Design Considerations in Boeing 777 Fly-By-Wire Computers

Y. C. (Bob) Yeh
Boeing Commercial Airplane Group
Flight Systems
P. O. Box 3707, M/S 02-KA
Seattle, WA 98124-2207
ying.c.yeh@boeing.com

Abstract

The new technologies in flight control avionics systems selected for the Boeing 777 airplane program consist of the following: Fly-By-Wire (FBW), ARINC 629 Data Bus, and Deferred Maintenance.

The FBW must meet extremely high levels of functional integrity and availability. The heart of the FBW concept is the use of triple redundancy for all hardware resources: computing system, airplane electrical power, hydraulic power and communication paths.

The multiple redundant hardware are required to meet the numerical safety requirements. Hardware redundancy can be relied upon only if hardware faults can be contained; fail-passive electronics are necessary building blocks for the FBW systems. In addition, FBW computer architecture must consider other fault tolerance issues: generic errors, common mode faults, near-coincidence faults and dissimilarity.

1.0 Introduction

The NASA FBW projects [1],[2] provide the numerical integrity and functional availability requirements for FBW computers. A finding from the research, Byzantine General problem [3], also serves as a design consideration to assess robustness of FBW computer architectures. Past Boeing and other industry experiences in dealing with generic faults [4], near-coincidence faults [5] provide ground rules for the Boeing 7J7 FBW program. The experiences on the 7J7 program [6],[7],[8],[9] and the academic research on design diversity [10],[11], design paradigm [12] are carried over to the 777 FBW program [13],[14],[15].

Furthermore, to certify the 777 FBW program, the flight controls design and development process considers all requirements from: airplane functional groups, certification agencies, customers, in-service experiences, technology trends and design paradigm. The Boeing 777 FBW requirements were then derived and developed.

The purpose of this article is to describe the new technologies employed directly and indirectly for the 777 primary flight control system, with an emphasis on the design considerations for the FBW computer architecture. The fail-passive electronics for flight critical avionics systems are defined to illustrate the necessary building blocks for the forward path, from pilot inputs to control surface, flight controls electronics.

2.0 Outline of New Technologies for 777 Flight Controls

Traditionally, new technologies are introduced for a new airplane program, and the 777 is no exception. The challenge is the selection of the new technologies which can best meet the desire for more functionality with higher reliability and easier maintainability. That is to say, the incorporation of new technologies is to add value for our customers. The new technologies selected directly or indirectly for the flight controls were: 1) FBW, 2) ARINC 629, and 3) deferred maintenance.

2.1 Outline of the Primary Flight Control Function

The outline of the 777 FBW system has been described [6],[13],[14],[15]. The primary flight control surfaces are illustrated in Figure 1, and an overview of the FBW system is shown in Figure 2. Figure 3 shows the hydraulic power distribution for the Power Control Units (PCUs) to which Actuation Control Electronics (ACEs) provide electrical control.

2.2 ARINC 629 Digital Data Bus

The ARINC 629 data bus [16] is a time division multiplex system. It includes multiple transmitters with broadcast-type, autonomous terminal access. Up to 120 users may be connected together. The users communicate to the bus using a coupler and terminal as shown in Figure 3. Terminal access is autonomous. Terminals listen to the bus and wait for a quiet period before transmitting. Only one terminal is allowed to transmit at a time. After a terminal has transmitted, three different protocol timers are used to ensure that it does not transmit again until all of the other terminals have had a chance to transmit.

