APPROACHES TO ASSURE SAFETY IN FLY-BY-WIRE SYSTEMS: AIRBUS VS. BOEING

Andrew J. Kornecki, Kimberley Hall
Embry Riddle Aeronautical University
Daytona Beach, FL
USA
<kornecka@erau.edu>

ABSTRACT
Fly-by-wire (FBW) is a flight control system using computers and relatively light electrical wires to replace conventional direct mechanical linkage between a pilot's cockpit controls and moving surfaces. FBW systems have been in use in guided missiles and subsequently in military aircraft. The delay in commercial aircraft implementation was due to the time required to develop appropriate failure survival technologies providing an adequate level of safety, reliability and availability. Software generation contributes significantly to the total engineering development cost of the high integrity digital FBW systems. Issues related to software and redundancy techniques are discussed. The leading commercial aircraft manufacturers, such as Airbus and Boeing, exploit FBW controls in their civil airliners. The paper presents their approach, the difference of control philosophy, and the implementation resulting in a comparable level of safety assurance essential for airline operations.

KEY WORDS
Avionics, Software Engineering, Software Safety, Fault Tolerance

1. Introduction

A fly-by-wire (FBW) system is a computer-based flight control system that replaces the mechanical link between the pilot's cockpit controls and the moving surfaces by much lighter electrical wires. Pilots maneuver their aircraft by controlling the moveable parts, known as flight control surfaces, on the aircraft's wings and tail planes. The computers convert the pilot's commands into electrical impulses delivered to the control surfaces. Airbus and Boeing use slightly different ways of taking advantage of FBW in their commercial aircraft.

The objective of this paper is to compare the different approaches used by commercial aircraft manufacturers in implementing their FBW systems. The paper attempts to the systems usability and safety from the perspective of the system and software engineering design decisions. The aircraft manufacturers examined for this paper are Airbus Industries and The Boeing Company. The entire Airbus production line starting with A320 and the Boeing 777 utilize fly-by-wire technology.

The first section of the paper presents an overview of FBW technology highlighting the issues associated with its use. The second and third sections address the approaches used by Airbus and Boeing, respectively. In each section, the nature of the FBW implementation and the human-computer interaction issues that result from these implementations for specific aircraft are addressed. Specific examples of software-related safety features, such as flight envelope limits, are discussed. The final section compares the approaches and general conclusions regarding the use of FBW technology.

2. Fly-By-Wire Technology

The concepts behind FBW systems are not new; all guided missiles use this type of control. In its analog implementation, FBW has been in use in military aircraft since the first test on a modified F-8 Crusader in 1972. The delay in commercial aircraft implementation was due to the time required for the development of economically viable failure survival technologies and providing assurance that the overall system integrity will be as high as the mechanical control system it replaces.

The FBW system allows manufacturers to save weight and reduce fuel consumption, due to the elimination of the bulk and mechanical complexity of the linkages connecting the pilot's stick/yoke to the control surfaces. It also allows them to exploit multiple aircraft configurations increasing aerodynamic efficiency (more lift, low drag) and providing better overall performance. However, this may result in a reduced natural stability, with the aircraft becoming unstable over part of the range of speed and altitude conditions (the flight envelope). FBW systems overcome this by providing high-integrity automatic stabilization of the aircraft to compensate for the loss of natural stability. All these factors provide the pilot with good control and handling characteristics over

the whole flight envelope and under all loading conditions.

2.1 FBW System Basics

Figure 1 demonstrates the basic elements of a FBW flight control system characterized by:

- total elimination of all mechanical controls and linkages; all commands and signals are transmitted electrically along wires,
- placement of a computer between the pilot's commands and the control surface actuators,
- use of aircraft motion sensors which feedback the components of the aircraft's angular and linear motion to the computer, and
- use of air data sensors supplying altitude and airspeed information to the computer,

