Challenges in Building Fault -Tolerant Flight Control System for a Civil Aircraft

M. Sghairi, A. de Bonneval, Y. Crouzet, J.-J. Aubert and P. Brot

***Abstract*— The civil aircraft's electrical flight control system has been changed to take benefit of technical improvements. New technologies, when mature, can be incorporated in aircrafts. Evolutions are considered towards a digital network between computers and actuators/sensors, and more distributed processing for actuators and sensors. Thus, new architectures are possible for future aircraft systems. The difficulty is to achieve the same safety and availability requirements with additional operational reliability (required by airlines). The challenge that faces the engineers is to design mass-produced fault-tolerant systems with reasonable cost. Analysis of existing electrical flight control system architectures of the Airbus and Boeing airplanes as well as future requirements drive us to introduce a brief overview for an incremental methodology of architectural design process based on progressive requirements injection.**

***Index Terms*— dependability, fault-tolerance, safety analysis, critical avionics systems, digital electrical flight control systems**

I. Introduction

Fig. 1 shows a commercial transport aircraft's Flight Control System (FCS). It is an electrical system with digital technologies: Fly-By-Wire (FBW) since the Airbus A310. In general, pilot commands are sensed electrically and processed by digital computers to position the control surfaces. The components of FCS include sensors, actuators (hydraulic and electric), flight control surfaces, the respective cockpit controls, connecting linkages, the necessary operating mechanisms, and digital flight control computers (central processing units) as the system's core.

The flight control system provides airplane control and envelope protection in pitch, roll, and yaw axes. All system processing on FCS is performed by flight control computers because computers are the only components of the system which have functions implemented in software (intelligent components). Traditionally, digital signals are used for inter communication between Flight Control Computers (FCC), while analog signals are used for communication between FCC and sensors/actuators. During the last few years there has been a considerable amount of effort undertaken in the area of integrated modular avionic (IMA) [1], and digital communication based on AFDX [2] switch in order to minimize aircraft cabling to provide further weight, cost reduction, and high operational reliability.

The primary concern of our project is to develop a new low-cost architecture for future aircraft flight control systems based on digital communication technologies. The commercial transport industry can benefit from Fly-By-Wire technologies. Unfortunately, the equipments and architectures proposed for FBW applications must meet stringent safety and availability requirements [3] for being certified. For such applications, the probability of losing aircraft's function or a critical failure must be less than 10^{-9} per flight hour.

The paper is organized as follows: Section I presents flight control systems. Section II and III provide the fundamental concepts and definition of dependability. Sections IV and V describe basic architecture of Airbus and Boeing fault tolerance flight computer. Section VI is dedicated for system's safety and economic requirements. Section VII presents a brief overview for the incremental methodology process to define primary optimal architecture. While section VIII presents conclusions and perspectives of this work.

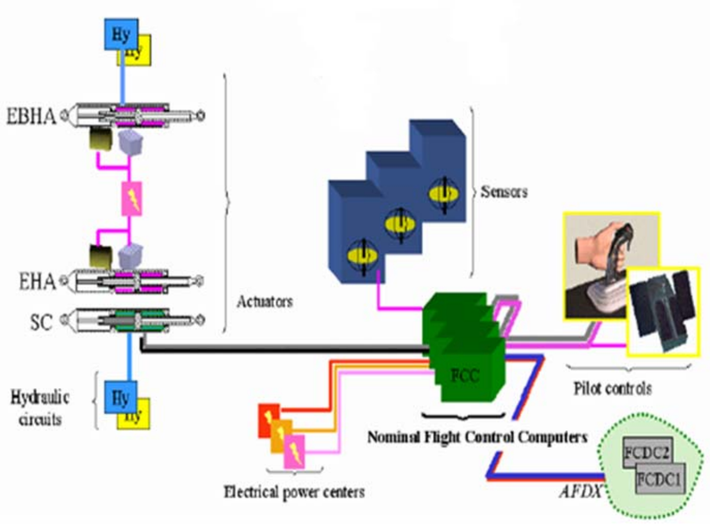

Fig 1: Flight control system's elements.

M. Sghairi is with LAAS-CNRS, Université de Toulouse, 7, avenue du Colonel Roche, F-31077 Toulouse, France. She is also with AIRBUS France, Flight Control System Department, 316 route de Bayonne, 31060 Toulouse, France (e-mail: msghairi@laas.fr or sghairi@airbus.com).

A. de Bonneval is with LAAS-CNRS, Université de Toulouse, 7, avenue du Colonel Roche, F-31077 Toulouse, France. He is also with Université de Toulouse, Université P. Sabatier, 118, Route de Narbonne, F-31062 Toulouse, France (e-mail: agnan@laas.fr).