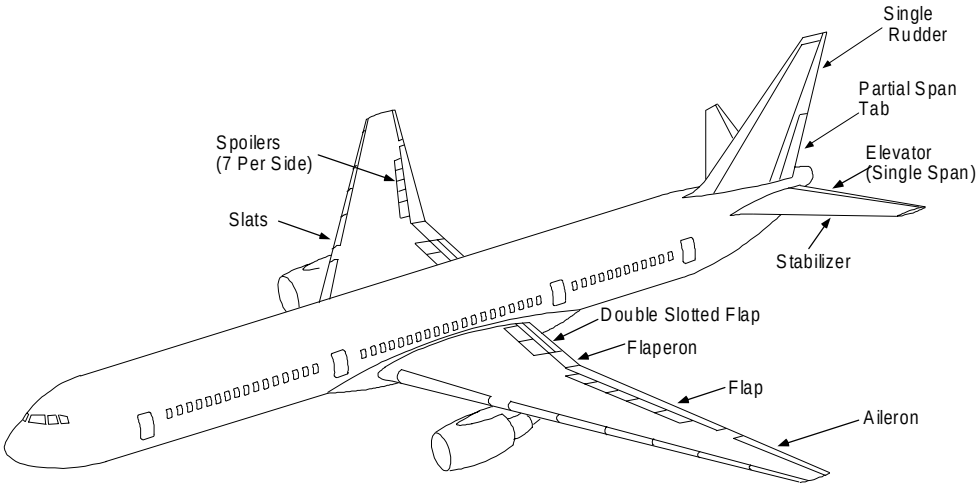

FIGURE 1 777 FLIGHT CONTROL SURFACES

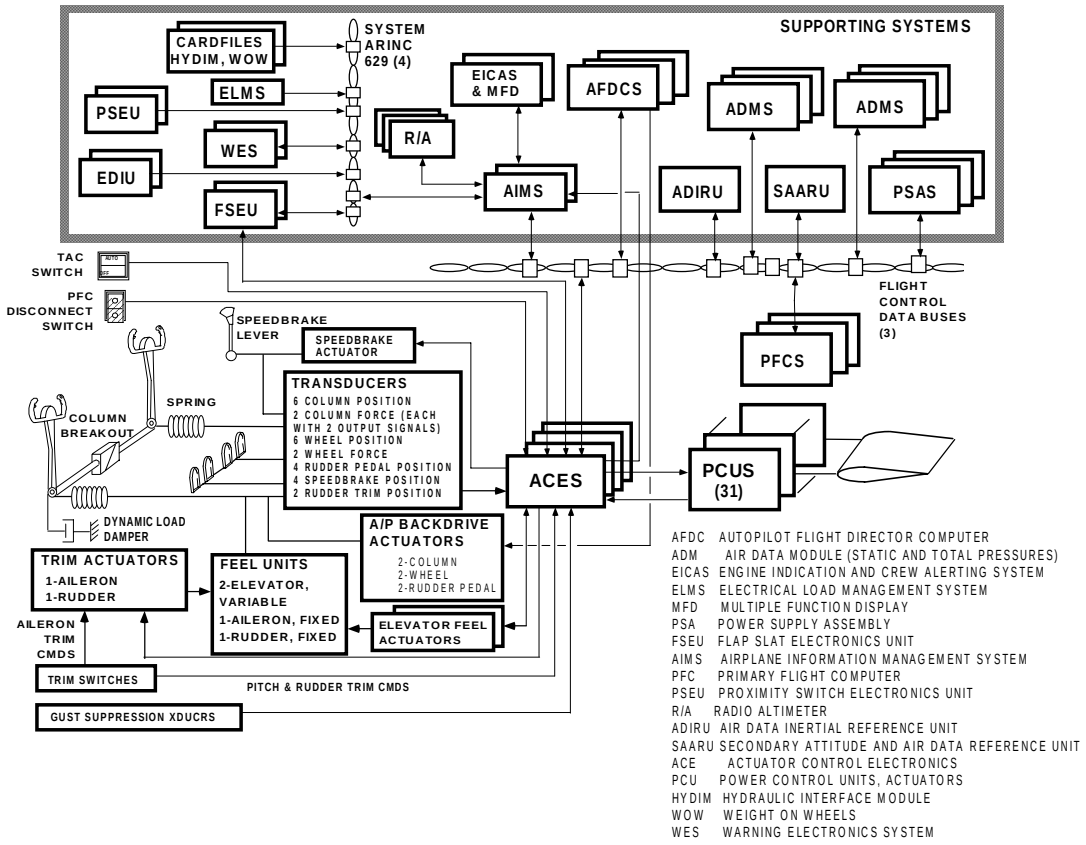

FIGURE 2 777 PRIMARY FLIGHT CONTROL SYSTEM OVERVIEW

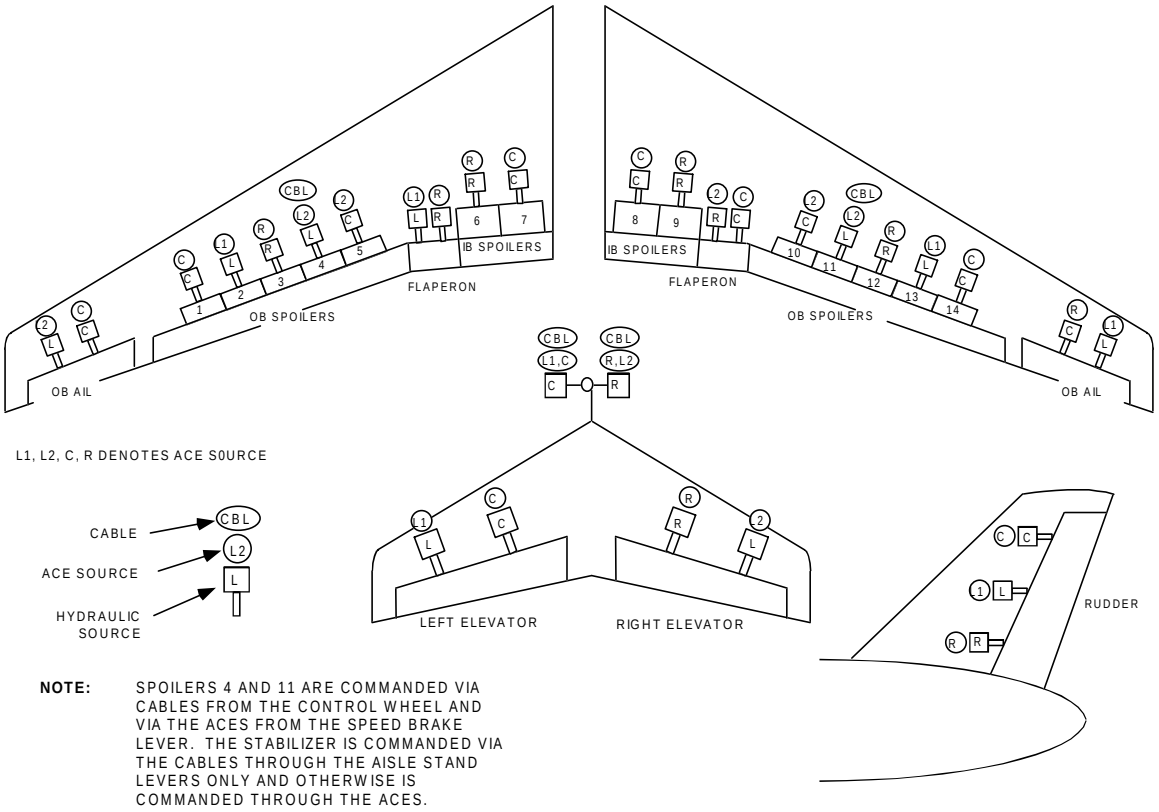

Figure 3 Primary Flight Controls Hydraulic/ ACE Distribution

Figure 4 shows the interconnection of two systems using an ARINC 629 terminal controller and Serial Interface Module (SIM) which are installed on a circuit board within each Line Replaceable Unit (LRU). The SIM interfaces with the stub cable via a connector on the LRU. The stub cable is then connected to the global data bus via a current mode coupler.

A representation of the main internal logic and data flows within an ARINC 629 terminal controller is shown in Figure 5. Data enters through the demodulator and is checked for faults. The receiver circuitry monitors all incoming labels and determines which wordstrings are needed. The data needed by the attached users is sent to the subsystem interface and to the users.

2.3 Deferred Maintenance

The deferred maintenance has been a desirable attribute for customer airlines to enhance airplane dispatch reliability. The deferred maintenance concept mandates the need for the fault tolerant design for the major digital avionics systems such as PFC, ADIRS (Air Data Inertial Reference System) and AIMS (Airplane Information Management System.) Based on Life Cycle Cost study for an optimum redundancy level for airlines, these computer architectures contain one level of redundancy beyond that required to achieve the functional integrity for airplane dispatch. Consequently, repair of random hardware failures can be deferred to a convenient time and place, resulting in reduction of dispatch delays or cancellations.

The triple-triple redundant PFC architecture, triple channels with triple dissimilar lanes in each channel, has been described [14]. The PFC can be dispatched with one failed lane: maintenance alert is generated for maintenance attention. The PFC can also be dispatched with one failed channel: flight deck status message is generated requiring replacement of a PFC channel within three flights.

