hence to give landing behaviour consistent with a conventional aircraft.

General

Back stick is required in turns greater than 30° bank. The aircraft has positive roll stability for bank angles greater than 35° and neutral stability for roll angles less than this value. There are negligible flight path deviations with configuration changes; indeed pilots who have flown both aircraft have commented that the 777 is superior to the A320 in this respect. Overall, the 777 feels like a conventional aircraft. All of the pilots controls are backdriven. Even if sidesticks had been implemented then they would also have been backdriven due to the importance of tactile feedback.

E.6.1 Protections

The envelope protection is achieved through increasing the stick forces appropriately as the aircraft gets closer to the edge of the flight envelope, and the removal of the ability to trim the aircraft when it gets into this condition.

The FBW system also includes a gust-suppression. The wing is designed to the gust rather than the manoeuvre load limits. The lateral gust suppression system will operate differently from existing systems: sensors on the vertical fin will apply signals on the rudder to counter lateral accelerations rather than to respond to them. Aircraft body movement will be reduced, which is important since it improves passenger comfort.

The FBW control system incorporates stall and overspeed restraint, bank angle protection and pitch stability augmentation. The natural pitch stability will be around 6%. Low or high speed, and excess bank will create excessive forces on the controls, but the pilot will be able to overpower them if he so decides though it is not possible to trim out these loads. Roll restraint comes in at 35° bank and returns to normal at 30°. Pitch forces rise to 60 lbs, and a stick shaker is fitted. The response is C*U, and will be also tailored in the flare. Boeing decided against neutral speed stability in the pitch channel as it leaves the airspeed to invisible, hence there is some speed stability. The trim will also act a little differently to a conventional aircraft as it will effectively reference airspeed which will then be used in the PFC.

E.6.2 Failures and alternate modes

There are two alternate modes, the secondary mode and the direct mode, as discussed in the flight control section. Direct mode is engaged by a switch on the overhead panel. The secondary mode cannot be engaged manually. In direct mode, there are no configuration or trim bias for configuration changes. Handling in this mode is conventional, with the aircraft feeling slightly looser in roll and yaw. Dutch Roll is slow to damp, and roll response to rudder inputs is high. Switching back to normal law was kick-free, apart from the cancelling of some residual yaw which was immediately cancelled by law damping in the PFCs.

There is also thrust asymmetry compensation (TAC) for asymmetric flight. This works by compensating for large trim changes during engine out flight cases. It does not remove completely the cues associated with an engine failure, but removes much of the pilot workload associated with an engine failure.

E.7 Bibliography

Aerospace. The Royal Aeronautical Society. Jul. 1992.

Aerospace. The Royal Aeronautical Society. Mar. 1994.

Flight International. Reed Business Publications. 20-26 Nov. 1991..

Flight International. Reed Business Publications. 31 Aug. - 6 Sep. 1994.

Flight International. Reed Business Publications. 26 April - 7 May 1995.

Hills, Andy D. Mirza, Nisar A. *Fault Tolerant Avionics*. GEC Rochester, Kent. AIAA 88-3901-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988.

Johnson, Mark. *Boeing 777 Airplane Information Management System - Philosophy and Displays*. Proceedings; Advanced Avionics on the A330/A340 and the Boeing 777 Aircraft. RAeS, London. 17 November 1993.

McWha, James. *777 Systems Overview*. Proceedings; Advanced Avionics on the A330/A340 and the Boeing 777 Aircraft. RAeS, London. 17 November 1993.

Moir, Ian. *Load Management*. Smiths Industries. Proceedings, Aircraft Generation and Distribution Systems Conference. RAeS. 14 October 1992.

Pottenger, Simone. *Boeing 777 629 Data Bus - Principles, Development and Application. Boeing Commercial Aircraft Group*. Advanced Avionics on the Airbus A330/A340 and The Boeing 777 Aircraft. RAeS London. 17 November 1993.

Sebring, David L; McIntyre, Melville D. *An Air Data Internal Reference System for Future Commercial Airplanes*. Boeing Commercial Airplanes. AIAA 88-3918-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988.

Tenning, Carl. *The Boeing 777 Electrical System*. Boeing Commercial Aiplane Group. Proceedings, Aircraft Generation and Distribution Systems Conference. RAeS. 14 October 1992.

Tucker, Brian. *Primary Flight Control Computer System - Philosophy and Implementation*. Proceedings; Advanced Avionics on the A330/A340 and the Boeing 777 Aircraft. RAeS, London. 17 November 1993.

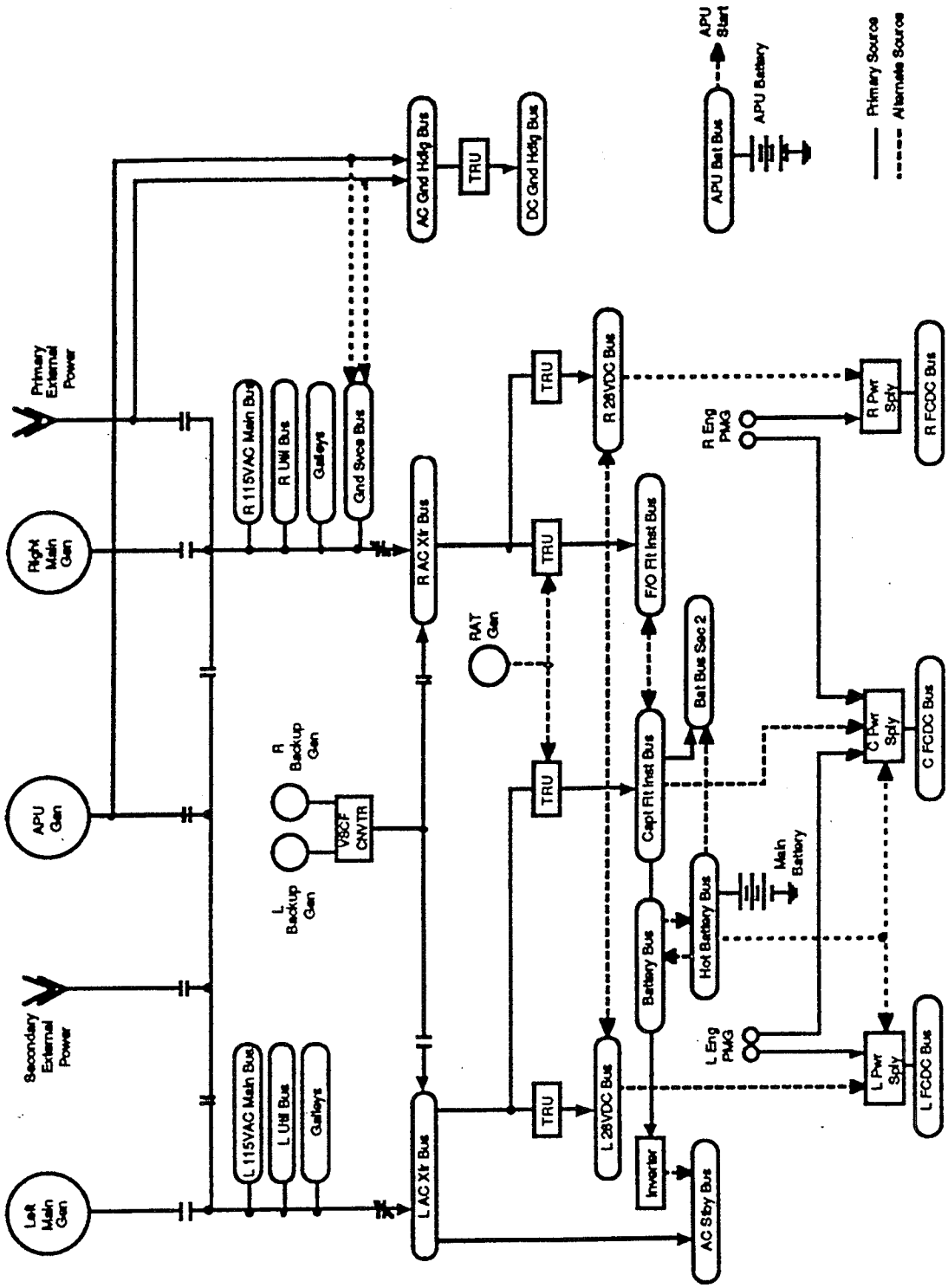
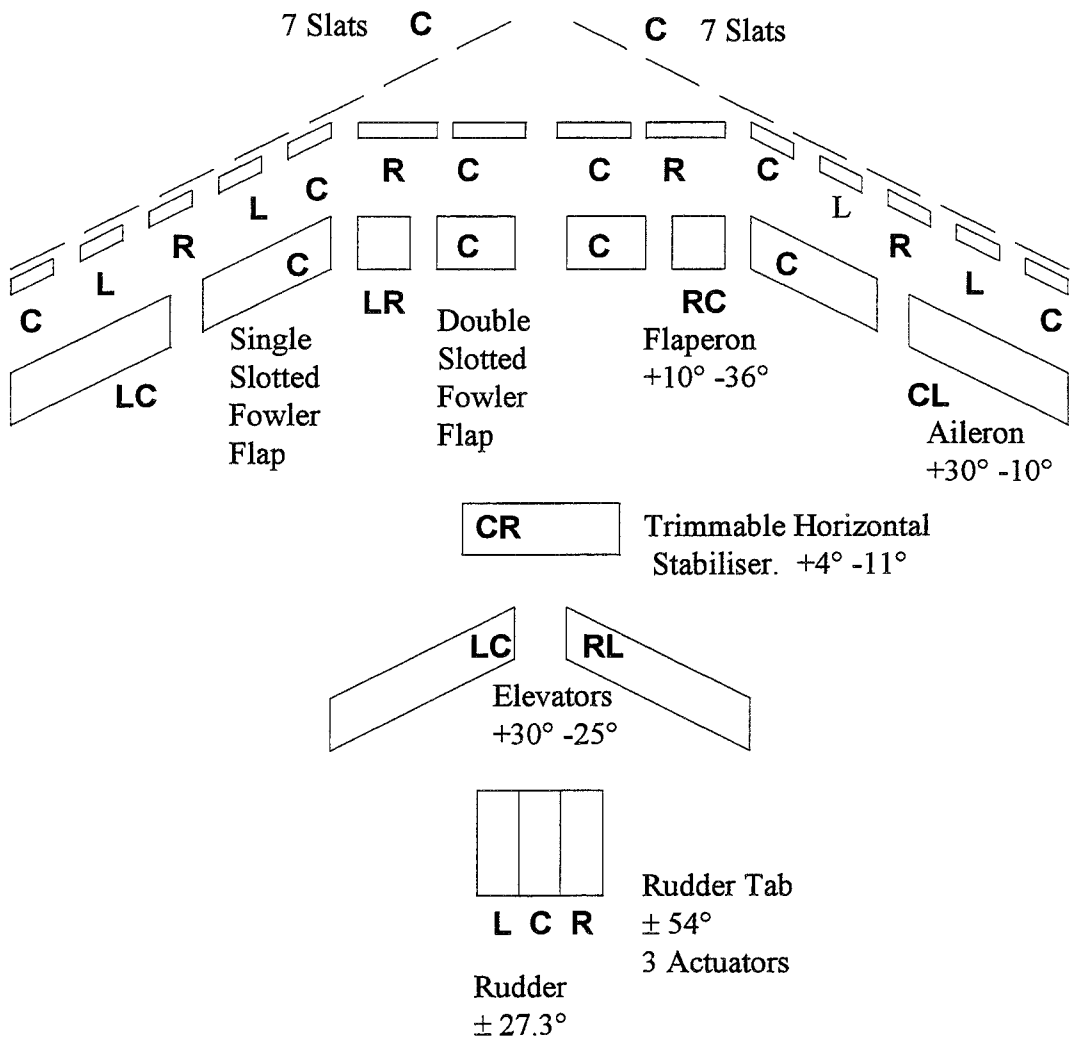