Y. Crouzet is with LAAS-CNRS, Université de Toulouse, 7, avenue du Colonel Roche, F-31077 Toulouse, France (e-mail: crouzet@laas.fr).

J.-J. Aubert and P. Brot are with AIRBUS France, Flight Control System Department, 316 route de Bayonne, 31060 Toulouse, France (e-mail: aubert@airbus.com and brot@airbus.com).

(Advance online publication: 20 November 2008)

II. Dependability of Flight Control System

Flight control system is complex and too critical to be susceptible to failure. In fact, only ideal systems can be perfectly reliable and never fail. Unfortunately, this is impossible to be achieved in practice, because there are many reasons for system's failure (i.e. design error, physical error…). System's dependability analysis is a very important phase in any architectural validation process of flight control system. Dependability is the system's property that allows reliance to be placed justifiably on the service it delivers. Dependability is characterized by six fundamental attributes: Availability (readiness of correct service); reliability (continuity of correct service); safety (absence of catastrophic consequences on the user(s) and the environment); integrity (absence of improper system state alterations); maintainability (ability to undergo repairs and modifications); and security.

In the literature there are many techniques to attain dependability. For example, fault prevision and fault tolerance. Fault tolerance techniques are massively used to tolerate faults (hardware or software) in flight control systems.

Fault-tolerance is the system's ability to maintain its functionality, even in the presence of faults. It has been extensively studied in the literature: [4] and [5] gives an exhaustive list of the basic concepts and terminology on fault-tolerance. A fail-safe technique is applied to the system's design to enhance the system's robustness and to allow it to continue functioning in the presence of faults.

The fail-safe design concept and techniques are used to ensure that, if any single element in a system or sub-system fails in any flight, such failure should not prevent the continuity of safe flight and landing, or significantly reduce the capabilities of the airplane. Thus, the application of the fail-safe design concept enables minimal occurrence and/or effects of failures, and provides protection against catastrophic failure conditions.

In this paper we are only interested in fault tolerance techniques [6] used for flight control systems to tolerate hardware and software faults. Both Airbus and Boeing use fault tolerance techniques to confine design fault .The principal techniques used are redundancy, diversity, and segregation.

III. Fault Tolerance Techniques on FCS

A. Redundancy

Redundancy consists of hardware components' physical replication such as replicated computers. Thus, redundancy is a fundamental prerequisite for a system that either recovers from or hides failures [7]. Redundancy can be provided in two different ways called static or dynamic redundancy.

In static redundancy, the idea is to use three or more modules which have the same input signals while they are all active. Their outputs are connected to a voter that compares these signals. The correct signals are then chosen by majority voting. The faulty module can be masked by 2-out-of-3 voting.

Dynamic redundancy uses less number of modules on the expense of more information processing. A minimal configuration uses 2 modules. One module is usually in operation and if it fails the standby or backup unit takes over. This requires a fault detection unit to detect the faulty situations. Simple fault detection modules use the output signal for consistency checking, comparison with redundant modules, and information redundancy in computers like parity checking or watchdog timers.

The task of the reconfiguration module is to switch to the standby module from the faulty one after the fault is detected. As in its hardware counterpart redundancy methods, software redundancy methods are used.

B. Diversity

Diversity is software redundancy where different software implementations are proposed to ensure the independence of common development errors of the redundant components. Design diversity is a defense against "common mode" or "common cause" development errors in safety critical systems [8]. It is a system design concept that attempts to reduce the possibility of failure stemming from a common development error in one functional failure path; this can result in another functional failure path. This is accomplished by designing a functional failure path to be sufficiently different to minimize the likelihood that the error will manifest itself in another component. Faults can be generated, but successfully masked and ignored within the system.

The two major forms of software redundancy on flight control system are N Self-Checking Programming and N-version programming.

N Self-Checking Programming:

A self- checking program results from adding redundancy to a program so that it can check its own dynamic behaviour during execution. A self-checking software component consists of either a variant and an acceptance test or two variants and comparison algorithm.

N-version Programming:

In an N-version software system [9], each module is made with up to N different implementations. Each variant accomplishes the same task, but hopefully in a different way. Each version then submits its answer to voter or decider which determines the correct answer. An important distinction in N-version software is the fact that the system could include multiple types of hardware using multiple versions of software. The goal is to increase the diversity in order to avoid common mode failures.

Design diversity in a very expensive approach, as the same software has to be developed several times, by several teams Flight control system requires fault tolerance software (diversity) to complete fault tolerance hardware.

Both redundancy and diversity increase hardware costs, weight, and power requirements for all redundant components.