The ADIRS and AIMS architectures can be summarized as follows.

2.3.1 Air Data Inertial Reference System

This system evolved from the Air Data Computers and Inertial Reference Systems on previous airplanes. The system consists of traditional triple-redundant pitot and static ports, whose signals are converted to electrical signals by Air Data Modules mounted near the probes. Digital signals are sent via Flight Control ARINC 629 buses to the ADIRU and SAARU for processing, as shown in Figure 6. The ADIRU and SAARU are fault tolerant computers with angular rate sensors and accelerometers mounted in a skewed-axis arrangement [17]. The ADIRU can be dispatched with one failure of each of the following assemblies: angular rate sensor, accelerometer, processor, and I/O module.

2.3.2 Airplane Information Management System

The AIMS is the data cruncher for the following functions: 1) flight management, 2) thrust management, 3) display, 4) data communication, 5) central maintenance, 6) airplane condition monitoring, 7) flight data recording, and 8) digital data gateway.

The AIMS communicates with the majority of avionics systems on the airplane. These interfaces are implemented through several different media, including ARINC 629 data buses and ARINC 429 data buses. The AIMS [18]consists of two separate and independent cabinets, each with four core processors and four input/output modules. The AIMS can be dispatched with one failed processor module and one failed I/O module.

3.0 Design Considerations for Primary Flight Computers

Earlier on the research program for the Boeing 7J7 airplane, we were to define a methodology for determining need and means of protection against generic errors [4] and common mode faults. The approach taken evolved to the 777 program.