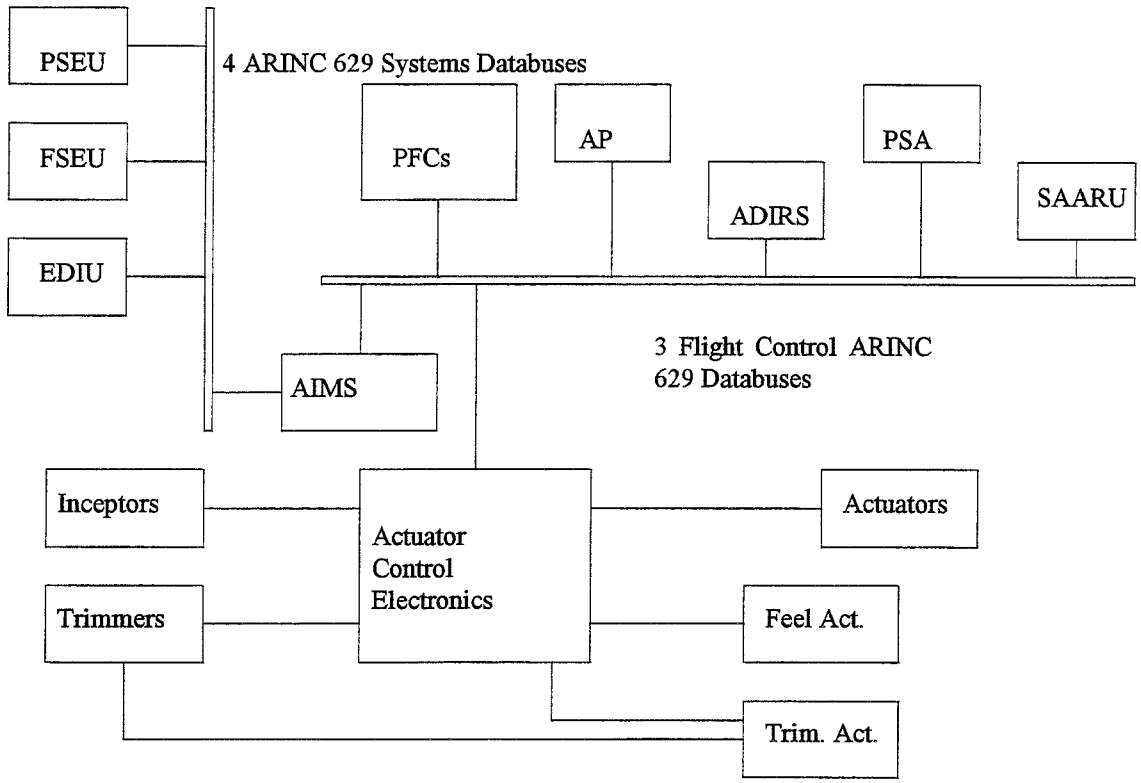
Figure E1 : Boeing 777 Electrical System



Key :

L	:	Left Hydraulic System
C	:	Centre Hydraulic System
R	:	Right Hydraulic System

Figure E2 : Boeing 777 Control Surfaces and Hydraulic System Distribution



Key :

ADIRS	:	Air Data & Internal Reference System
AIMS	:	Airplane Information Management System
AP	:	Autopilot
EDIU	:	Engine Data Interface Unit
FSEU	:	Flap / Slat Electronics Unit
PFC	:	Primary Flight Computer
PSA	:	Power Supply Assembly
PSEU	:	Proximity Switch Electronics Unit
SAARU	:	Standby Attitude & Air data Reference Unit

Figure E3 : Boeing 777 Primary Flight Computer System Architecture

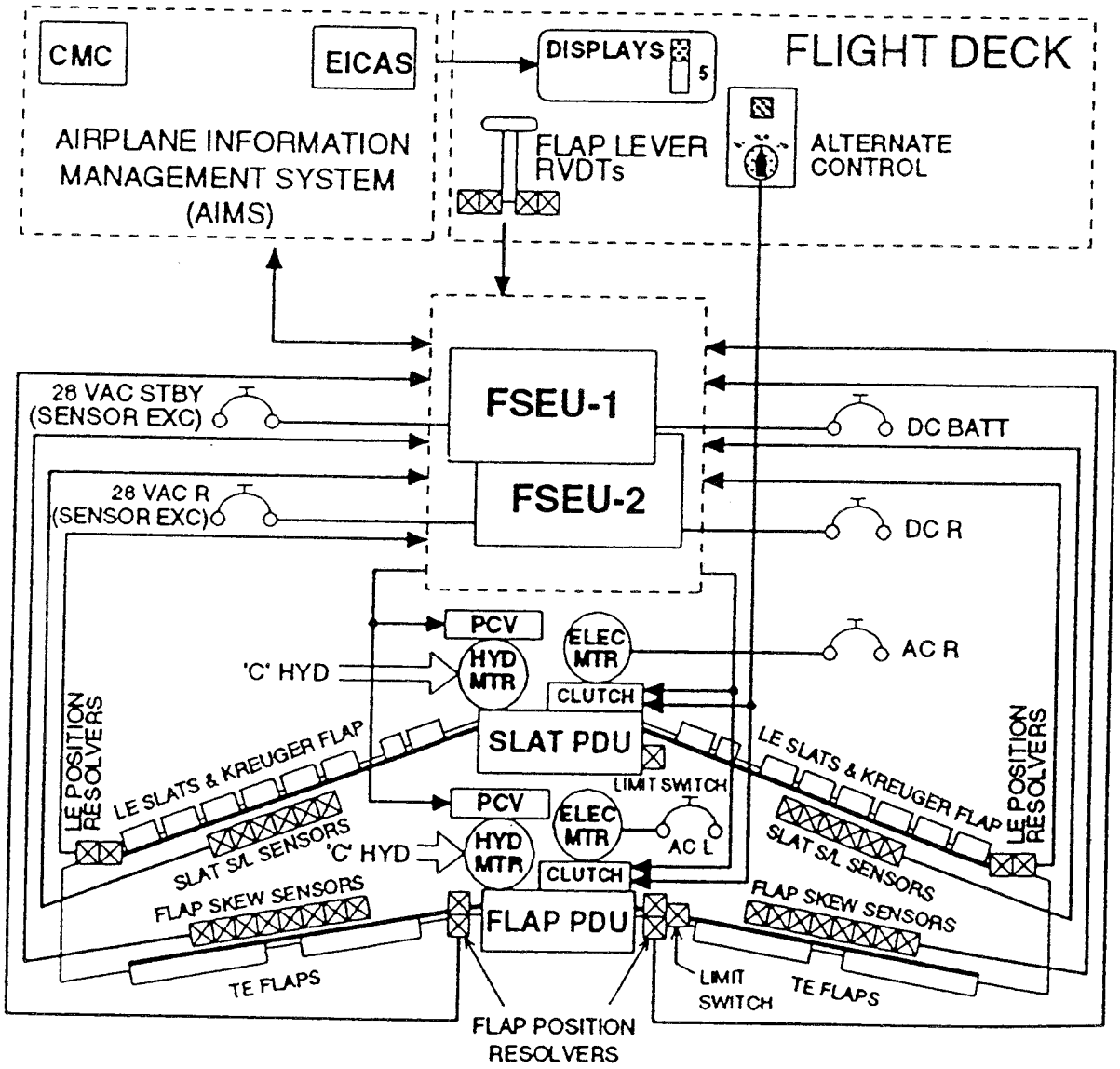


Figure E4 : Boeing 777 Flap and Slat System Schematic

Appendix F. Avro Regional Jet (RJ)

The Avro Regional Jet is a small 100 seat Regional Jet powered by 4 turbofan engines mounted on the wing. It has been included for this report since it represents a mechanically signalled version of the Generic Regional Aircraft under consideration.