C. Segregation

This concept is based on isolation and separation of redundant architecture's elements. This redundant system separation requires multiple hydraulic system lines and components, communication buses, signal paths, and electrical components. These redundant components have to be distributed in different locations. For example, actuators are managed by any of the flight control computers, to protect against failure of single calculator that causes loss of control in any axis (roll, pitch or yaw).

The linkages between the flight control computers and the flight surfaces are arranged so that each surface is controlled by multiple independent actuators. Each actuator is controlled by different computers so loss of a single actuator or computer will not lead to a loss of the surface's control. Another form of segregation is the hydraulic system which is 3-way replicated through different dedicated paths.

IV. Industrial Practices and Strategies

A. *Airbus Basic Internal Architecture Computer*

The airbus flight control system is based on many self checking flight computers composed of two software variants or unit (command and monitoring unit) [10] as show in Fig. 2 whose results are compared. The command unit and the monitor unit are separated channels within a single computer. Each channel has separate hardware and different software. If the results of the channels disagree (as checked by the comparator) or are not produced at the same time then an error is assumed and control switches to another computer. The software for the different channels in each computer has been developed by different teams using different programming languages. There are two kinds of computers: primary computer (for complex processing) and secondary computer.

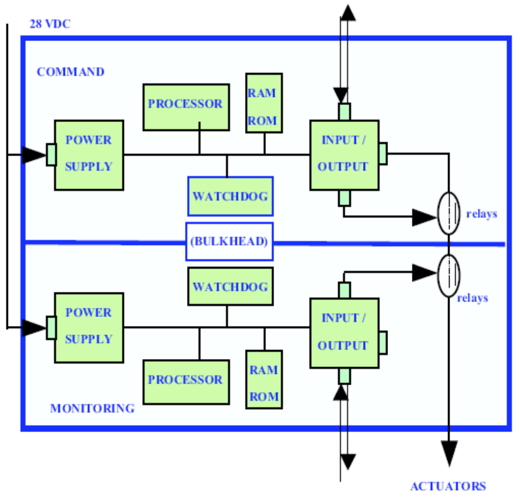

Fig. 2: Airbus basic computer global architecture.

B. *Boeing Basic Internal Architecture Computer*

Flight control computer comprise three Primary Flight Computer (PFCs), each of identical design and construction. Each PFC (Primary Flight Control) is identified as a channel and is composed of three dissimilar computing lanes [11] as depicted in Fig 3.

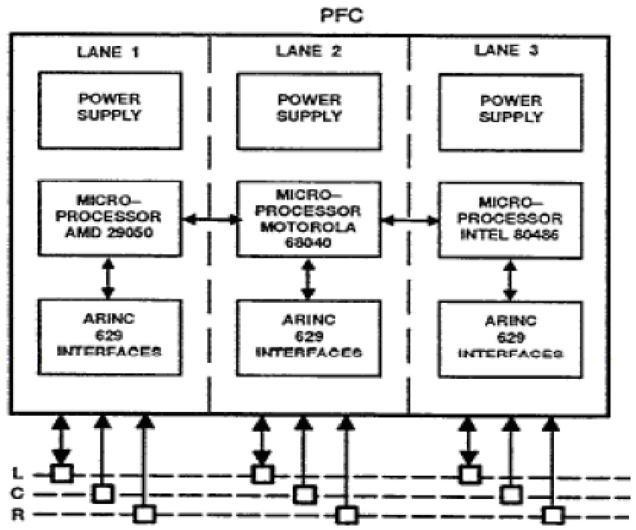

Fig 3: Boeing basic computer global architecture.

Primary flight control system's lines have the same input signals and are all active. Their outputs are connected to a voter that compares these signals. The correct signals are then chosen by majority voting. The faulty module can be masked by 2-out-of-3 voting.

V. System Architecture and Redundancy

Flight control system requires fault tolerance software (diversity) to complete fault tolerance hardware.

The analysis of Airbus and Being FCS shows that the design and implementation of such a safe system of operation through the combined use of redundancy and diversification to minimize the probability of failure common mode between units and redundant to make independent software design faults can be optimized by proper adjustments of the redundancy. It also shows that a level of redundancy is very important. This "over-redundancy" is justified by the desire for a demonstration of safety, which is guided by both regulations and certification. However, given the high level of redundancy practiced, it seems interesting to try to propose alternative architectures on less hardware and software resources. To conduct this exercise, we first have to identify and formalize the requirements to be met by the flight control systems.