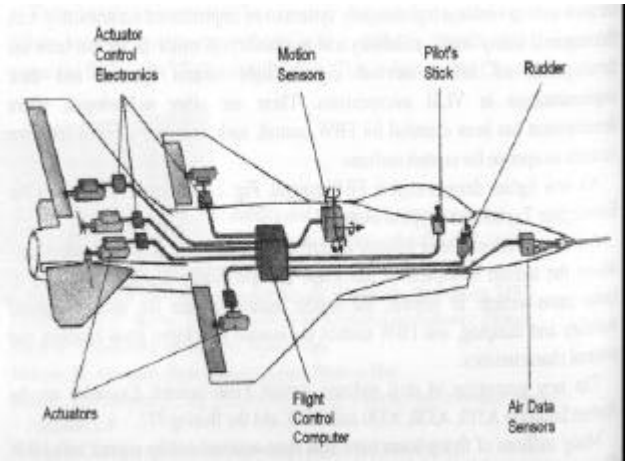

Figure 1. Basic Elements of a FBW System

Not shown, but certainly critical, is the incorporated redundancy of all components and connections to assure that the system can survive the failures.

Data transmission. Electrical transmission of signals and commands is a key element in a FBW system. Modern systems use a serial digital data transmission scheme with time division multiplexing. The signals are transmitted along twisted pair of wires (only one set of data is being transmitted at any particular time). The most popular standards are military MilStd 1553, ARINC 429 used by Airbus, and ARINC 629 used in Boeing 777.

Control surface actuation. The actuation systems controlling the movements of the control surfaces must be able to survive any two failures. The FBW two-stage servo actuators drive the duplex control valves of the main power control actuators. Both electro-hydraulic and electrical first stage actuation systems are used, however the trend is now towards direct drive electrical motors. First stage multiple totally independent electrical actuators drive the power control unit (PCU) servo control valve. For the lack of mechanical feedback, the FBW systems electrically feedback the position of the control surface to the actuator control electronics, using four independent position sensors. This technique improves the speed of response of the actuation system essential to minimize the lags that are a part of the FBW loop.

Motion sensor feedback. A FBW system has to have motion sensor feedback by definition. These motion sensors are made up of rate gyros and linear accelerometers.

Air data. The FBW system is supplied with airspeed, altitude, and Mach number to adjust or scale the control surface deflections. Again, redundant data sources are used. The FBW system also requires information on the aircraft angles in the pitch and yaw planes between the airstream and fuselage datum as a control term in the pitch and rudder control system.

Computing system. In order to meet flight safety requirements, the flight control computing system must be of very high integrity and have failure survival capabilities. The tasks carried out by the system in this capacity are: failure detection, fault isolation and system reconfiguration in the event of a failure, computation of the required control surface angles, monitoring, and built-in test.

2.2 Safety & Integrity in FBW Systems

The FBW system must be no less safe than the mechanical control systems, which it replaces. It is specified [1] that the probability of a catastrophic failure in the system must not exceed $1x10^{-7}$/hour for a military aircraft or $1x10^{-9}$/hour for a civil aircraft. The statistical level of civil aircraft safety, derived from the total number of civil aircraft crashes occurring in a year from all causes divided by the total number of aircraft flying and their annual operating hours, corresponds to $1x10^{-6}$/hour. The mean time between failures (MTBF) of a single channel FBW system is about 3,000 hours. The system must therefore incorporate redundancy with multiple parallel channels so that it is able to survive at least two failures. Assuming sufficient redundancy, it may be acceptable to fly with one failed channel. An MTBF that is too low may seriously impact the availability.

Redundant configurations. The assumption is made that the probability of three or four channels failing at the same time is negligible leading to redundancy solutions.

A *quadruplex* system is composed of four totally independent channels of sensors and computers in a parallel arrangement to give the required failure survival capability. They are configured that the system of interconnected sensors, computers and actuators can survive any two failures from whatever cause. The incorporation of a monitoring system to check the correct functioning of a channel by an acceptance tests allows the system to identify the failed channel. This is the base of

an alternative failure survival configuration known as *monitored triplex* composed of three independent parallel channels. Each channel is monitored by a dissimilar system to detect a failure. If this monitoring has a high degree of integrity and confidence level, this configuration can survive two failures.

Figure 2 shows the two configurations. The monitored triplex has less hardware and so may cost less, however the confidence level is higher for failure survival in a quadruplex configuration, particularly when it incorporates self-monitoring.