3.1 Common Mode Fault

Common mode or near-coincidence faults[4],[5] need to be considered for multiple redundant systems such as the FBW. Airplane susceptibility to common mode and common area damage is addressed by designing the systems to both component and functional separation. This includes criteria for providing installations resistant to maintenance crew error or mishandling.

The FBW design and installation has been developed with the following fault or event considerations (to name a few):

- impact of objects
- electrical faults
- electrical power failure
- electromagnetic environment
- lightning strike
- hydraulic failure
- structural damage
- radiation environment in the atmosphere
- ash cloud environment in the atmosphere
- fire
- rough or unsafe installation and maintenance

These common mode concerns led to the FBW requirements for separation of FBW components and FBW functional separation.

3.1.1 Separation of FBW Components

The separation is required for redundant flight control elements including LRUs, associated wiring and hydraulic lines to the greatest extent possible.

General system/airplane design decisions for separation include the following:

- multiple equipment bays for redundant LRUs,
- physical separation of redundant LRUs,
- flight deck equipment and wiring separation and protection from foreign object collision, and
- separation of electrical and hydraulic line routing through airplane structure.

Thus triple PFC channels are separated physically, and tight synchronization among PFC channels is deemed undesirable. To maintain source congruency and system states convergence, PFCs are required to consolidate their system states, and to equalize critical variables. The assumption of near-coincidence [5] PFC shutdown is considered in the redundancy management design for the PFC restart and for determining PFC system state convergence rates.

3.1.2 Functional Separation

All triple redundant hardware resources are aligned to the Left (L), Center(C) and Right (R) positions. These hardware resources are electrical power, flight control ARINC 629 buses, PFCs, ACEs, Hydraulic systems.

ACE functional actuator control is distributed to maximize controllability in all axes after loss of function of any ACE or supporting subsystem. In general, the electronics components powered by the L/C/R flight control electrical bus controls the actuation components powered by the L/C/R hydraulic system, respectively.

