TRIPLE–TRIPLE REDUNDANT 777 PRIMARY FLIGHT COMPUTER

Abstract. For two recent decades the redundancy aspect has become one of the key principles in the architecture for time critical systems. The current paper describes the Triple–Triple Redundant Primary Flight Computer (PFC) engineered for Boeing 777. This critical system could be taken as an outstanding example of the safest critical system ever made. It has been proved by extensive testing and more than ten years of intensive use. Boeing 777 PFC meets the reliability requirements which are even higher than it was maintained for civil aviation.

1. INTRODUCTION

The first Boeing 777 entered service on June, 1995. Since then 777s have flown more than two million flights without any catastrophic malfunctions that may cause humans death. None of 777s crashed yet. Boeing engineers designed and electronically pre-assembled the 777 using computers. New laboratory facilities enabled the various airplane systems to be tested together as a single integrated entity in simulated flight conditions, before the first jetliner took to the air. The 777 underwent the most extensive flight-test program ever conducted on a commercial jetliner. The flight-test program included nine airplanes, which flew more than 7,000 hours and 4,900 flights. Today's 777 operators enjoy a 99 percent dispatch reliability rate – the highest amongst all twin-aisle airplanes in service today. The flight-control system for the 777 airplane is different from those on other Boeing airplane designs. Rather than have the airplane rely on cables to move the ailerons, elevator, and rudder, Boeing designed the 777 with fly-by-wire technology. As a result, the 777 uses wires to carry electrical signals from the pilot control wheel, column, and pedals to a primary flight computer. There are 3 million parts in a 777 provided by more than 900 suppliers from 17 countries around the world. Taking previous statement into consideration it could be said that there is nothing wrong with the details and parts in the other planes as well, the main problem is how the system is designed and put together in order to face the highest reliability.

A. The Boeing 777 Family

The Boeing 777 family consists of six airplanes: five passenger models, with the ability to fly point-to-point nonstop to bypass crowded and busy hub airports, and a freighter model. The less take-offs are done to reach the destination point the less pollution will be discharged to the environment. The 777 Boeing have seats for 301 to 368 passengers in a three-class board configuration. In comparison to the common know Boeing 747 which has 467 passenger seats in the same three-class configuration it provides more space (baggage and seat) per passenger. The flight range capability of Boeing 777 is 5235 nautical miles (9695 km) to 9450 nautical miles (17 500 km), which is much longer than the 747 model allows: 8000 nm (14 815 km). The six airplanes from Boeing 777 family are: the 777-200; 777-200ER (Extended Range); a larger 777-300; two new longer-range models, the 777-300ER and 777-200LR (the world's longest range commercial airplane); and the Boeing 777 Freighter.

The wing span of the 777-200LR is 64,8 meters, the overall length is 63,7 meters. These measures may differ between airplanes in the 777 family. For example, the cruise speed of the Boeing 747 is 0,85 mach at the 10 000 meters which is slightly faster than the airplanes from the 777 family achieve: 0,84 mach, however, the new wing construction and more efficient fuel consumption allows to perform cheaper and longer flights.

B. Primary Flight Controls (PFC – hydraulics, PFC – surfaces)

The 777 FBW computers control electric and electro-hydraulic actuators using electrically transmitted commands. The 777 FBW system provides manual and automatic control of the airplane in the pitch, roll and yaw axes.

Pilot commands are inputted through conventional column, wheel and rudder pedal controls and are electrically transmitted and processed for application to the primary flight control surface. Two elevators and a horizontal stabilizer are used for control in the pitch axis. Roll control is achieved with two ailerons, two flaperons and is augmented with fourteen spoilers. The spoilers also provide speedbrake control. Yaw control is provided with a single, tabbed rudder. The primary flight control surfaces are illustrated in Fig 1. Fig 2 provides information about the way Actuator Control Electronics (ACE) are attached to the control surfaces. Namely, ACE controls hydraulic source that mechanically drives the control surfaces.