VI. Flight Control Systems Requirements

Architectures proposed for critical systems must meet stringent safety and availability requirements to achieve certification [12]. For flight control systems, the probability of loss of aircraft function or critical failure must be less than 10^{-9} per flight hour. This is normally achieved through the use of redundant architectures. In addition to the primary redundancy required to meet the safety requirements, manufacturers have also stipulated the inclusion of additional redundancy or second redundancy in key system to meet additional economic requirement.

A. Safety and Civil Aviation Regulation

Fail safe design concept is required by civil aviation regulation. The system has to meet the FAR/JAR 25 (Joint Aviation Authority/ Federal Aviation Regulations) large airplanes requirements for certification [13]: the examination of a planned or existing system to demonstrate its level of safety in order to be accepted by the authorities or the public. This is to show that the system is robust against any considerable failure (or combination of failures) [14]. The Flight control system usually has two types of Safety requirements:

Integrity: the system must not output erroneous signal. Especially computers should not send wrong information to the actuators.

Availability: the system must have a high level of availability. If the failure of any FCS component results in the unavailability of a service, this component is called a single point of failure for the system.

One of the most important problems in implementing fault tolerant systems is the identification of single points of failure in SSA (System Safety Assessments) and elimination of these single points of failure by using replaceable units.

B. Economic Requirements

1) Operational reliability

To assure a high operational reliability, FCS is a grouping of subsystems having sufficient redundancy of software and hardware components that a failure will not disrupt the availability of system's services. The availability objective of flight control system is to be able to dispatch the aircraft with one or more computer failure, so aircraft may take off with one defective piece of equipment ("MEL dispatch") (Master Equipments List). The number of successive flights under such conditions is limited.

The airplane will have a large operational availability and relatively few maintenance hours.

To enable airlines to organize easy maintenance for their fleet, it is required that the FCS is still usable with the expected level of safety, even if an equipment failure could not be repaired until several days (returning for maintenance). Again, without that requirement, a plane out of its maintenance base with an equipment failure could be banned from flying in anticipation for its equipment replacement, taking into account this requirement to increase redundancy.

2) Radiation environment in atmosphere

Electromagnetic Radiation: In designing the flight control system, the electromagnetic radiation should also be considered. The radiation must not affect communication between the control tower and the aircraft, or data communication associated with the Fly-By-Wire system. Particularly, the system must be especially protected against over voltages and under voltages, electromagnetic aggressions, and indirect effects of lightning.

3) Manufacturing error

The choice of technological components, and process development strategies [15] (quality control, the rules for equipment design) are important factors to control reliability. Despite of the precautions taken, it may happen that a decline in production quality and that this would be detected only after the commissioning of several defective components (less reliable). Thanks for the inclusion of additional redundancy, FCS provides sufficient margins allowing, for example, to avoid design and manufacturing error [16]. Beyond the requirements of Safety, manufacturers now typically take extra precautions, either to take account of experience in service, either as flat for cases of risk not seen in service, but we still want to cover this risk.

VII. Overview of The Incremental Methodology

Nowadays, the requirements for a safe flight control design are met through high redundancy in hardware and software [17]-[18]. The question we are trying to solve is: what level of redundancy has to be achieved?

The prime focus of our project is to develop a new low-cost safety architecture with the least redundancy. To achieve our goal, we decided to use an incidental methodology with iterative requirements injection.

Flight control system is a complex system; there are several subsystems (computer, sensor, actuators...) with functional and structural dependency. Each subsystem has timing and dependability requirements with different levels of criticality. For these reasons a structured approach is necessary to build a new architecture. This section introduces an incremental modeling approach with an illustrating example.

Indeed, it is difficult to get an overview of all the assumptions that characterize the behavior of a complex system's components and their interactions. Hence, it is more natural to proceed in a gradual manner by building and validating the architecture in stages: this is the objective of our incremental approach. Starting with a basic block "simplex unit" and then taking into account each requirement which results in duplication of hardware and software. This approach allows us to analyze the real needs and justify each additional cost hardware or software. Therefore, we propose a conceptual process which takes into account the different requirements in incremental manner.

Steps in the incremental methodology process:

Step 1: identification of all subsystems' boundaries, and requirements. At the beginning, we propose to define all of the system's principal subsystems without looking for their dependency;

Step 2: definition of safety objectives per subsystem. Safety objective is the probability of system's failure due to a subsystem's failure;

Step 3: defining or choosing basic architecture to meet functionality. Necessary functional capabilities must be realized. A single component should be sufficient;

Step 4: defining requirements for all subsystems;

Step 5: injecting the first requirement;

Step 6: assessment of quantitative reliability;

Step 7: preliminary calculation evaluation: quick evaluation of probability's objective with simple formula (we can use assumptions);

Step 8: iteration over all requirements;

Step 9: iteration over all sub-functions.