F.1 Power Supply Systems

F.1.1 Electrics

Two separate channels of electrical power are produced from a generator mounted on each outboard engine supplemented by an identical APU driven generator. DC power is obtained from three Transformer Rectifier Units (TRUs). AC and DC power can also be generated from hydraulically driven pumps.

F.1.2 Hydraulics

The RJ has 2 independent hydraulic systems.

1. Yellow system. This is powered by an engine driven pump (EDP) on No. 2 Engine plus an AC driven electric pump. There is also a DC pump solely for the Emergency landing gear plus the Anti-Skid. The Yellow system powers the roll spoiler, standby fuel transfer and emergency landing gear.
2. Green system. This has a EDP on the No. 3 Engine plus a power transfer from the Yellow system, plus a standby AC/DC generator. The Green system powers the landing gear, steering and airbrake.

Both systems power the anti-skid, rudders, lift spoilers and flaps. The primary flight controls, i.e. the ailerons and elevators are mechanically driven.

F.2 Electronic Flight Information System

The Honeywell EFIS became the standard fit on the RJ in mid 1990, with mechanical analogue instruments becoming an option. There is a laser gyro internal Reference System (IRS) with a Flight Management System (FMS). There is also a Flight Guidance Computer (FGC) and a Flight Control Panel (FCP).

F.3 Flight Control System

F.3.1 Flight Control Surfaces

The duplicated pitch and roll flying controls have split circuits incorporating a disconnect device in the event of a control jam on one side. A hydraulically operated duplex yaw damper system is fitted. The roll and lift spoilers and the large under-wing flaps are hydraulically operated. The flaps are single piece tabbed Fowler flaps, hydraulically powered, mechanically driven and electrically operated. Fuselage

mounted petal-type airbrakes, which form the aircraft tail-cone, are powered by a single hydraulic jack and are infinitely variable and deploy symmetrically. The control surfaces are shown on Figure F1 together with the hydraulic systems which power them.

Four spoilers are provided on each wing, three lift spoilers and one roll spoiler, all hydraulically powered. The lift spoilers are selected manually and controlled electrically. The landing gear is hydraulically operated and has a hydraulically assisted lock-down system for emergency lowering. The duplex hydraulic brakes have anti-skid units.

An automatic flight guidance system has an integrated autopilot and flight director, which provides three axis stabilisation and two axis manoeuvre computation in pitch and roll in addition to flight director computation.

Roll Control

Roll control is provided by aerodynamically and mass balanced ailerons, each operated by a servo tab, in conjunction with roll spoilers (one per wing) powered by the yellow hydraulic system. A geared trimming tab is also fitted to each aileron. Normally the two circuits are connected, but they can be disconnected in the event of a jam in one of the circuits. The ailerons are driven by conventional cables and rods, and a spring-operated feel unit complements the natural servo tab feel at large inputs, and provides a handwheel centring force at small angles. The feel unit is in the captain's side. Each servo tab has a blow back spring which limits the authority of the tab depending on the airspeed.

If a jam occurs in one roll control circuit then application of heavy pressure to the handwheel of the other circuit will cause the rigid detent strut to 'break-out' and transform into a sliding strut. The free circuit will then operate independently, allowing control to be maintained. As this break-out device operates a solenoid disconnects the aileron connect cable. This disconnection may also be done with a handle in the cockpit, but will not break the disconnect strut. After the strut or the solenoid have disconnected, they cannot be reconnected in flight.

Each roll-spoiler is operated by a hydraulic Power Control Unit (PCU). The spoiler is harmonised with the aileron servo tab, except that it remains closed for the first few degrees of tab operation. The PCUs have dual control valves which normally permit a single valve to retain control if the other fails. Should spoiler failure fail due to failure of the yellow hydraulic system then ailerons alone will provide limited control. The PCU servo valves are spring loaded to the closed position so that if the input linkage fails, the spoilers will automatically close.

Yaw Control

The rudder is operated by two servo units- one powered by the yellow circuit and one powered by the green. Rudder feel is powered by a spring strut. Each servo unit has dual control valves operated by a common linkage, but with two separate conventional cable and rod control circuits. One circuit is linked directly to the interconnected pair of rudder pedals, and the other is connected by way of a screwjack to the rudder trim wheel.

A rudder valve caption will illuminate if any control valve should stick or either / both hydraulic systems loose pressure over a period of time. Operation of the rudder trim also feeds into the feel system so the feel is equalised over the left and right side. If the Q-feel system fails then this is captioned since this failure could lead to the airframe accidentally being overstressed. Also, if the Q system fails above 160 kts then a warning that low speed rudder power availability is reduced is captioned.

Twin yaw dampers are fitted which act in series with the rudder servo units constrain dutch roll. The authority of the dampers is scheduled to increase with advancing flap selection from one degree either side of applied rudder position with flaps up to two degrees either side with full flap. There is no feedback from the dampers to the rudder pedals except when full rudder is applied at low airspeed.

Pitch Control

Pitch is controlled by two mass and aerodynamically balanced elevators, each operated separately by a servo tab and an elevator trim tab. Two separate conventional cable and rod circuits are connected to each pilot's control column provide control over the respective elevator servo tabs. There is also a spring loaded 'disconnect' device that links both columns. If a jam occurs in one pitch control circuit then application of heavy pressure to the handwheel of the other circuit will cause the rigid detent strut to 'break-out' and transform into a sliding strut. The free circuit will then operate independently, allowing control to be maintained. This disconnection may also be performed with a handle in the cockpit, and may be reconnected in flight by matching control column positions. An autopilot is fitted to the left hand servo tab and acts in parallel with the control column, so that the control column is back-fed.

Each elevator servo tab circuit has a blow-back spring to limit the tab authority relative to the airspeed. A separate mechanical system drives the trim system. A 'G' weight is fitted on the First Officer's side to enhance the pitch feel under acceleration. A 'Q' pot fitted to the Captain's circuit increases feel as the airspeed increases. If there is a failure in this system then a caption illuminates. Stall warning is given by stick shakers, and a stall identification system gives a nose down push on the control column on stall detection. This push can be overridden by the pilots if necessary.

The elevator trim system has two sources of input, either one of the two trim wheels, or an electric trim motor operated by the pilot's thumb switches. Both trim systems operate through a common clutch unit. Operation of either trim wheel overrides the

electric trim unit, hence a runaway trim motor can be overcome by holding the trimwheel. The trim system also changes the 'Q' pot datum hence feel forces are maintained in the correct relation with aerodynamic forces. The electric switches operate at two different speeds, low for flap settings of UP and 18° and high for flap settings of 24, 30 and 33°. Both halves of the switch need to be operated together to effect a trim change in flight. There is also flap trim compensation which is used to trim out the first 14° of flap movement. This system has a warning caption when there is a fault.

Flaps

The flaps are single piece tabbed Fowler flaps, each operated by two screw jacks driven from two torque tubes crossing the wing. The left and right side torque tubes are joined at a gearbox where there are two hydraulic motors, each driven from one system. Asymmetry brakes, driven from the yellow system lock the flaps in the event of a fault resulting in more than a couple of degrees asymmetry. If one hydraulic system fails, then its motor will be locked, and the flaps will be driven at half speed. If both systems fail then the flaps will be locked in place to inhibit further movement. Selection of flaps away from the UP position is prohibited with airspeeds greater than 220 kts.

The electronic unit has two control lanes and two safety lanes. The control lanes control the hydraulic motors in the flap control unit. The safety lanes monitor the system from electrical or hydraulic faults, physical failures, etc. The control lanes also have a self-monitoring facility. A single fault within a single control lane may have various effects from no perceived loss to full failure, but complete failure is unlikely. A fault in both control lanes is likely tc lock the flaps in their current position. There is a separate electrical supply for each control lane, and the safety lane has a separate supply.

Spoilers

There are three lift spoilers and one roll spoiler on each wing, all hydraulically powered. The system is divided into two channels, with yellow hydraulic system powering both roll spoilers and the inboard lift spoiler, and green hydraulic system powering the centre and outboard lift spoilers, which are also mechanically connected. For yellow lift spoiler deployment, three of the four thrust levers must be retarded below flight idle, and two of the three landing gear oleos must be compressed. The system also offers protection from nosewheel bounce. The green lift spoilers deploy 1.5 seconds after main oleo compression has been sensed. This is to allow for progressive deployment. If the hydraulic power units fail then lacks engage to keep the lift spoilers retracted. The supply of hydraulic fluid to the spoilers is also controlled by selector valves. The lift spoilers may be selected for use on the ground after landing, or during an aborted take-off run.