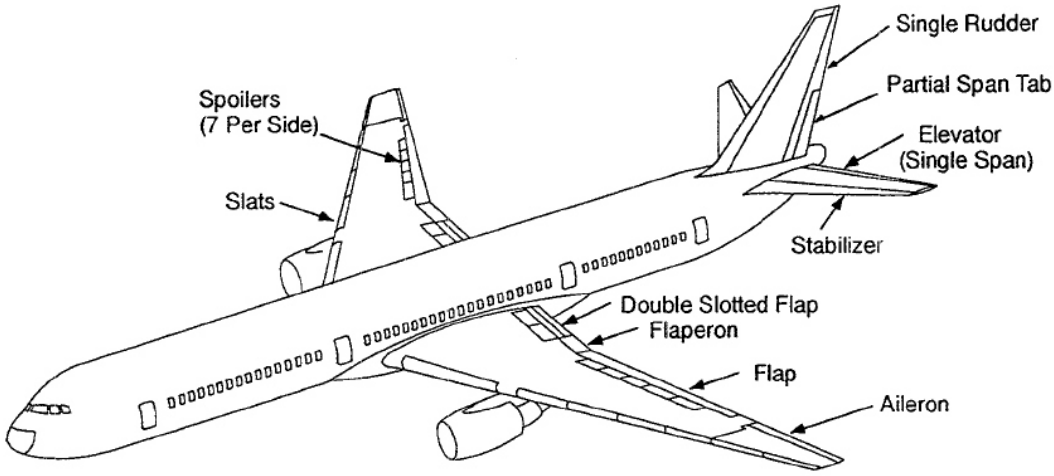

Figure 1. Primary Flight Control Surfaces.

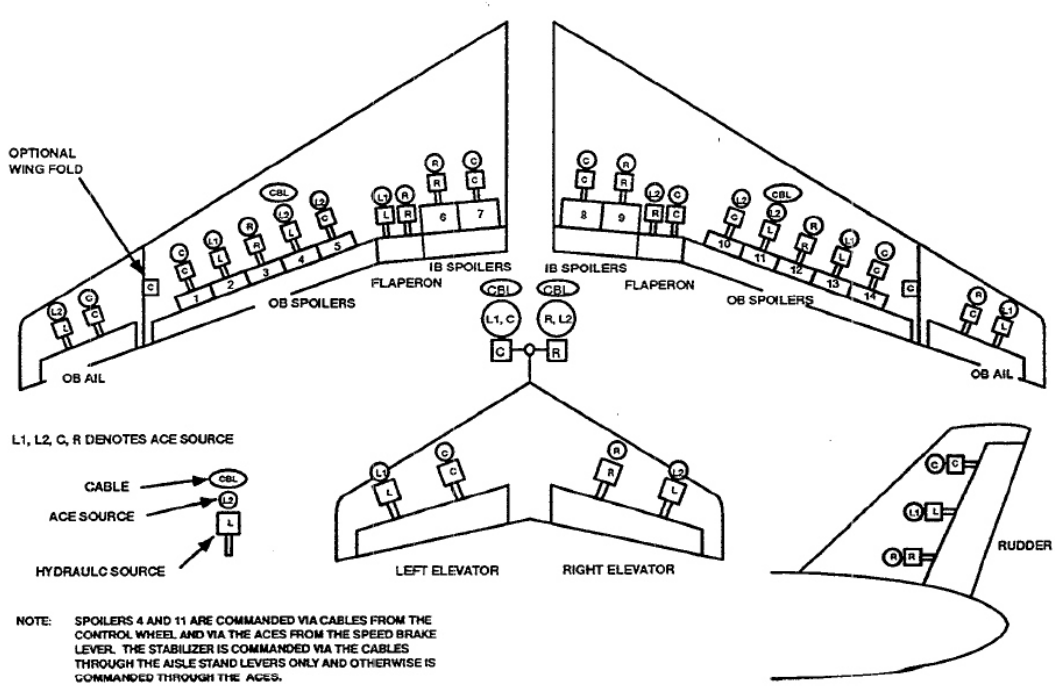

Figure 2. Primary Flight Controls Hydraulic/ACE distribution

2. FLY-BY-WIRE PRINCIPLES

The 777 FBW design philosophy for safety considers the following constraints:

(1) Common Mode/Common Area Faults
(2) Separation of FBW Components
(3) FBW Functional Separation
(4) Dissimilarity
(5) FBW Effect on Structure [1]

Common Mode/Common Area Faults

Airplane should not be susceptible to common mode and common area damage which is gained by designing the systems to both component and functional separation requirements. This includes criteria for providing installations resistant to maintenance crew error or mishandling.