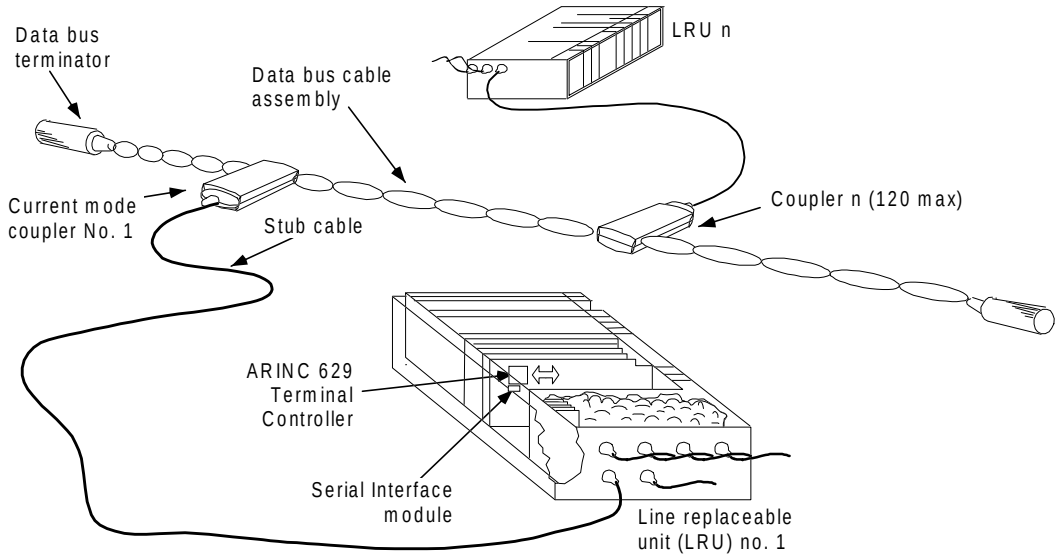

Figure 4 Interconnect of Systems using ARINC 629

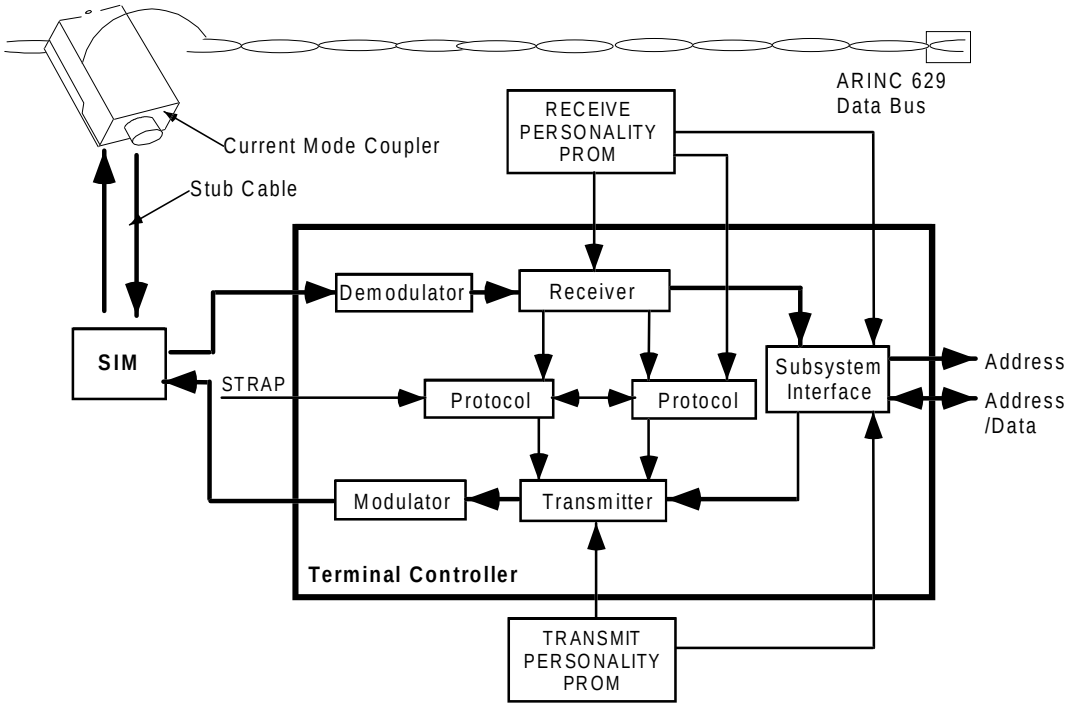

Figure 5 ARINC 629 Functional Block Diagram

3.2 Design Diversity

Based on the Boeing experience, the most likely design errors are, in order of likelihood:

a) i) Requirement errors
b) ii) Implementation misunderstanding
c) Software design or coding error
d) Future process errors in previously qualified
e) Semiconductor parts.
f) Relatively new, programmable VLSI circuits whose number of states approach infinity and therefore are non-deterministic.

The 7J7 FBW program goal regarding dissimilarity is developed as follows.

1. Dissimilar software/hardware architecture should be used.
2. Ada should remain the accepted standard for embedded software.
3. When dissimilar hardware and software is used to reduce error in FBW computers, steps should be taken to ensure the designs are also dissimilar.

In the design diversity experiment at UCLA [10], the isolation rules were employed in which programming teams were assigned physically separate offices for their work and that inter-team communications were not allowed. The research at academe [10],[11] indicate that multiple versions of programs developed independently can contain similar errors.

Boeing experience is that among sources of errors it is most often the basic requirements which are erroneous or misinterpreted. The key to a successful software implementation is the elimination of errors. The errors due to misinterpretation can be reduced by very close communication between the system requirements engineers and the software designers. In fact, the software designers can help the engineers recognize limitations in the software design when the requirements are being written. There is much benefit from this interactive relationship, which is precluded by the dissimilar software design approach, where systems and software teams much be kept segregated.

The development of the PFC software during the 7J7 program confirmed that the three separate teams, in order to code their logic from the requirements, were having to ask Boeing so many questions for clarification of the requirements that the independence of the three teams was irreparable compromised. This is the reason why Boeing elected to revert to the usual and customary method of creating and certifying flight critical source code. It was determined that there is a net gain in total system integrity with the single software design approach. The overall 777 FBW program decision on dissimilarity is described in [15], and is summarized as follows.

3.3 Safety Analysis

The safety analysis is performed which assesses all significant failures of the FBW system including single failures, latent failures, and failure combinations at the LRU level. Allowable level of dispatch with known faults is determined. Also considered is the scheduled maintenance necessary to limit exposure to latent faults. The analysis shows that the probability of a given failure condition is consistent with its severity, and that all failure combinations producing a catastrophe are extremely improbable. This analysis contains a proposed list of worst case failure conditions to be flight demonstrated based upon simulator evaluation, and documents confirming lab and flight test results.

Hardware component failure modes and potential LRU malfunctions are assumed. The assumptions, combined with the system architecture and fault detection/isolation algorithms, are used to eliminate the infinite possibilities of hardware gate level failure modes. Interfacing systems such as electrical and hydraulic power, ARINC 629 buses, and primary sensors are included. System separation, partitioning, and redundancy are addressed. Where possible in-service data are used to generate probability of faults.

3.4 Fail-Passive and Fail-Operational Electronics

An electronics function is fail-passive if, in the event of a failure, the continued safe flight and landing of an airplane can be maintained by the pilot. Firstly the FBW architecture study considering use of ARINC 629 data busses concluded that common interface requirements [15] should be developed including a common CRC (Cyclic Redundancy Check) algorithm.