Airbrake

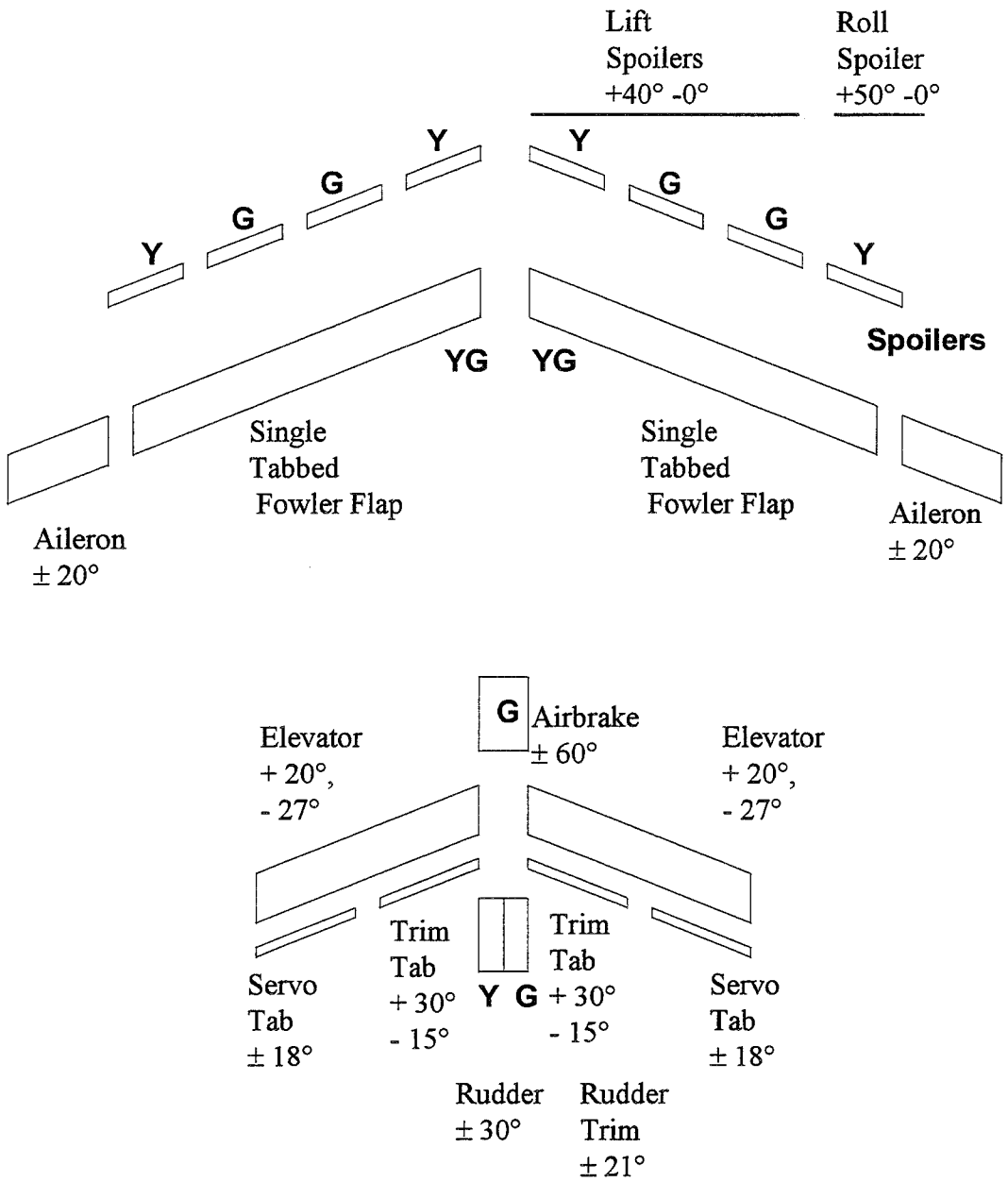
A twin petal airbrake is fitted as a tail cone. It is operated by a single hydraulic jack powered by the green system. The airbrake is inhibited when thrust levers 1 or 4 are at take-off settings. The airbrake will slowly close if this occurs, and will then re-deploy after the thrust levers are retarded, assuming it is still being demanded.

F.4 Bibliography

Anon. *BAe 146 Operations Manual.* British Aerospace.

MOIR, Ian; SEABRIDGE, Allan. Aircraft Systems. Longman, 1992

Flight International. Reed Business Publications. 9-15 Jan. 1991.



Key :

G	:	Green Hydraulic System
Y	:	Yellow Hydraulic System

Figure F1 : Avro RJ Control Surface and Hydraulic System Distribution

Appendix G. Kawasaki / National Aerospace Laboratory Aska (Flying Bird)

The Aska is a research aircraft designed to demonstrate the feasibility of short take-off and landing (STOL) at low airspeed. To improve low airspeed flying qualities, it has a Stability and Control Augmentation System (SCAS), which is designed to compensate for specific STOL aircraft characteristics.

The Aska was modified from a Kawasaki C-1 transport, with the added features listed

1. Four new turbofan engines installed above the main wing instead of the original two engines mounted below the wing. The engines provide powered lift through Upper Surface Blowing (USB), as with the Boeing YC-14 prototype.
2. Leading edge and aileron Boundary Layer Control (BLC) which uses engine bleed air, and provides improved flight characteristics at high angles of attack.
3. Acoustic panels in the engine nacelles to attenuate engine noise.
4. The Stability and Command Augmentation System (SCAS) which provides triple redundant digital flight control.

The aircraft made its first flight in October 1985, and the first STOL landing was demonstrated in March 1988.

G.1 Actuation

Two types of actuator are used. The first is a Series Servo Actuator (SSA), which is a triplex hydraulic actuator of the force summing type, which is used for elevator, ailerons, spoilers and the rudder. These control surfaces are commanded by mechanically summing the pilot's commands and the SCAS outputs.

The second type is a electric parallel servo motor which is used for control of the throttle levers, USB flaps and speed brakes. The USB flap control uses the fly-by-wire system, which is implemented only in hardware with a mechanical backup.

The SSAs are controlled by using the mid actuator signal from the three channels. When a failure is detected, i.e. the threshold value between the three signals is exceeded, that channel shuts down, and the appropriate hydraulic channel is de-energised at the actuator so as not to interfere with the operation of the remaining two channels. The transient from the first channel failure is negligible. When the second failure is detected, both channels stop the operation, and the SSA returns to the neutral position by a centring spring. Consequently the modes using it as a primary channel shut down. The transient caused by the second failure is at worst, 14% of the full stroke of the actuator.

G.2 Flight Control System

The development of the flight control system started in 1979, and emphasis was placed on fault-tolerant technology. Hence size and weight of the components was not a major design consideration, and off-the-shelf components were partly used. All SCAS flight functions had been tested by 1987. The general layout of the FCS can be seen in Figure G1 and Figure G2.

It has a triplex digital flight control system which provides one operational and two fail passive performance. This is applied to the SCAS because it is considered essential for STOL flight. To achieve fault tolerance performance, the system has redundancy management at two nodes. One node is the SCAS computer, which provides the redundancy management for the sensors and the computers themselves. The second nose is the Electronic Control Units, which provide redundancy management for the actuators with analogue circuits.

G.2.1 Independence of Redundant Channels

Achieving independence between the channels is essential in a fault-tolerant system. This means that failure of one channel does not cause failure of the other channels. A failure in one of the processors must not be transmitted across to the other processors, as happened on the second Iron-Bird test since the processors were initially connected by a single databus. In order to rectify this initial problem, the architecture was changed from the shared bus type to the dedicated bus type, where there is a dedicated link between ant two processors. However, this caused the problem that if a bus shut down, it was possible that one computer only receives two of the three possible input / actuator signals, and would not therefore carry out control law computation with identical signals. Hence a direct / indirect method was implemented in software, so that all of the data was passed both directly and indirectly. Hence all computers can cross-communicate via the databuses, even with one failed.

G.2.2 Flight Control Computers

These provides the following functions

1. Control law computation
2. Redundancy Management. This involves monitoring the computers and sensors.
3. Pre-flight Tests. These are automated and semi-automated. The checks are mainly on the hardware, and not on the functions which are monitored in flight.
4. Interactive function. This consists of the failure information display, parameter change, and navigational data display modes.

The flight control computers exchange data with the other two computers via the cross channel bus. The exchanged data is sensor signals, actuator commands, switch signals, mode logic flags and failure information. These bi-directional parallel buses independently interconnect between the computers to eliminate cross-channel fault

propagation. Frame synchronisation is established by software routines in the computers, which allows parallel operation of the computers.

When the monitors within the SCAS detect an intolerable failure, such as a CPU failure, or successive synchronisation failures, the SCAS stops the operation. Consequently the channel to which the failed computer belongs shuts down. After the first failure, the remaining channels operate continuously and provide flight critical functions. Upon the second computer failure, the SCAS shuts down.

G.2.3 Sensors

In normal operation, the control laws work with the data from the same sensor. Hence each channel selects the mid value of the three sensors. Also, the sensors are monitored, and any sensor which exceeds the threshold level from the other signals is declared failed. After the first failure, the average values of the remaining sensors is selected. When the difference between the remaining signals exceeds the threshold level, the correct signal is selected by a validity check routine. This routine depends on the sensor type. After the second failure, the remaining signal is always monitored by both the validity and data resemblance check routines. These latter routines monitor the rate of change of the signal with time, and when this exceeds pre-determined thresholds, this signal is also declared failed. Consequently the modes using it as a primary control signal are shut down. However, the other associated modes function continuously by using the last normal value. Thus the redundancy management scheme for the sensors provides two fail operational / three fail passive / degraded operation, unlike in computer failures.