This approach is a part of a complete safety process methodology that allows us to define a new safe architecture for a complex real time safety-critical system. At the current stage we don't introduce a real time requirement.

VIII. Conclusions

To meet extreme high safety requirements (of 10^{-9} per flight hour) as well as economic requirements, multiple redundant hardware and software resources are required for flight control systems. Unfortunately, redundancy increases hardware costs, weight, and power requirements. In the economy and business world, consumers usually choose to purchase the cheapest product that meets their needs. Presumably, one of the watchwords that will guide the design of future aircraft generation will be "eco-efficiency". In this context, the FCS must offer a service that consumes less resources.

References

[1] Paul J. Prisazunk Integrated Modukar Avionics Airlines Eletronic Engineering Committee CH3258 -3/92/0000 -0039 1992 IEEE

[2] Brajou, F.; Ricco, P.;The Airbus A380 - an AFDX-based flight test computer concept AUTOTESTCON –IEEE 2004, pages 460-465

[3] Traverse P., Lacaze I., Souyris J., « Airbus Fly-by-Wire: A Total Approach to Dependability », Proceedings 18th IFIP World Computer Congress, Building the Information Society, Toulouse, France, 22-27 août 2004, pp. 191-212.

[4] Arlat J., Blanquart J.-P., Boyer T., Crouzet Y., Durand M.-H., Fabre J.-C., Founau M., Kaaniche M., Kanoun K., Le Meur P., Mazet C., Powell D., Scheerens F., Thevenod-Fosse P., Waeselynck H., Composants logiciels et sûreté de fonctionnement - Intégration de COTS, Hermès Science Publications, Paris, 2000, 158 p.

[5] Laprie J.-C., Arlat J., Blanquart J.-P., Costes A., Crouzet Y., Deswarte Y., Fabre J.-C., Guillermain H., Kaâniche M., Kanoun K., Mazet C., Powell D., Rabéjac C., Thévenod P., Guide de la sûreté de fonctionnement, Toulouse, Cépaduès-Éditions, 1995-96, 369 p.

[6] D. Brière, and P. Traverse, Airbus A320/A330/A340 electrical flight controls – a family of fault-tolerant systems, Proc. 23rd IEEE Int. Symp. On Fault-Tolerant Computing (FTCS-23), Toulouse, France, pp. 616-623 (1993).

[7] DO178B/ED12, Software Considerations in Airborne Systems and Equipment Certification, published by ARINC, no. DO178B, and EUROCAE, no. ED12, 1992.

[8] C. Favre, Fly-by-wire for commercial aircraft: the Airbus experience, International Journal of Control, vol. 59, No. 1, pp.139-157 (1994).

[9] Avizienis A., « The N-Version Approach to Fault-Tolerant Software », IEEE Transactions on Software Engineering, vol. SE-I 1, no. 12, December 1985, pp. 1491-1501

[10] ARP 4754/ED79, Certification Considerations for Highly-Integrated or Complex Systems, published by SAE, no. ARP4754, and EUROCAE, no. ED79 (1996).

[11] Yeh Y.C., « Triple-Triple Redundant 777 Primary Flight Computers », Proceedings IEEE Aerospace Applications Conference, Aspen, CO, USA, 3-10 février 1996, pp. 293-307.

[12] Riter, « Modeling and Testing a Critical Fault-Tolerant Multi-Process System », Proceedings 25th International Symposium on Fault-Tolerant Computing (FTCS-25), Pasadena, CA, USA, 27-30 juin 1995, pp. 516-521

[13] FAR/JAR 25, Airworthiness Standards: Transport Category Airplane, published by FAA,title 14, part 25, and Certification Specifications for Large Aeroplanes,

[14] FAA (Federal Aviation Administration), System Safety Handbook, chapitre 3:Principles of System Safety, 30 décembre 2000, 19 p.

[15] DO254/ED80, Design Assurance Guidance for Airborne Electronic Hardware, published by ARINC, no. DO254, and EUROCAE, no. ED80 (2000).

[16] SAE (Society of Automotive Engineers), Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Document No. ARP 4671, décembre 1996.

[17] EASA (former JAA), CS-25.5. A. Avizienis, J.C. Laprie, and B. Randell, Fundamental Concepts of Dependability,LAAS report no. 01-145 (2001).

[18] Yeh Y.C., « Safety Critical Avionics for the 777 Primary Flight Controls System », Proceedings 20th Conference on Digital Avionics Systems, Daytona Beach, FL, USA, 14-18 octobre 2001, pp. 1C2/1.1C2/11.