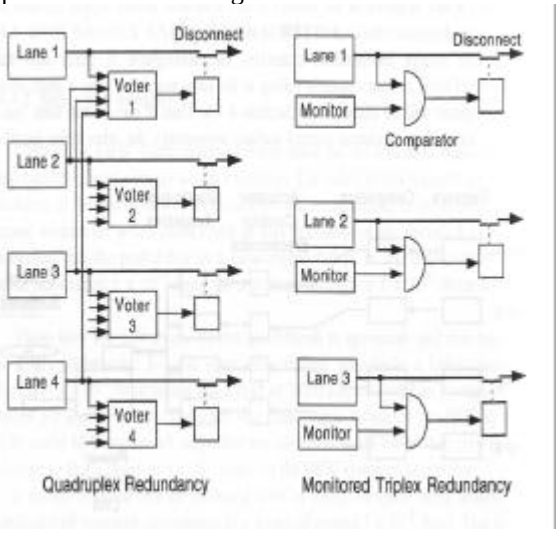

Figure 2. Redundancy configurations

Dissimilar redundancy. The basis for fault detection and isolation relies on the probability of a single event causing all the parallel channels to fail simultaneously as being negligibly small. There are certain types of failures that can affect all systems at the same time. These are known as "common mode failures" [1]. Examples of these are: lightning strike, electro-magnetic interference. fire/explosion, incorrect maintenance, common design errors (e.g. software).

Dissimilar redundancy is used to counteract the problem of eliminating the possibility of a common mode failure. Dissimilar redundancy may take one or more of the following forms:

- Use of two or more different microprocessor types with dissimilar software.
- Use of a back-up analog system in addition to the main digital system, at triple or quadruple level of redundancy.
- Use of a back-up system with different sensors, computing and control means.

Digital technology implementation. The use of digital technology creates certain advantages as compared to analog implementations. These include:

- Hardware economy: one computer can control all three axes of control, whereas an analog system requires dedicated hardware for each axis of control. More complex systems are therefore more economical to implement digitally.
- Flexibility: control laws and gearings can be changed by software changes as opposed to hardware modifications giving greater flexibility in the design and development phases.
- Reduced nuisance disconnects: digital computations allow more sophisticated voting and consolidation algorithms to minimize potential disconnects.
- Smaller failure transients: sophisticated consolidation algorithms can be implemented to minimize the transients experienced on disconnecting a failed channel.

However, it also has certain disadvantages arising from the need to sample data and the frequency at which the data is sampled. These disadvantages include aliasing, data staleness (overcome by synchronization) and latency.

2.3 Software Issues

Software generation for high integrity digital FBW systems can account for between 60% and 70% of the total engineering development cost of the complete FBW system. It is due to the size of the software required to carry out the flight control functions and the problems associated with establishing the safety of the software. The functions carried out by the software may be divided into three basic areas: control laws, built-in-test, and redundancy management. Flight control laws, representing the functional aspect of the system, account for 25% to 30%, while the built-in-test accounts for around 10% of the total software. Thus over 60% the code account for configuration and redundancy management [1]. Some of these tasks involved in failure detection and isolation, and reconfiguration in the event of a failure include: sensor data validation, failure detection and consolidation, sensor failure isolation and system reconfiguration, cross lane data transfer, computer output voting and consolidation, iteration period synchronization, recording of fault data, system status and control.

Programming languages have been a major issue in flight control systems – from assembly language, Jovial, FORTRAN, and Ada to growing reliance on C/C++. Recently, the industry considers modern tools with automatic code generation capability. The modern tools like SCADE, BEACON, Simulink with Real-Time Workshop, or Sildex provide automatic code generation capability and allow developers to shift the focus on the architectural design and system engineering. Regardless whether is it manual coding or tool usage, a rigorous adherence to the software aspects of certification as verbalized by DO-178B must be followed.

Due to the difficulty of proving the integrity of a system using common software in its parallel redundant

channels/lanes to the safety levels required by the regulatory authorities, dissimilar redundancy has become necessary. Two or more independent flight control computing systems are installed using different types of microprocessors and software written in different languages by different development teams. Despite the stringent procedures and methods used to produce this software, the degree of independence between the dissimilar versions is not always 100% due to common requirements. Part of the problem exists in the requirements ambiguity and unforeseen problems in interpretations. The rigorousness and degree of control of the software development process is also a factor. The use of formal methods to define system requirements is also seen as a means of further improving confidence in the software.