The FBW design and installation has been developed considering the following fault types:

- impact of objects
- electrical faults
- electrical power failure
- electromagnetic environment
- lightning strike
- hydraulic failure
- structural damage. [2]

Separation of FBW Components

The FBW design philosophy focuses on the isolation and separation of redundant flight control elements including different kind of replaceable units, associated wiring and hydraulic lines to the greatest extent possible. In this case the possibility of loss of function minimized due to common-mode or common area faults, and failures of other systems are prevented from affecting the FBW operation as well. General system airplane design decisions target common mode/common area faults considering the following:

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

Functional Separation

Electrical power is allocated to Primary Flight Computer (PFC) and Actuator Control Electronics (ACE) to provide maximum physical and electrical separation between the Left (L), Centre (C) and Right (R) flight control electrical buses. For flight controls ARINC 629 bus [4] is used. The functional allocation of flight allocation bus is aligned with electrical power allocation. Although PFCs and ACEs listen to all three ARINC 629 buses, only the L PFC (L ACE) may transmit onto the L ARINC 629 bus, the C PFC (C ACE) onto the C ARINC 629 bus and the R PFC (RACE) onto the R ARINC 629 bus. This prevents an ARINC 629 transmitter failure or a WC/R electrical power failure from disrupting more than one ARINC 629 bus. [1]

ACE functional actuator control is distributed to maximize controllability in all axes after loss of function of any ACE or supporting subsystem.

The hydraulic systems are also aligned with the actuator functions to provide maximum controllability after loss of hydraulic power in one or two systems.

Dissimilarity

Generic design faults have been studied for various flight critical systems. Design errors can defeat redundancy strategies, and can even result in shutdown of multiple computer channels. Various combinations of dissimilar hardware, different component manufacturers, dissimilar control/monitor functions, different hardware design teams, different software design teams, and different compilers are considered.

FBW Effect on Structure

Failures in the FBW components which can result in oscillatory or handover control surface motion may have an adverse effect on airplane structure. The structural requirements are analyzed and apportioned to all FBW components.

3. TRIPLE–TRIPLE REDUNDANCY OBJECTIVES

In order to meet some demanding performance requirements such as a particular component becoming totally inoperative or a failure which results in some particular faulty component remaining active, providing an error information, a fault-tolerant system generally uses both types of fault tolerance (hardware and software) and has the capability for automatic, dynamic reconfiguration of the system. To deal with it, different levels of redundancy (dual, triple, or quadruple) are used, depending on the level of criticality and, therefore, on the allowable probability of failure. Redundancy extends to all hardware elements, such as processors, sensors actuators, and data buses, and to the software.

The microprocessors are considered to be the most complex hardware devices. The INTEL 80486, Motorola 68040 and AMD 29050 microprocessors were selected for the PFCs. The dissimilar microprocessors lead to dissimilar interface hardware circuitries and dissimilar ADA compilers.[1]

In the 777, for example, there are three PFCs in the Primary Flight Control System, each with three identical computing “lanes” within each PFC. Consequently, this results in nine identical computing channels. Any of the three PFCs themselves can fail totally due to loss of power or some other failure which affects all three computing lanes, but the Primary Flight Control System loses no functionality. All four ACEs will continue to receive all their surface position commands from the remaining PFCs. Likewise, any single computing lane within a PFC can fail, and that PFC itself will continue to operate with no loss of functionality. Because the system is controlled electronically, there is an opportunity to include system control augmentation and envelope protection features that would have been difficult to provide in a conventional mechanical system.

The three computing lanes in each PFC channel, with frame synchronization and data synchronization are proved to produce outputs with tight command tracking. Thus, generic errors in compilers and potential microprocessor hardware interface deficiencies are detected during the development phase.

