DISTRIBUTED AND RECONFIGURABLE ARCHITECTURE FOR FLIGHT CONTROL SYSTEM

Manel Sghairi, Jean-Jacques Aubert, Patrice Brot; Flight Control System Department AIRBUS France
316 route de Bayonne, 31060 Toulouse, France
Agnan de Bonneval, Yves Crouzet, Youssef Laarouchi; CNRS; LAAS; Université de Toulouse; UPS, INSA, INP, ISA; F-31077 Toulouse, France

Abstract

New airplanes must meet rigorous requirements of aviation safety, operational reliability, high performance and energy efficiency at a low cost. To meet this challenge, we should optimize current system and take advantage of available technology for the next decade.

This work is aiming at proposing some evolutions for Flight Control System (FCS) and to build alternative FCS low-cost and safe architectures for the next decade with less hardware and software resources.

The main contribution of this paper is twofold. First, we will provide an incremental methodology to give guidelines for architecture optimization. Second, we will present a full distributed reconfigurable architecture for FCS based on smart actuators and digital communication network where all system functions are distributed to simplex Flight Control Computer (FCC) nodes and remote actuator electronics nodes (FCRM). Communication between FCC and FCRM will be based on Airbus embedded communication network (ADCN, Advanced Data Communication Network) [1] and a 1553 bus. We will use ALTARICA language to perform dependability evaluation at architectural level in order to check the effects and benefits of the new architecture on the dependability of FCS.

Introduction

Airplane performance and business pressures related to cost have been the main drivers to change flight control system from mechanical to digital Fly-By-Wire (FBW) design [2]. Technical improvements considered for the future, such as smart actuators/sensors with remote electronics and digital communication, will change drastically avionics architectures design for future commercial and military programs [3,4]. A FBW control system has several advantages over a mechanical system but equipments and architectures proposed for FBW critical systems such as FCS must meet stringent safety and availability requirements before they can be certified. For FCS, the probability of losing an aircraft critical function or of an occurrence of a critical failure must be less than 10^{-9} per flight hour.

Traditionally [5], FCS has used a centralized /federated architecture where a specific fault tolerant computer has performed all processing and authority. This architecture is inherently robust, because it is based on a high level of software and hardware redundancy. However, it can be very costly in terms of space, weight and power, and also wiring requirements between the elements of the system especially for large airplane. This also increases all continuous monitoring of "non-intelligent" components like actuators and sensors that the computers are performing at the present.

Given the high level of redundancy practiced, it seems interesting to try to propose alternative architectures with less hardware and software resources and to take advantage of technical improvements.

In this context, there is a great motivation for future programs to change current flight control architectures to more distributed and better optimized architectures as shown in Figure 1.

FCS architectures will be based on digital technologies and intelligent subsystems and offer many improvements on centralized architectures. They can help to reduce redundancy and the complexity of principal computing elements in FCS through the migration of some functions out of the FCC and the integration of smart subsystems.

978-1-4244-4078-8/09/$25.00 ©2009 IEEE.

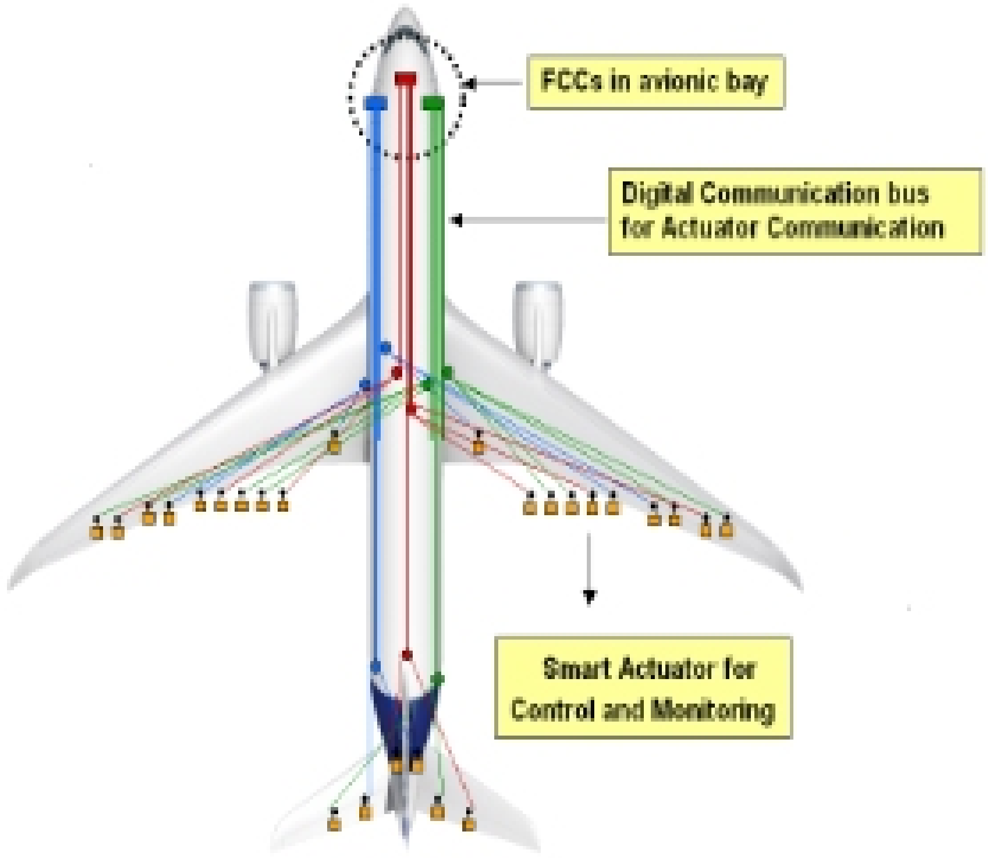

Figure 1. Full Distributed FCS Architecture

In this paper we propose a conceptual fully decentralized and reconfigurable architecture for FCS with architecture optimization and control distribution, where it is possible to use systems resources and new technologies better.