3. Airbus Approach

3.1 FBW Implementation

In the A320 (Figure 3) the five dissimilar computers are running four dissimilar software packages. They are two elevator and aileron computers and three spoiler and elevator computers. In the A330/A340 there are five computers to command flight controls: three flight control primary computers (FCPC) and two flight control secondary computers (FCSC). In addition, two redundant flight control data concentrators (FCDC) manage the warning, maintenance and recording data [2].

Each computer is partitioned into two different and independent channels. A failure is detected by comparing control/monitoring channel commands to predefined thresholds, and the channel is subsequently disconnected. Latent failures are detected during daily power up and peripheral tests. The computers can operate without ventilation and are protected against electromagnetic impulses and indirect effects of lightning. Five flight control computers are active simultaneously in charge of control law computation and individual actuator control. The system incorporates redundancy to provide nominal performance and safety levels, making it possible to fly aircraft safely with only one active computer [3].

Computer architecture is designed for failure detection thus redundancy is essential at all levels. In A330/A340 three hydraulic circuits can be pressurized by three sources: engine driven pump, an electric pump, and a ram air turbine. In the case of a double hydraulic failure, the high-level control law is still available. Redundancy in computer to actuator path is assured due to use of four computers. Two or four engine-driven generators (depending on aircraft type) provide redundancy in electrical generation and power distribution. Two batteries provide backup power.

All Airbus airliners utilize dissimilar redundancy in their FBW flight control systems to control the flight control surfaces [1]:

- The FCPC uses three independent monitored computing lanes. An entirely independent processor made by a different manufacturer with software generated by a different development team monitors each primary processor.
- The FCPC controls the spoilers, ailerons, elevators, rudder and horizontal stabilizers.
- The FCSC is composed of two independent monitored computers that control a second set of control surfaces comprising spoilers, standby ailerons, standby elevators and rudder.
- There is a backup mechanical link to control the horizontal stabilizer trim and the rudder.

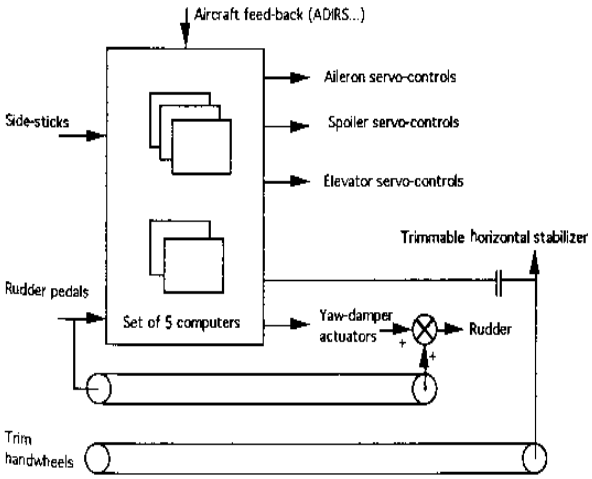

Figure 3. Airbus FBW system architecture

3.2 Human-Computer Interaction

Airbus aircraft utilize a maneuver demand approach, i.e. pilots command the maneuver they want the aircraft to perform. The design of the Airbus flight control systems takes advantage of the potential of FBW to incorporate control laws providing extensive stability augmentation and flight envelope limiting. The positioning of the control surfaces is no longer a simple reflection of the pilot's control inputs and, conversely, the natural aerodynamic characteristics of the aircraft are not fed back directly to the pilot [4].

The major factor in human-computer interaction in FBW systems is the implementation of "flight envelope protection". Airbus implements this protection according to the philosophy of "hard limits". This means that even if pilots want to exceed these limits, such as the maximum bank angle, the system will not allow them to do so [5]. Known as "alpha protection" [6], the software is designed to guard against stalling the airplane is one of the crown jewels of the Airbus flight control system. There have also been accidents and incidents related to these

transitions, which are not commanded by the crew, and the resulting changes in flight logic behavior. For example, and "un-commanded" mode transition during a simulated engine failure on take-off contributed to the fatal crash of an A330 in Toulouse, France in 1994. During takeoff, the aircraft automatically transitioned to an automated mode. Due to the limitations of this mode, the aircraft lost speed and stalled before the crew could disengage the automation and take manual control. The dynamic conditions of the situation were beyond the control logic of the flight mode. Airbus has since change the mode logic to address this.