The threshold levels for comparison and data resemblance monitors were determined from flight test data by measuring relative sensor performance under a variety of flight conditions, and hence determining acceptable thresholds. In particular, those signals from air data sensors were larger than the rest since they varied particularly with flight condition and sensor position. The thresholds were also calculated so they do not give large transients the ability to build up.

G.2.4 Databuses

The aircraft uses ARINC 429 databuses to interface the Internal Reference System (IRS), Head Up Display (HUD) and Monitor / Test Unit (MTU) to Interface Unit (IFU) the which then connects to the SCAS computer. The actuators are signalled through the Electronic Control Unit which receives its signals from the IFU. The rest of the connections are hard-wired links.

The SCAS computers are all connected by cross-channel databuses, with a bi-directional bus linking each processor pair.

G.3 Flight Control Laws

The Aska's flying qualities are inherently poor at low airspeed, and the SCAS has control modes which improves them. The following modes are available:

- Pitch and Roll Command Wheel Steering (CWS)
- Autotrim
- Yaw Damping
- Speed Hold - uses USB flaps as a Direct Drag Control device.
- Go around mode - provides automatic USB flap transition from STOL landing to Go Around position.
- Stall warning
- Auto USB and Auto Flap control.
- Engine failure compensation - minimises attitude change with failure
- Flight path control - flight path is controlled by a separate lever next to the throttles in the STOL configuration by varying the engine thrust and by using the speed brake spoilers as DLC.

G.4 Bibliography

Yamato, Hiroyuki; Okada, Noriaki; Bando, Toshio. *Flight Tests of the Japanese USB STOL Experimental Aircraft ASKA.* AIAA 88-2180. 4th Biennial Flight Test Conference. 1988.

Uchida, Tadao; Watanabe, Akira; Okada, Noriaki; Shimizu, Yukio; Iwasaki, Koji; Ishikawa, Munenori. *Triplex Digital Flight Control System for the STOL Research Aircraft "ASKA".* AIAA 88-3883-CP. 8th Digital Avionics Systems Conference. San Jose, California. 17-20 October 1988.

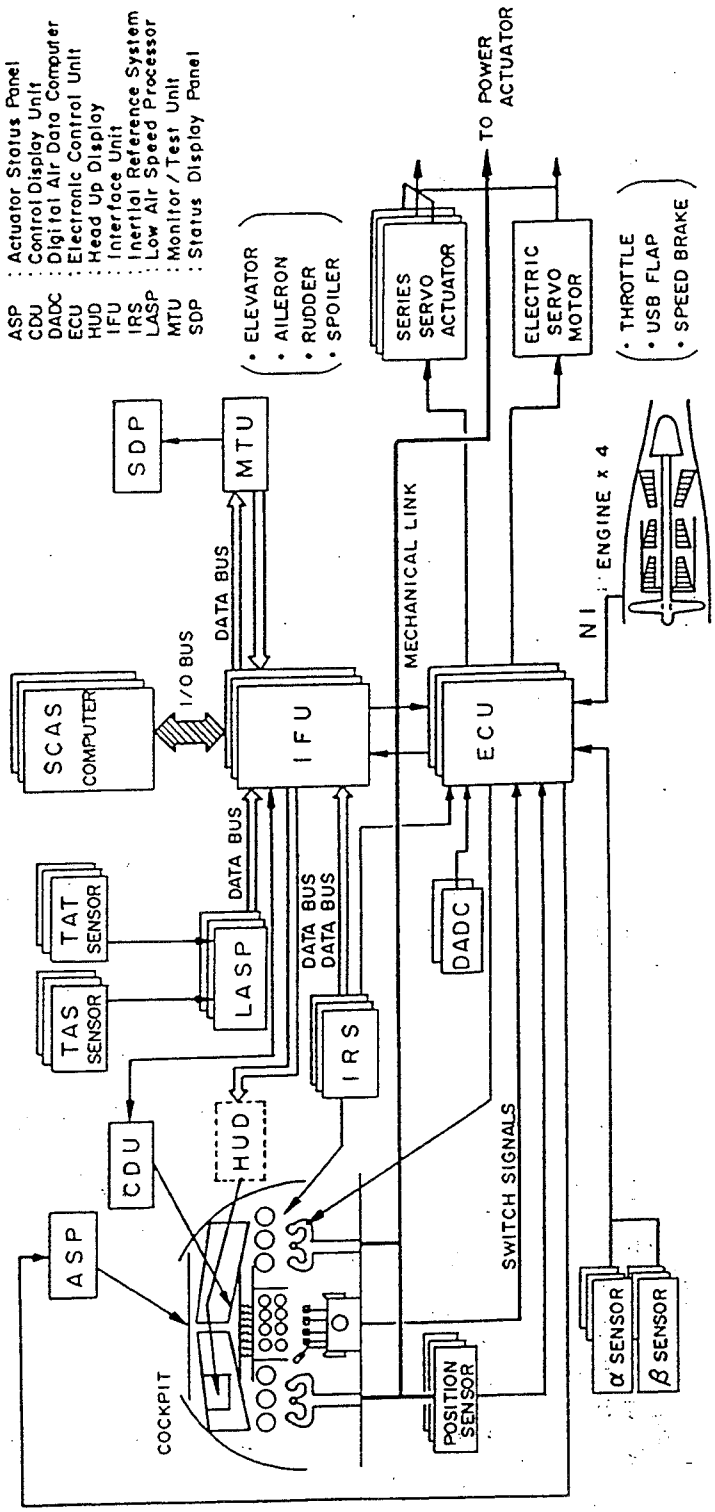


Figure G1 : SCAS Flight Control System Architecture

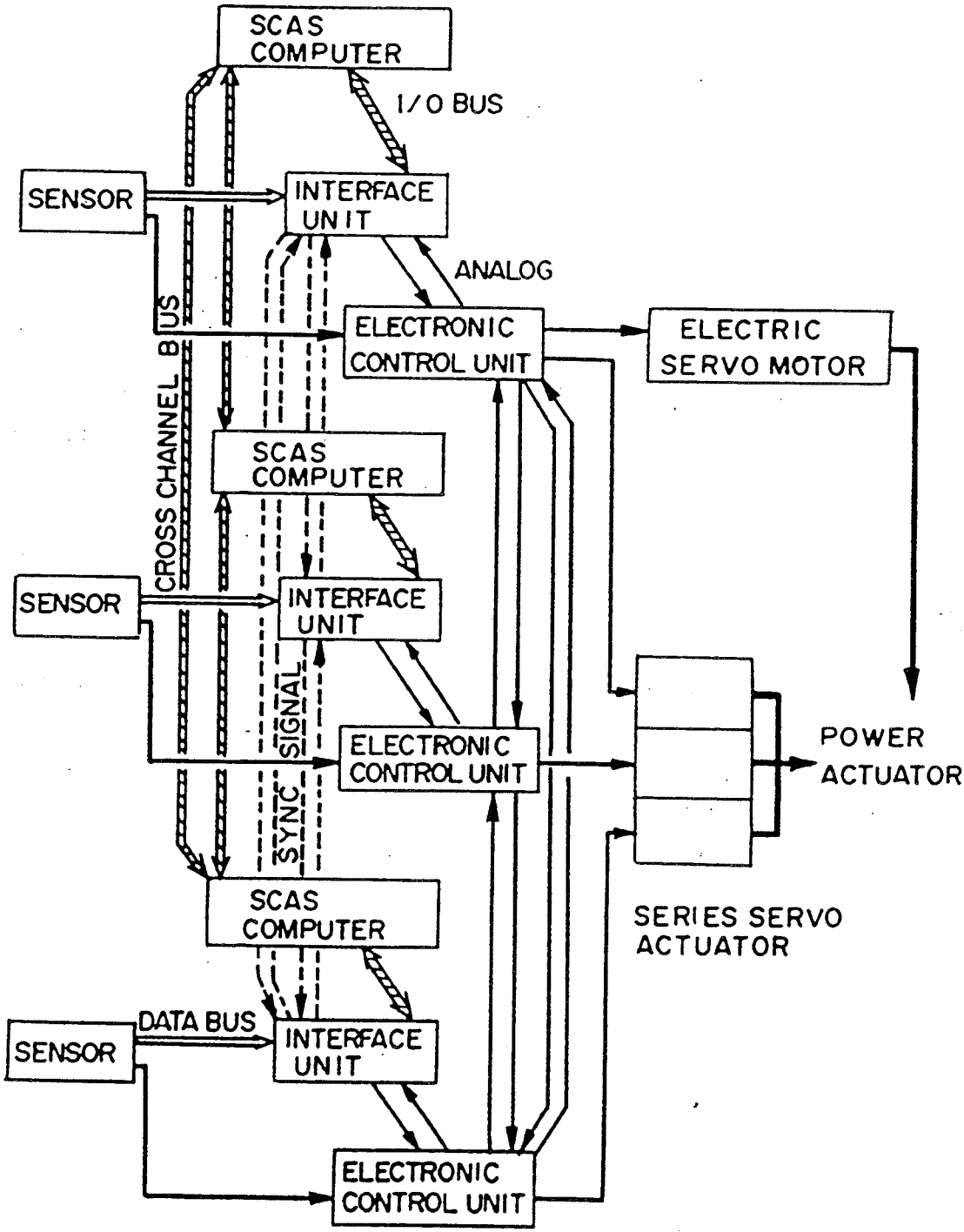


Figure G2 : SCAS Flight Control SystemTriplex Construction

Appendix H. McDonnell Douglas C-17 Flight Control System

The C-17 was designed to provide for rapid intertheatre deployment of combat forces to support national strategy goals, meet mobility requirements within a theatre of operation, provide a tactical outsize capacity not available now and provide needed total force structure modernisation. The C-17 made its first flight on 15th September 1991.