The ACE functional overview diagram is shown in Figure 7, and the FBW forward path (ACE to/from PFC) signal monitoring concept is shown in Figure 8 to illustrate the application of fail-passive electronics.

The transducers used to sense the pilot control commands are monitored with in-line monitors of common mode monitor (CMMs) and demodulator monitor (DMMs). This includes the position and force transducers. The CMMs detect short circuits and open circuits in the pilot control transducers, while the DMMs are used to monitor demodulation of each AC transducer signal. If either monitor indicates failure, this signal will not be used by PFCs for FBW control law function.

The servo command wraparound monitors verify the proper operation of ACE digital-analog and analog-digital conversion hardware and verify proper distribution of each PCU/Actuator command to the appropriate servo loop function.

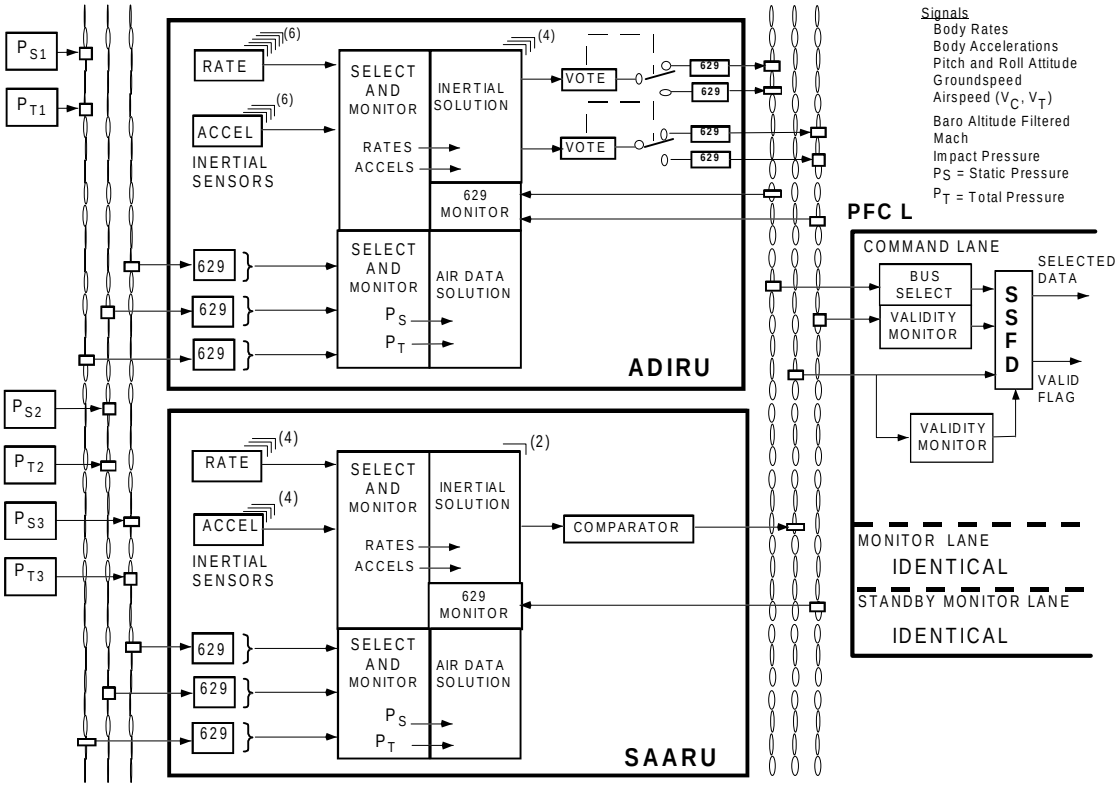

Figure 6 ADIRU/SAARU Redundancy Management

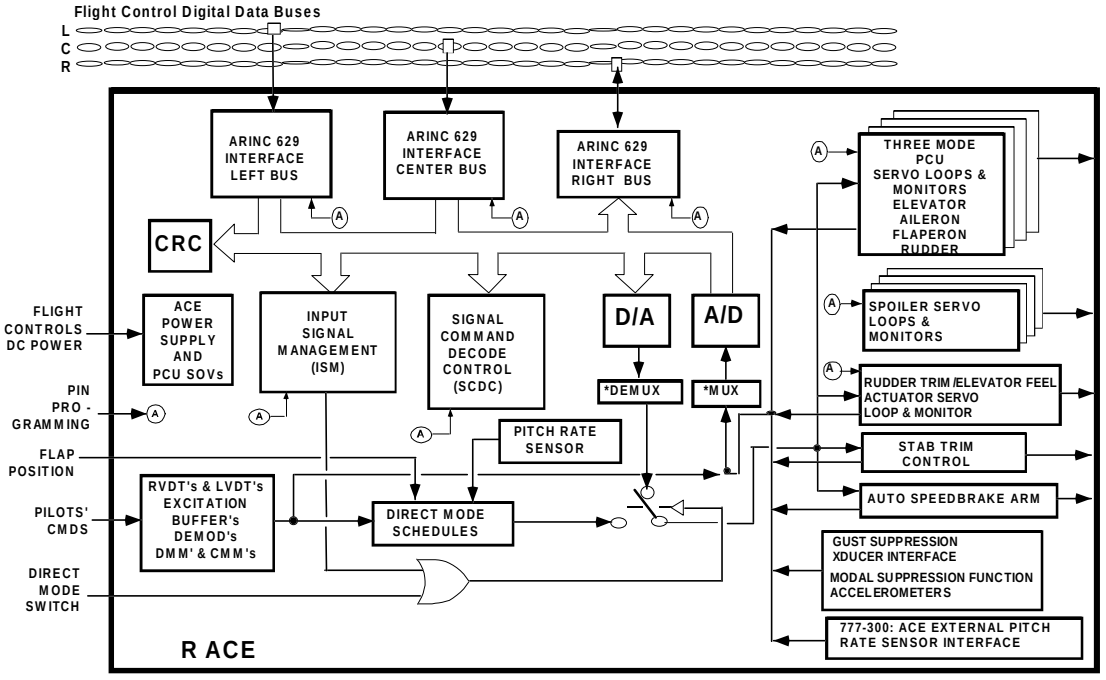

Figure 7 Typical ACE Architecture

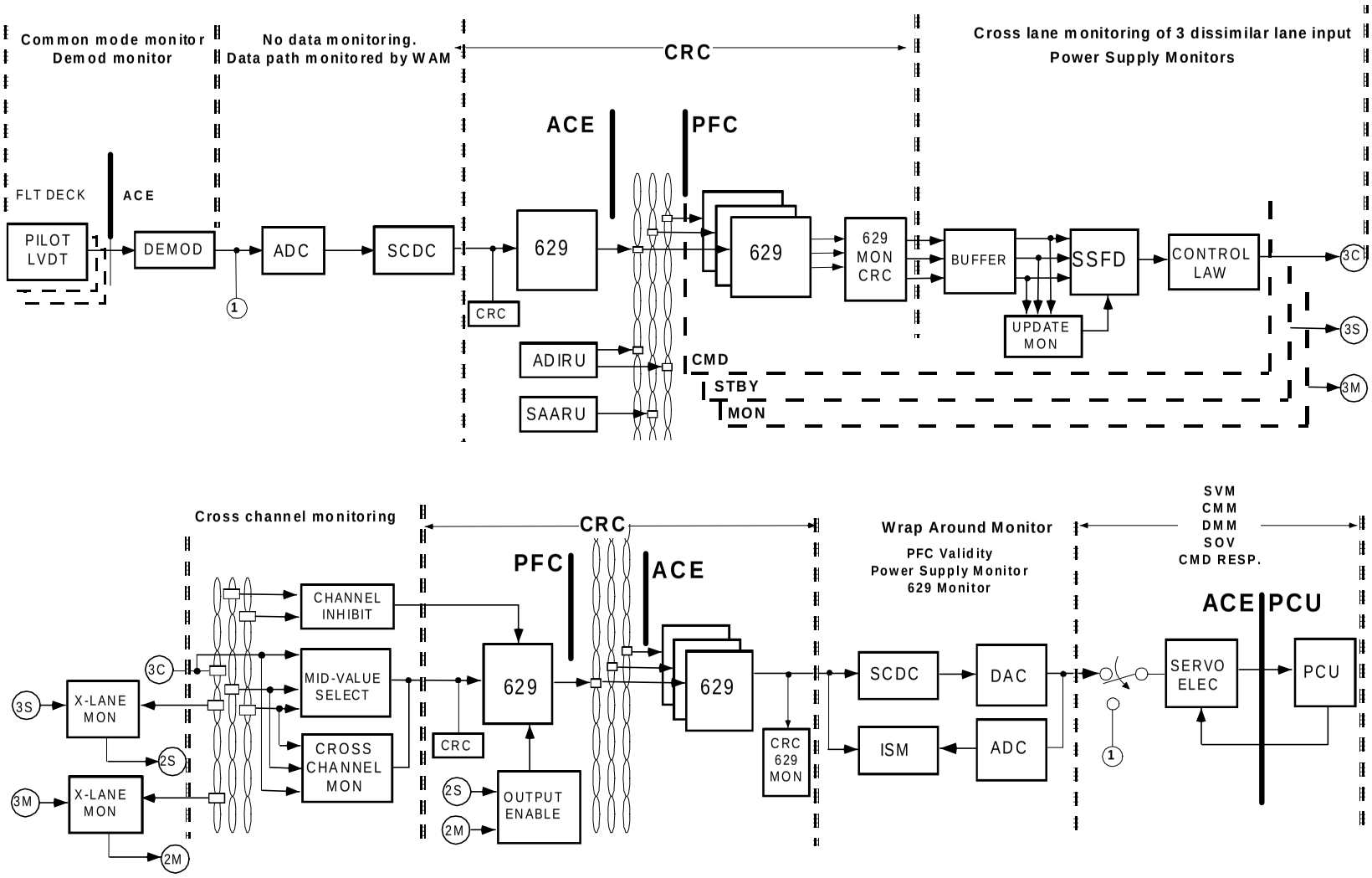

Figure 8 PFCS Signal Path Monitoring

Digital commands received from the PFCs are converted to analog commands for use by the actuator servo loops. The analog servo loop commands are also converted ("wrapped") back to digital form for use by the Wraparound Monitor. The monitor then compares the original digital commands with the wraparound commands to verify operation of digital to analog and analog to digital conversion.

All LRUs transmitting critical data on ARINC 629 bus are required to comply with the Flight Controls Bus Requirements [15] inclusive of providing CRC checkwords. All flight critical LRUs (eg, PFC & ACE) perform CRC monitoring of each received wordstring.