4. 777 PRIMARY FLIGHT COMPUTER ARCHITECTURE DESIGN

A. Fly-By-Wire components in 777 PFC

Actuator Control Electronics (ACEs)

Four ACEs provide the interface between the FBW analogue domain (crew controllers, electro-hydraulic actuators and electric actuators) and the FBW digital domain (digital data buses, PFCs etc.). The ACEs provide excitation and demodulation of all position transducers and the servo loop closure for all flight control surface PCUs and the variable feel actuators. Each ACE contains three terminals which comply with the ARINC 629 specification to communicate with the data buses. In Direct Mode, the ACEs do not respond to commands on the digital data bus but instead provide simple analogue control laws to command the surface actuators directly [1].

Primary Flight Computers (PFCs)

Three PFCs provide triple redundant computational channels for the primary flight control system. Each PFC receives data from all three flight controls data buses, but transmits only on its associated bus. Each PFC contains three internal computational lanes. Each lane interfaces with all three data buses using dedicated hardware. Each PFC channel contains three dissimilar processor lanes, and software from Ada source code using three different Ada compilers to provide triple dissimilarity. Each PFC lane includes three ARINC 629 terminals and bus couplers to communicate with the data buses. Each PFC lane contains its own microprocessor and power supply, besides that it has own monitor module, command module and standby module to fulfil redundancy objectives.

Each PFC lane operates in two roles: command role or monitor role. Only one lane in each channel is allowed to be in command role. The command lane will send proposed surface commands to its ARINC 629 bus. A command lane will receive the proposed surface commands from two other PFC channels. The hardware device residing in the PFC lane will perform a median select of three inputs of each variable or discrete: two from other channels and one from its own. The output of the median select hardware is sent in the same word string as the “selected” surface commands. The PFC lanes in the monitor role will perform a “selected output” monitoring of their command lane. The PFC command lane, meanwhile, performs the “selected output” monitoring of other two PFC channels. The median value select provides fault blocking against PFC faults until the completion of the fault detection and identification and reconfiguration via the PFC cross-lane monitoring. The PFC command lane will be cross-lane inhibited via the cross-lane inhibit hardware logic.

The PFC channel common-mode fault is detected by the cross channel “selected output” monitoring function. A PFC channel will be cross-channel inhibited via the cross-channel inhibit hardware logic.

ARINC 629 Digital Data Bus

The ARINC 629 data bus [4] 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 with the bus using a coupler and terminal. 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. Data enters through the demodulator and is checked for faults. The receiver circuitry monitors all incoming labels and determines which word strings are needed. The data needed by the attached users is sent to the subsystem interface and to the users.

B. 777 PFC Architecture Design

The 777 program decision to use the ARINC 629 global bus concept and the 777 FBW philosophy for fault isolation mandate the PFC architectural concept of asynchronous PFC channel operation. The PFC safety requirements are described herein, followed by the PFC design features pertinent to deal with the communication asymmetry and the functional asymmetry.

PFC Safety Requirements

Safety requirements apply to PFC failures which could preclude continued safe flight and landing, and include both passive failures (loss of function without significant immediate airplane transient) and active failures (malfunction with significant immediate airplane transient). The numerical probability requirements are both $1x10^{-10}$ per flight hour for functional integrity requirements (relative to active failures affecting 777 airplane structures) and functional availability requirements (relative to passive failures).

(1) The PFC should be designed to comply with the above numerical safety requirements for the 777 Nominal Mission for the following configurations:

A. All PFC system lanes operational,

B. Any single PFC lane inoperative.

(2) The PFC should be designed to comply with the numerical functional availability of $1x10^{-10}$ per autoland operation for the following system configurations:

A. Any single PFC lane inoperative in one, two or all three PFCs.

B. Any one PFC inoperative.

C. Any one PFC inoperative in combination with any single PFC lane inoperative in either or both of the remaining two PFCs.

D. All PFC lanes operational.

(3) The PFC should be designed to comply with the following non-numerical safety requirements:

A. No single fault, including a common-mode hardware fault, regardless of probability of occurrence, should result in an erroneous (assumed active failures for the worst case) transmission of output signals without a failure indication.

B. No single fault, including a common-mode hardware fault, regardless of probability of occurrence, should result in loss of function in more than one PFC.

C. Safety analysis

The target or safety objective was to be able to dispatch the aircraft with one PFC computer failed and still meet the following two objectives:

- Complete loss of control: extremely improbable.
- Any significant reduction of handling quality: remote.