H.1 Power Supply Systems

The fuel, pneumatics, hydraulics and electrical switches are "set and forget" controls. The engines are controlled by the aircraft/propulsion data management system which is comprised of two Aircraft/Propulsion Data Management Computers. (A/PDMC). The A/PDMCs are linked by the data bus and 1553 mission bus.

H.1.1 Electrics

The electrical power system operates automatically to minimise pilot workload during normal and abnormal conditions. Manual controls are provided in the event of an automatic circuit failure. Primary electrical power is provided by 1 AC integrated drive generator per engine (75/90 kVA) connected to a split parallel bus. The DC power is supplied through 4 rectifiers. Emergency DC power and starting is provided through two Ni-Cad battery systems. A single phase inverter provides power for refuelling and emergency power. The batteries will power all emergency systems for 30 minutes.

Emergency DC power and APU starting is provided through two 42 amp-hr NiCad battery charger systems. A single phase 2000 VA inverter provides power for ground refuelling and emergency services.

H.1.2 Hydraulic System

Each of the four engines powers an independent 4000 psi hydraulic system. There are two pumps on each engine, plus an electrical motor-driven pump for redundancy. There is also a RAT on the No. 4 system for fail-safe protection that can be used for in-flight power. Any single hydraulic system with a single pump provides sufficient power for a safe landing. A reversible motor pump can provide power to a system that has lost all of its power sources.

The RAT powers the fourth hydraulic system in the event of loss of the four normal systems. The RAT would provide power to the right aileron, right mid-board and outboard spoiler, the lower rudder and the two left elevators. The stabiliser trim is also active, and the flaps are controllable.

H.2 Flight Control System

The probability of catastrophic failure is 10^{-9} per hour. This requirement is allocated between the Electronic Flight Control System (EFCS) and Mechanical Flight Control System (MFCS). The requirements also state that the flying qualities below level 3 shall not have a cumulative probability of 5×10^{-7} per mission (3.8 hours). The EFCS is allocated 10^{-7} per mission, and the remainder (4×10^{-7}) is allocated to the mechanical system and some hydraulic system (flight control) failures. The MFCS reliability requirement is 10^{-2} per mission. These requirements called for a quadruplex electronic flight control system with a simplex mechanical backup.

Automatic control functions provided by the EFIS are 3 axis Stability and Control Augmentation System (SCAS), autopilot, flight director, autothrottle and Automatic Flight Control System (AFCS). Full-authority quadruplex flight configuration is maintained in the 'electronic control' mode as long as 2 or more of the 4 FCCs are operational. In the event of 3 of the 4 FCCs failing, the hydromechanical system is automatically engaged.

The redundancy in the EFCS is incorporated by having

- 4 Flight control computers
- 2 Spoiler control / electronic flap computers
- 2 dual air data computers
- 3 three axis rate sensors
- 3 three axis accelerometers
- 1 quadruple sensor in each control stick
- 1 quadruple sensor in each rudder pedal

The quad redundant system provides an automatic three axis Stability Control Augmentation System than has a two fail operational /fail passive capability. The Automatic Flight Control System (AFCS) provides autopilot, flight director and autothrottle functions to reduce pilot workload in a variety of mission scenarios. The thrust management system allows the pilot to abuse the throttles without abusing the engines, and there is detection and compensation for engine out conditions.

The C-17 uses Department of Defense approved languages. At the inception of the C-17 contract JOVIAL was selected for use in the avionics computers including the FCC, SC/EFC, and AFCS. Other languages have been used in the computerised controllers such as C, Pascal etc. since they provide cost effective use of off the shelf microprocessors and their higher order languages that are prevalent in the industry. Assembly languages have been used for high throughput applications.

The Manual Flight Control System of the C-17 is provided by the SCAS function of the EFCS. The EFCS, in collaboration with the appropriate sensors and actuation system elements implements SCAS control laws which are intended to provide level 1 flying qualities.

H.2.1 Air Data Computers

There are two Air Data Computers (ADC). Air data signals and inertial signals are provided by quadruplex (two dual channels) Air Data Computers and quadruplex Internal Reference Units via the quadruplex FCS MIL-STD-1553B multiplex data bus. This interface can be seen on Figure H1.

H.2.2 Flight Control Surfaces

There are 29 control surfaces comprising

- 1 trimmable horizontal stabiliser
- 4 elevators
- 2 articulated rudders
- 2 ailerons
- 8 spoilers
- 4 flaps
- 8 slats

It was initially conceived as a dual redundant system, but a deep stall characteristic was discovered with this design hence a switch was made to a quad-redundant system employing digital FBW technology. A mechanical backup is incorporated on the ailerons, elevators, horizontal stabiliser and one rudder. The engines are fly-by-wire only. The aircraft could reach the deep stall condition about two seconds after the stall.

H.2.3 Flight Control Computers

Each FCC is the bus controller for a dual MIL-STD-1553B multiplex databus. The IRU and ADC interface with the FCS through the flight control bus and with the avionics system through a separate MIL-STD-1553B mission bus. Communication between the FCC and SC/EFC is also through the FCS databus. There is a 2 MHz serial broadcast bus Cross Channel Data Link (CCDL) between the FCCs which allows them to share data. The SC/EFCs also have a similar CCDL. The Electronic Engine Controller (EEC) communicates with the FCC through an ARINC 429 serial data bus.

Inputs from the pilot's controls and from the aircraft sensors are received on a channellised basis on the FCC databuses and from direct connections with the pilot position and force sensors. This data is exchanged via the CCDL. Each of the FCCs will therefore have identical data. An algorithm then selects one of the signals dependent on the sensor failure states. This is the average of the mid two signals for four signals, the mid value for three signals, and the average for two signals. A signal is deemed to be valid using threshold levels. The signals are also filtered to avoid nuisance faults. As output commands are generated, they are passed to an output buffer.

The actuator arrangement is shown in Figure H2. Each FCC is connected to each primary control surface actuator. Outputs from each FCC are summed at each of the electrohydraulic servo valves. An actuator interface filters out failed FCC outputs or faults, and prevents these faults from propagating to the control surfaces. Actuator outputs from the FCCs are compared across the CCDL in order to detect, identify and remove local faults. The FCCs also control the actuator valves in order to shut-off faulty actuator channels.

Each elevator, rudder and aileron is driven by two hydraulic actuators controlled by an integrated flight control module. The wing leading edge flaps are driven by two actuators on each of the 8 segments. The actuators are all controlled by a dual electromechanical actuator controlled by the Spoiler Control/Electronic Flap Computers (SC/EFCs), see Figure H3. Each of the four flap segments are driven by two hydraulic actuators controlled by a dual tandem electrohydraulic control valve. All four flap control valves are governed by the SC/EFCs. In addition, the SC/EFCs control the control law computations for the flaps, spoilers, slats and speedbrakes. These computers drive a redundant (except for the spoilers) set of electrohydraulic servoactuators. In the event of all failure of all digital control to the flaps, a backup analogue control channel is available to raise the flaps to the required TOGA position.

Full authority quadruplex flight control is installed with a two fail operational/fail safe configuration. In the event of three failures, the hydromechanical system is automatically installed.

H.2.4 Aircraft/Propulsion Data Management Computers (A/PDMC)

There are two of these computers which continuously monitor and control the engines. The A/PDMCs are integrated with the inertial navigation systems and the autothrottles through the mission computers. At forward airfields, taxi and ground operations can be conducted with only the inboard two engines running. Electrical and hydraulic power can be provided by these two engines for all the systems needs.

H.2.5 Databuses

The quadruplex FCCs and dual SC/EFCs operate as a frame synchronous set. Sync signals are exchanged between computers via a discrete signal interface. Should a computer fall out of synchronisation, it will immediately try to resynchronise. During an interval when a computer is unsynchronised it is more susceptible to nuisance failures. Loss of synchronisation is not grounds for computer shutdown.

There are a combination of MIL-STD-1553B and ARINC 429 databuses. ARINC 429 are used for the electronic engine controllers and also to link the flight control computers. The 1553 buses are used for the four dedicated flight control buses and the two mission buses. Cross channel data links allow the other computers within the system to pass data between themselves. The databuses can be seen on Figure H1.

H.3 Handling and Control Laws

The aircraft was designed to have better than level 3 handling qualities throughout all of the flight envelope, and this was met, except at high altitude. Here, it was found that the dutch roll metric was not quite met. Hence an emergency yaw damper was provided which operates on emergency electrical power. Two of the fight control computers retain control of the lower rudder in order to provide this damping.

The aircraft commences take-off in a direct control law. After take-off, this mode is cancelled, and the aircraft is flown in a rate command law. Stick force sensors take-over from the displacement sensors in the event of a stick jamming. The C-17 flies like an airliner in CWS mode. roll attitude hold is fitted, but without it, there were no problems due to the good spiral stability. In rate command, trim is automatic, but the trim is operational with the stick neutral.

There are only two control configurations. With the flaps retracted, the autopilot controls flightpath and the autothrottle controls speed. On approach and landing, when the flaps are lowered to three-quarters or full, the control shifts to the backside of the power curve technique that Naval Carrier pilots use. In this mode, the autopilot controls airspeed by varying aircraft pitch attitude, while the autothrottles control vertical speed. A conventional control wheel has been used since it was decided that a sidestick would not provide sufficient control forces in the manual back-up mode. The basic flight control mode is rate command attitude hold which makes the manoeuvrable C-17 stable.