Input Signal Management (ISM) processing is performed by each PFC on ARINC 629 input signals received by the PFCs including those originating from the ACEs, ADIRU, SAARU, ADMs, AFDCs, and AIMS. ISM includes Signal Selection and Fault Detection (SSFD) algorithms which perform signal selection and static and dynamic fault monitoring. This algorithm must be designed to adequately isolate failed components for an extended period of time where delayed maintenance is desired.

4.0 Summary

The successful certification of the first Boeing FBW airplane, airplane in general and FBW in specific, in four and half years depends to a large extent on the following: 1) a new facility to accommodate a large number of test labs, the Integrated Aircraft Systems Lab (IASL), 2) a viable FBW architecture, 3) working together with customer airlines for their help in designing the airplane, 4) certification planning, 5) research work from the fault tolerant computing community.

References:

1. J.H. Wenseley et al "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control", Proceeding of the IEEE, Vol. 66, No. 10, October 1978.
2. A.L. Hopkins Jr., T.B. Smith,III, J.H. Lala, "FTMP-A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft", Proceeding of the IEEE, Vol. 66, No. 10, October 1978.
3. L. Lamport, R. Shostak, M. Pease, "The Byzantine Generals Problem", ACM Trans. on Programming Languages and Systems, Vol. 4, No. 3, July 1982.
4. S.S. Osder, "Generic Faults and Architecture Design Considerations in Flight-Critical Systems", AIAAJournal of Guidance, Vol.6,No.2, March-April 1983.
5. J. McGough, "Effects of Near-Coincident Faults In Multiprocessor Systems", Fifth AIAA/IEEE Digital Avionics Conference, October 1983.