The difficulty in factually demonstrating that a momentary loss of all electrical power is extremely improbable led to the retention of a minimal mechanical backup system. Performed tests demonstrated that it is possible to maintain safe control in any configuration, over the entire flight envelope by using only the rudder for yaw and roll and the trimmable horizontal stabilizer (THS) for pitch control.

The safety analysis was performed to cover all significant failures of FBW system including single failures, latent failures, and failure combinations at the LRU (Line Replaceable Unit) level. It is remarkable that there is a general classification of failures included in the system:

- passive failures (loss of function without significant immediate airplane transient) and
- active failures (malfunction with significant immediate airplane transient).

There is a major constraint that the PFC should have been engineered to comply with the following non-numerical safety requirements:

- No single fault, including a common mode hardware fault, regardless of probability of occurrence, should result in an erroneous (assumed active failures for the worst case) transmission of output signals without failure indication.
- No single fault, including a common mode hardware fault, regardless of probability of occurrence, should result in loss of function in more than one PFC.

And the numerical probability requirements are both $1x10^{-10}$ per flight hour for functional integrity requirements and functional availability requirements.

The analysis and tests have shown that the probability of a given failure condition is consistent with its severity, and that all failure combinations producing a catastrophic consequences are extremely improbable.

D. Testing

Fault Tolerance

Tolerance is the ability of a system to continue satisfactory operation in the presence of one or more non-simultaneously occurring hardware or software faults. "Fault tolerance becomes especially significant when the system performs a flight critical or flight essential as defined by Federal Aviation Regulation (FAR) Part 25.1309: Equipment, Systems and Installation or by MIL-F-9490: Flight Control Systems. In brief, FAR 25.1309 specifies a probability of failure for a flight critical system of < $1x10^{-9}$ per flight hour". [2]

The 777 uses software in lieu of hardware replication to achieve fault tolerance in analytical redundancy. In the case of a faulty sensor, analytical redundancy combines data from the remaining functioning sensors with data from other sources in the aircraft in algorithms that compute the most probable value from the failed sensor. This computed value is then used in the same ways as a value from a functioning sensor. An equivalent concept can be applied to flight control actuators and surfaces where, if an actuator fails or a control surface is lost, the remaining functioning actuators and surfaces can be combined in a way to offset the loss. Analytical redundancy and its companion concept for actuators are two of the corner stones of reconfigurable flight control systems.

The 777 software, working with the operating system, is capable of restarting a given process within a partition based on predefined parameters established for each partition type. Using this technique, it executes the fault recovery approach having the minimum system effect while maximizing the probability of eliminating the fault condition. In the case of frequent transient hardware or software faults or persistent faults, the software is able to shutdown a specific process in a partition, a specific partition, or an entire Core Processing Modules (CPM) as required by the system safety analysis.

What about fault detection? It is obvious that before any fault-tolerance scheme can be invoked, a fault must be detected. There are several approaches to fault detection: replication (triple or higher) and voting duplication and comparison, and self-checking. In replication and voting, a highly fault-tolerant voting circuit compares the values from multiple processors computing the same parameter, and if one of values does not agree with the others, the value is ignored and the processor that generated the suspect value is switched off line. Based on the degree of fault tolerance required in the system, a replacement processor can be brought on line or the system can revert to a lower level of replication or to the duplication and comparison mode of operation. The

failed processor then executes self-diagnostic check and, if no permanent faults are found, returns active status.

All critical interfaces into the 777 FBW Primary Flight Control System use multiple inputs (to be more precise: three input busses), which are compared by a voting plane. By employing methods such as this, it is assured that the 777 Primary Flight Control System is able to withstand a single or multiple failures and be able to contain those failures in such a manner that the system remains.[2]

Flight-critical systems require fault-tolerant software to complement the fault-tolerant hardware. Many of the concepts for fault-tolerant hardware, such as similar and dissimilar redundancy and standby sparing, have parallels in fault tolerant software. Fault-tolerant software falls into three categories: multiversion programming, recovery blocks, and exception handlers. None of these techniques will give the desired results if the software specification is incorrect. The importance of beginning the software design process with an accurate and complete software specification cannot be overemphasized. An error in the software specification will probably produce an error in the software, one that may not be found, even in exhaustive testing, but may later cause catastrophic failure of the system. Multiversion, or N-version, programming requires the development of two or more versions of a program that performs a specific function described in the software specification. These different program versions should be developed by separate software teams and may even be designed to operate on different processors. Finally, the software engineer must decide whether the versions are to be executed in parallel or sequentially. Clearly the trade-off here is between minimum hardware and slower execution (sequentially) or more hardware and maximum (parallel). All techniques that were described above were implemented during the 777 development process.