The General Electric FBW system is held in take-off mode (direct stick/elevator coupling) until lift-off, then it takes up rate command in pitch and roll axes. The FBW masks the trim effects of configuration changes. In this take-off mode the elevator and rudder deflections relate to stick or pedal force while the aileron and spoiler deflections relate to stick angle in the take-off EFCS (Electronic Flight Control System). This mode is cancelled as soon as the stick is centred after take-off. The EFCS is used mostly in rate command mode which relates control surface position to stick deflection to give nearly constant stick force per 'g' and proportional roll rate. Having both position and force sensors means that force sensing can take over if a stick jams. There is an angle of attack sub-mode on the EFIS. If the alpha limit is approached then the pilot's sticks and pitch trim can only command nose down.

Spring breakout forces are well balanced, with feel springs in pitch and roll. Roll attitude hold will be fitted, but the spiral stability is good, and hence is hardly seems necessary. In rate mode the system autotrims, but trim becomes effective with the stick neutral. A 'coolie hat' switch on top of the stick operates pitch and roll trim.

Automatic spoiler functions are complex. With 3/4 or full flap, the small spoiler-up bias is modulated for DLC, large power lever movement or low speed. The drag adjustment gives immediate acceleration or deceleration, important for flying on the back side of the drag curve. The bias is removed above 75° thrust-lever angle. Flap

deployment or retraction is balanced by opposite spoiler movement to reduce the ballooning effect from the powerful blown flaps. However a small, but prompt change in pitch attitude is still required.

The pitch SCAS has the following submodes :

1. Pitch takeoff mode - direct elevator deflection to stick force. Active when on the ground
2. Pitch rate command / attitude hold mode - this is the basic mode and provides nearly constant stick force per g at a given airspeed.
3. Pitch attitude command / attitude hold mode - this mode commands a change in attitude from the pre-programmed reference value, and is active primarily during approach and landing.
4. Pitch rate command roll submode - this becomes active at large bank angles, and provides pitch rate command without an attitude hold function when the stick force is less than breakout.
5. Pitch rate command angle of attack limit submode - In this mode the pitch angle is commanded to prevent exceedance of the angle of attack limit.

The roll SCAS has the following basic modes :

1. Roll take-off mode - here the stick commands direct aileron deflection.
2. Roll rate command attitude hold - this is the basic roll command mode. Only the aileron commands are augmented, the spoiler commands are unaugmented.
3. Roll approach mode - this is the same as the roll rate command attitude hold except that the spoiler commands are also augmented.

The yaw SCAS has the following modes :

1. Yaw take-off mode - this is used on the ground and provides direct coupling of the rudder pedals to the rudder.
2. Yaw normal mode - this mode provides yaw damping, turn co-ordination, response to pilot rudder pedal input and parallel rudder pedal trim for yaw control. The turn co-ordination is active whenever the flaps are retracted.
3. Yaw emergency power mode - this is identical to the yaw normal mode except that turn co-ordination is not provided. It is intended to be used at altitude after the loss of electrical power. This is because the unaugmened dutch roll just does not meet level 3 requirements under these conditions.

Initial impressions were the pitch trim rate is very slow, but the auto trim responds to configuration and CG changes, hence it is only a nuisance in pre-departure checks.

Idling an outer engine with controls hands-off resulted in 2° adverse bank with only one-third displacement of the sideslip wedge. The system characteristics are similar to those of a FBW Airbus, except for the centre sticks, and the soft flight envelope

protection, as Boeing. A short period dutch roll was cancelled in one cycle. Bank angles can be rapidly reversed up to the mach buffet without any problems.

In the landing approach and touchdown the aircraft is flown on the backside of the drag curve by angle of attack, similar to an Aircraft Carrier style approach. Thrust controls descent, and pitch maintains speed, accepting small variations. As the flightpath vector (FPV) is raised, the angle of attack is reduced and vice versa. The FPV is adjusted to keep the approach-slope reference (ASR) line, which matches the ILS slope across the touchdown point. DLC is available when more than half flap is selected. This results in the spoilers being biased up, and are then moved to give DLC. Unlike other aircraft, where the DLC is coupled to the elevator control, the DLC is coupled to the thrust control. The pilot modulates the DLC by the speed brake 'paddle' switch, by holding it forward or back for short periods. It is easier and better to select the thrust for the required rate of descent, and then to control the flightpath by DLC.

Landings can be made with no change in attitude, giving a rate of descent up to 750 ft/min. The gear is stressed to 15 fps. There is a noticeable ground effect, with 200 fpm being removed just before touchdown. The gear is extremely effective in removing the impact. The spoilers can also be used to cushion the landing phasing out the up-bias based on a radio height schedule. Approaches made with an engine shut down are not too difficult since the problems created by the lack of thrust and lack of one blown flap are countered by the EFCS.

The C-17's control on the back side of the drag curve bears favourable comparison to Concorde with its delta wing or the Lockheed C-130 high-technology testbed with blown flaps. The C-17 flaps can be set at any angle, enabling the deck angle to be accurately specified on airdrops. The command attitude control seems to be the right tool for precise landings on small strips (such as on aircraft carriers).

In the manual backup mode, dutch roll can be excited to large levels with deliberate inputs, but it is convergent, and can be captured. There is a fair amount of yawing on entering and leaving turns, but in steady, still air flight it does damp out or can be countered with well-judged counter-aileron. The yaw damper requirement is being revised since some reduction in yaw stability is expected above 20000 ft. The rule is hence to slow up and descend if problems are experienced. The pitch stability was good.

H.3.1 Protections

One of the main reasons for putting quadruplex fly-by-wire instead of dual-dual into the C-17 was the deep stall characteristic that wind tunnel tests showed to be unrecoverable. Hence there is an angle-of-attack limiter system (ALS) which prevents stalls by not letting the aircraft get into unrecoverable attitudes by limiting the angle of attack the pilot can command. A stick shaker is also provided. The ALS computes the limited angle of attack based on speed, engine pressure ratio and aircraft configuration.

H.3.2 Failures and Alternate Modes

In the event of three channel failures, the C-17 can revert to a mechanical backup on the elevators, lower rudder, ailerons and horizontal stabiliser.

Some specific failure modes that the FCS is designed to cope with are a jammed control stick, triplex failures, and generic software faults. Position and force sensors are located at the top and bottom of the stick respectively, with the position sensors being used with normal operation. The mechanical system can be selected by hand. Reversion from position to force sensors has a small transient, and the handling remains level 1.

H.4 Bibliography

Aviation Week and Space Technology. McGraw-Hill. 6 Feb. 1995

Flight International. Reed Business Publications. 13-19 Nov. 1991

Flight International. Reed Business Publications. 19-25 May 1993.

Kowal, Brian W; Scherz, Carl J; Quinlivan, Richard. *C-17 Flight Control System Overview.* NAECON 92. Dayton Convention Center. 18-22 May 1992.

Tavernetti, Leonard R. *The C-17: Modern Airlift Technology.* Douglas Aircraft Co. SAE Paper 911967.

Watkins, Mike; Garrette, Doug. *Advancing Airlift Avionics C-17 Avionics Suite.* McDonnell Douglas Aerospace. AIAA 93-0986. AIAA Aircraft Design, Systems and Operations Meeting. August 11-13 1993. Monterey, CA.

Weindorf, Paul. *The C-17 Multifunction Display - A building block for Avionic Systems.* NAECON 92. Dayton Convention Center. 18-22 May 1992.