FCS is a very critical system and consequently must be carefully designed and exhaustively checked. We validate the proposed architecture through simulation using ALTARICA language (a high level formal description language) and SDT (System Design Tool) for system safety and reliability assessments.

The paper is organized as follows. This first section has presented flight control systems evolutions. The second section analyzes the state of the art of current FCS architectures. The third section gives an overview of an incremental methodology for architecture optimization. The fourth and fifth sections describe and analyze massive voting architecture, and illustrate the use of ALTARICA for dependability evaluation.

State Of The Art Of Current FCS And Their Requirements

Traditionally, FCSs have used a centralized and federate architecture where a specific computer has performed all processing and authority. In the context of our work we have analyzed a set of FCS architectures. The first subsection presents the Airbus and Boeing design. The second subsection presents a short analysis of redundancy, and the last subsection presents the system requirements identified.

Airbus And Boeing Design

The Airbus flight control system is based on many self-checking flight control computers [6]. Each FCC is composed of two software variants or units (command and monitoring unit) [7] 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 don't correspond (as checked by a comparing function) or are not produced at the same time then an error is assumed and system control switches to another computer. Computers communicate with each other through point-to-point digital communication in order to manage FCS redundancy taking into account different failure cases.

The Boeing PFCS (Primary Flight Control System) [8] comprises three Primary Flight Computers (PFCs), each of identical design and construction and four analog computers ACE (Actuator Control Electronic).

The PFCs compute control-surface position commands and transmit position commands to ACE via ARINC buses. The ACEs position the control surfaces using actuator systems. The ACE units act as an intermediate stage between the PFC and the pilot and actuators. Each PFC is identified as a channel and is composed of three dissimilar computing lanes [9]. Primary flight control system lines have all the same input signals and are all active. Their outputs are connected to a voter that compares these signals. Majority voting then chooses the correct signals. 2-out-of-3 voting can mask the faulty module. Each actuator is controlled by a single ACE and each ACE can receive orders from all PFCs.

All Flight Computers in Airbus and Boeing design are installed in the avionics bay and are connected directly by individual wires to all relevant sensors/actuators through point-to-point links. The relations between flight computer and actuators are arranged so that different computers control each actuator with priority order, so loss of a single computer will not mean loss of control of that surface.

System Analysis

The analysis of current flight control architectures shows that the design and implementation of such a safe system are realized through the combined use of redundancy and diversity (software redundancy) to minimize the probability of common mode failure between redundant units. It also shows that level of redundancy is very important.

This "over-redundancy" is justified by the need for a demonstration of safety and operational reliability especially for commercial airplane, which is guided by regulation authority and economic pressure.

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 classify all requirements to be met by flight control system architecture.

System Requirements

Safety And Civil Aviation Regulations

Fail-safe design concepts [10] are required by civil aviation regulations. The system has to meet the FAR/JAR 25 (Joint Aviation Authority/Federal Aviation Regulations) requirements for certification [11, 12]. It means that for a planned or existing system it must imperatively be possible to demonstrate its level of safety in order to be accepted by the authorities. This is to show that the system is robust against any considerable failure or combination of failures [13, 14].

The flight control system usually has two types of dependability requirements:

- Integrity: the system must not output erroneous signals. In particular, Flight Computer should not send incorrect information to the actuators.
- Availability: the system must have a high level of availability.

Economic Requirements

Operational reliability is very important for airlines to stay competitive. FCS must have sufficient redundancy of software and hardware components so that a failure will not disrupt the availability of the system services. The availability objective of flight control systems is to be able to dispatch the aircraft with one or more components failure, so aircraft may take off with one defective equipment. 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 be still usable with the expected level of safety, even if an equipment failure could not be repaired for several days (ie. before returning for maintenance). The number of successive flights under such conditions is limited.

Radiation Environment

Electromagnetic radiation should also be considered. The radiation must not affect 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.

Manufacturing Faults

The choice of technological components and process development strategies [15] (quality control, rules for equipment design) are important factors to control reliability. Despite the precautions taken, a decline in production quality may occur in several defective components (less reliable). Thanks to the inclusion of additional redundancy, FCS provides sufficient margins to tolerate this kind of fault [16].

Incremental Methodology

Analysis of existing FCS architectures, and their requirements, lead us to introduce a brief overview of an incremental methodology to build a new architecture based on progressive requirements injection and distribution of the function of the system [17]. The question we are trying to solve is: what level of redundancy has to be achieved?

Flight control systems are complex. There are several subsystems (flight control computer nodes, actuator nodes, communication network,) with functional and structural dependency. Each subsystem has different timing and dependability requirements with different levels of criticality. For these reasons, a structured approach is necessary for architecture optimization. It is more natural to proceed in a gradual manner by building and validating the architecture step by step, this is the objective of the incremental methodology: starting