Each CPM contains two identical processors operating in a redundancy checked pair with each processor monitoring the other processor. Each processor and its associated address, memory and control hardware is referred to as a processing lane. The state of the address, instruction, data and control lines in each lane are compared against each other on every processor clock cycle. This redundant processor operation is referred to as lock step processing. Any divergence between the two processing lanes operating in lock step is detected on the actual clock cycle when the failure occurs. This instantaneous detection of the fault condition allows program execution to be immediately passed to a software fault handler and prevents corrupted information from being executed. Implementation of the lock step architecture has facilitated the design of many additional high integrity monitors to check every aspect about each processor operation. These additional monitors evaluate both software and hardware fault conditions. The lock step architecture and its associated monitors have resulted in a system that will detect virtually all hardware faults, transient or persistent. The probability of an undetected hardware fault 777 CPM lock step processing architecture is $< 1x10^{-9}$ per hour.

Recovery blocks are another concept in fault-tolerant software. Acceptability checks are made on the results from a primary version of a program. If the results fail the acceptability checks, an alternate version of the program that is different from the primary version is invoked, and the process of computation and acceptability checks is repeated. If no alternate version produces an acceptable result, the software block is judged to have failed.

Fault containment and isolation is of little value unless an appropriate recovery response is defined for each type of fault event that can occur.

5. TESTING

In order to provide the required validation test coverage a number of laboratory facilities were used. System Level integration testing was conducted at the 777 Flight controls Test Rig (FCTR), Systems Integration Lab (SIL), and an Engineering Simulator Cab (Cab 2). The FCTR, and the SIL and Cab 2 were primarily use for airplane level validation with some flight controls validation when appropriate. [2]

For requirements compliance testing was also the most desirable method. Analysis is used to validate system performance, reliability, and safety predictions based upon system redundancy. Where review of an installation or document was sufficient, inspection was used as a method. Similarity was also used as a method of validation when the system implementation was identical or comparable to previous system which demonstrated satisfactory performance. But similarity was never the sole method, supported by analyses or tests to show that the previous system meets the current system requirements. Suppliers also performed various tests and analyses to verify that their designs meet requirements. Analyses and tests were also performed for supporting systems outside the responsibility of the Flight Controls Organization.

SUMMARY

Boeing 777 airplane remains one of the most reliable long range airplanes, mostly due to the wisely conducted development process starting from the airplane specification documents and finishing with extensive testing program. Requirements analysis phase estimated reliability bounds that were even higher than used to be. Nevertheless, the triple – triple redundant PFC is main success in Boeing 777, that make this plane look so brilliant from the reliability point of view even nowadays, more than 12 years later when it firstly took to the air.

REFERENCES

1. *Y. C. (Bob) Yeh* “Triple-Triple Redundant 777 Primary Flight Computer”, Aerospace Applications Conference. Proceedings IEEE, 1996

2. *Engin Uzuncaova, Miguel A. Ayala* “Boeing 777 Flight Control System”, SW 4582 Weapons Systems Software Safety Naval Postgraduate School, Monterey CA, 2003

3. *William Sweet and Dave Dooling* “Boeing’s seventh wonder”. – IEEE Spectrum, 2004

4. *Y. C. (Bob) Yeh* “Safety Critical Avionics For The 777 Primary Flight Controls System”. Digital Avionics Systems, DASC. The 20th Conference, 2001

5. *Michael J. Morgan* ‘’Avionics Handbook’’. Chapter–29 Boeing B-777, 2000

Anton Tõertov
Tallinna Tehnikaülikool
Infotehnoloogia teaduskond