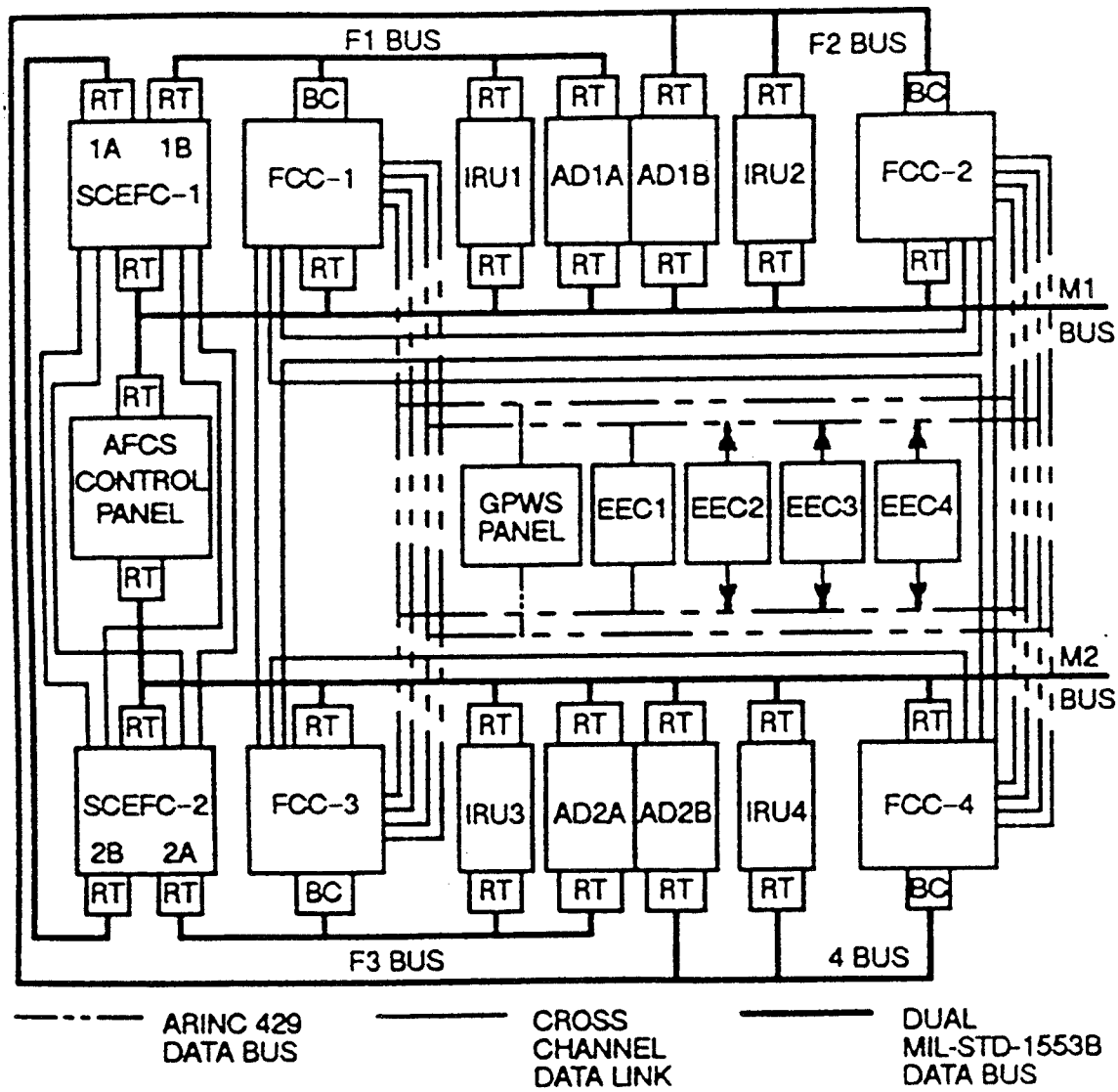


Figure H1 : McDonnell Douglas C-17 Electronic Flight Control System Databus Architecture

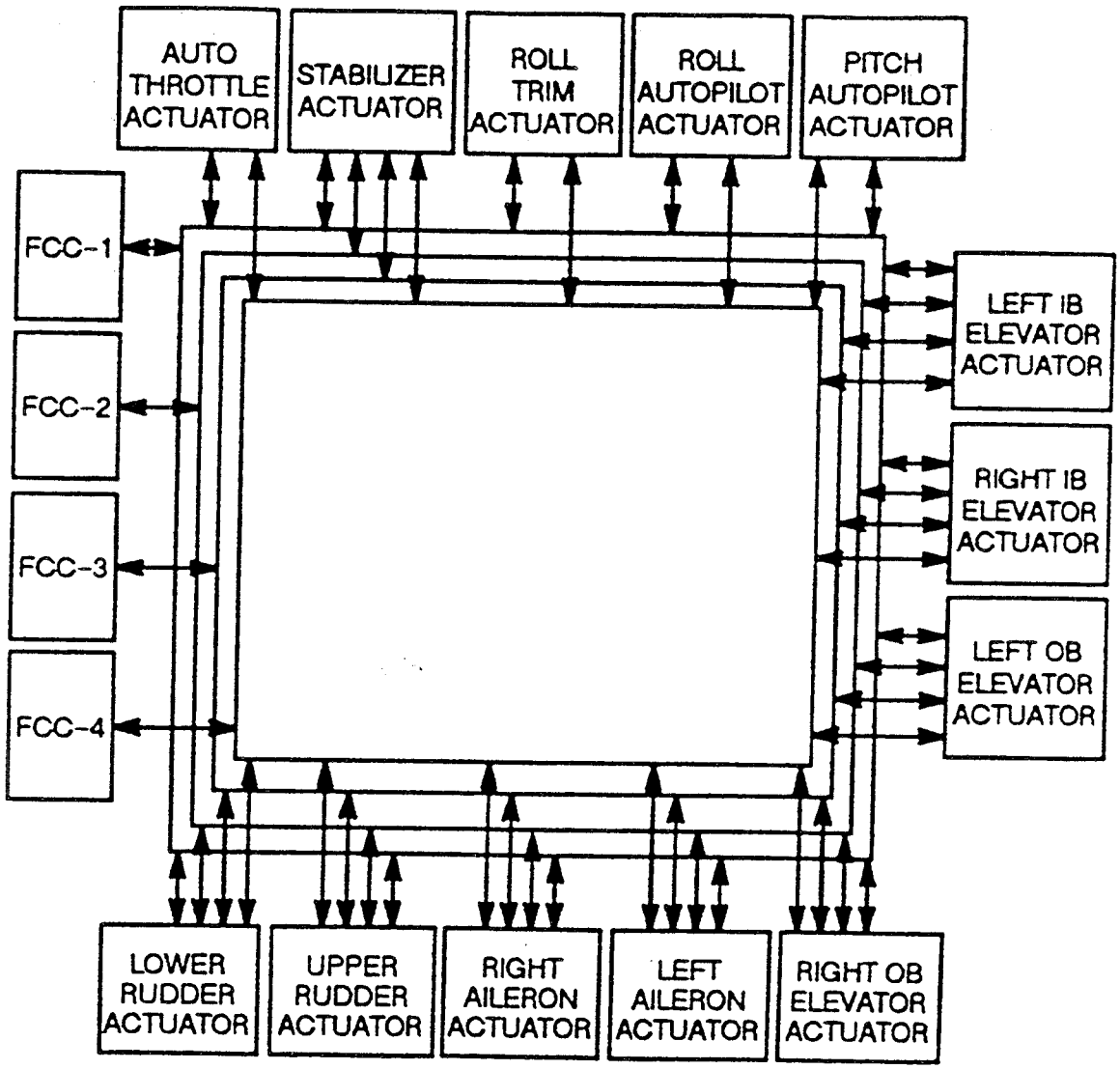


Figure H2 : McDonnell Douglas C-17 EFCS Interface

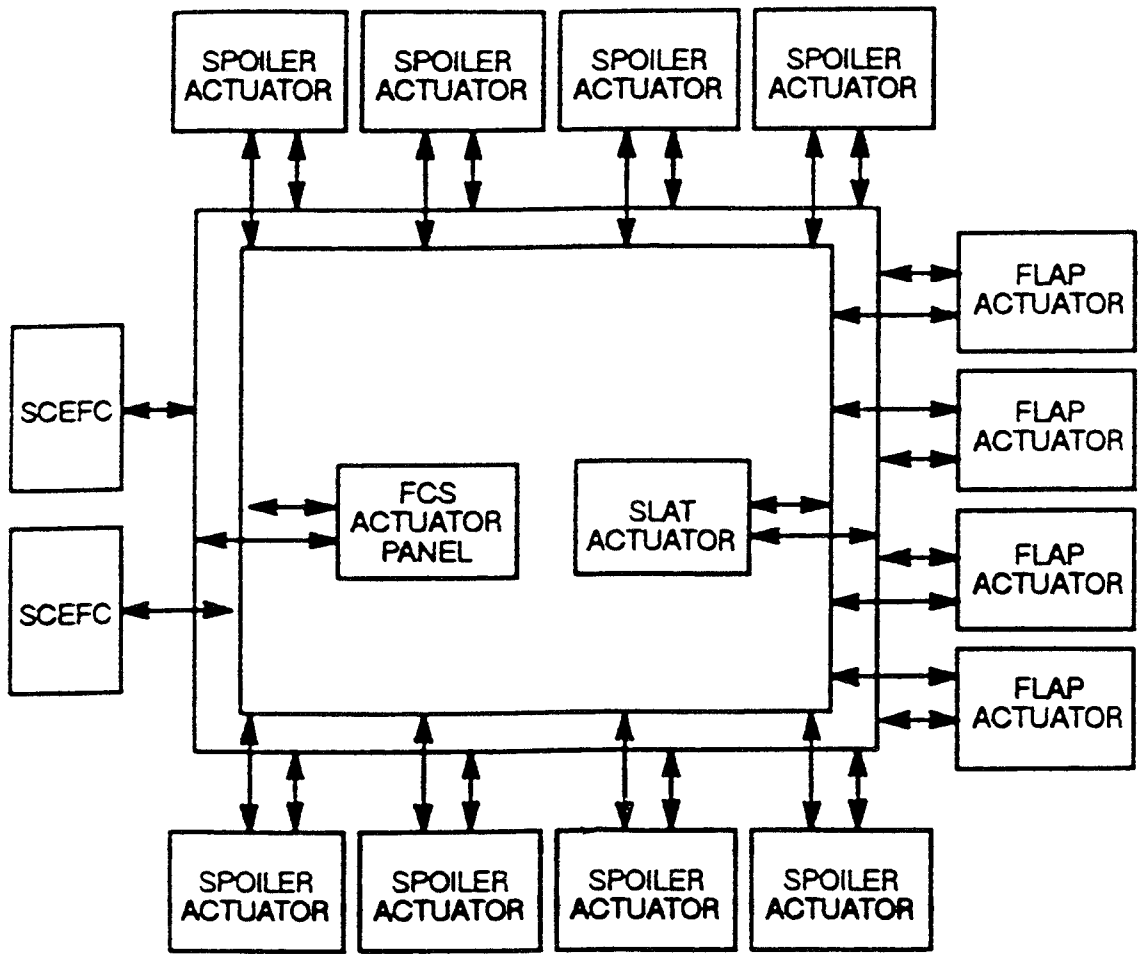


Figure H3 : McDonnell Douglas C-17 SCEFC Interface