6. R.J. Bleeg, "Commercial Jet Transport Fly-By-Wire Architecture Consideration", Ninth AIAA/IEEE Digital Avionics System Conference, October 1988.
7. C.J. Walter, "MAFT: An Architecture for Reliable Fly-By-Wire Flight Control", Ninth AIAA/IEEE Digital Avionics Conference, October 1988.
8. A.D. Hill, N.A. Mirza, "Fault Tolerant Avionics", Ninth AIAA/IEEE Digital Avionics Conference, October 1988.
9. R.A. Hammond, D.S. Newman, Y.C. Yeh, "On Fly-By-Wire Control System and Statistical Analysis of System Performance", Simulation, October 1989.
10. A. Avizienis, M.R. Lyu, W. Schutz, "In Search of Effective Diversity: A Six-Language Study of Fault-Tolerant Flight Control Software", FTCS-18, 1988.
11. J.C. Knight, N.G. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multversion Programming", IEEE Trans. On Software Engineering, January, 1986.
12. A. Avizienis, "A Design Paradigm for Fault-Tolerant Systems", AIAA Computers in Aerospace Conference, October 1987, Paper 87-2764.
13. J. McWha, "777 Systems Overview", RAeS Presentation, November 1993.
14. Y.C. Yeh, "Triple-Triple Redundant 777 Primary Flight Computer", 1996 IEEE Aerospace Applications Conference, February 1996.
15. Y.C. Yeh, "Dependability of the 777 Primary Flight Control System", DCCA-5, September 1995.
16. J.L. Shaw, H.K. Herzog, K. Okubo, "Digital Autonomous Terminal Access Communication(DATAC)", Seventh AIAA/IEEE Digital Avionics System Conference, November 1986.
17. D.L. Sebring, M.D. McIntyre, "An Air Data Inertial Reference System for Future Commercial Airplane", Ninth AIAA/IEEE Digital Avionics Conference, October 1988.
18. K. Hoyme, K. Driscoll, "SAFEbus", Eleventh AIAA/IEEE Digiatl Avionics Conference, October 1992.