Other automated mode accidents and incidents have been related to crew confusion with regard to the automated mode. In two cases (Moscow, 1991 and Nagoya, Japan, 1994), an automated mode commanded nose-up pitch while the pilot commanded nose-down pitch during an autopilot-coupled go-around. The crew attempted to reacquire the glide slope by commanding nose down elevator, which conflicted with the automated mode's logic and pitch up commands. In addition, the automated stabilizer system had trimmed the aircraft to maximum nose-up, following its go-around logic. The situation was recoverable, but the crew, interacting with the automation, put the aircraft in an unrecoverable position. An underlying issue relates to the mechanism enabling a pilot to disengage the automated mode and regain manual control. The autopilot was designed to disengage by an alternate mode when in go-around below a specific altitude; the crew may have believed the autopilot was disengaged when in fact the automation was still operating. Ultimately, the automated flight mode dominated and the aircraft pitched up, stalled and crashed.

4. Boeing Approach

4.1 FBW Implementation

There are two flight control systems onboard the B777, both FBW. Figure 4 shows the primary flight control system (PFCS), which controls the elevators, rudder, ailerons, flaperons and horizontal stabilizers. The secondary system controls the flaps and slats [7].

The Boeing 777 airliner makes extensive use of dissimilar redundancy. The pilot's commands are transmitted directly to the four Actuator Control Electronics (ACE) units and are then routed to the redundant ARINC 629 data buses. At the heart of the system there are three identical Primary Flight Computers (PFC). Each PFC forms a channel so that the three separate PFC provide three independent control paths in the primary flight control system [8].

Internally, each PFC is composed of three independent dissimilar processors physically segregated within the box. Independent developer teams generated the software using different compilers for the three processors from the same requirement specification. The system normally operates with one processor in each PFC in command with the other two processors acting as monitors. The PFC is able to absorb multiple random component failures or a combination of a software generic error and random failures. In the event of the PFCS becoming totally inoperable, a reversionary analog command path is available directly to the ACE to provide aircraft control. There is also an independent mechanical link provided to the stabilizer trim system and a pair of flight spoilers.

B777 flight deck control column, yoke and rudder pedals each have appropriately redundant sensors to provide positional data to the FBW system via ACE. The three PFC are active at all times computing and comparing the required surface position for the rudder, flaperons, spoilers, horizontal stabilizer, trim and control column feel system. Each PFC transmits to only one, and different, data bus to protect against common mode failures. Computed surface position demands then output to the ARINC 629 bus and broadcast to the ACE, where they are decoded and turned into actuator demands.

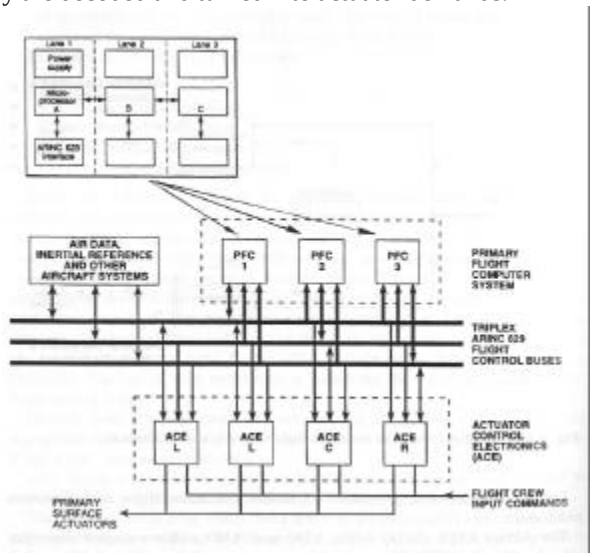

Figure 4. Boeing 777 FBW system architecture

In the very unlikely event that all PFC were inoperative, the flight can be continued by the use of the direct electrical link between the inceptor and ACE, with the redundancy of ACE functions further protecting this feature. During manual control, the commands come directly from the control columns with the addition of stability augmentation terms. Under automatic control, inputs to the FBW system come from the triplex autopilot and the control column follows these commands, thus providing direct crew feedback.

The FBW system uses three modes of operation. Normal mode provides augmentations such as stall and bank angle protection. In secondary mode augmentation is lost. The direct mode is the most degraded mode of operation and would only be activated in the most improbable event of

serious malfunction. In addition, the primary flight control system also supports maintenance functions, which interface with the onboard maintenance system. These include fault reporting, line replaceable unit (LRU) replacement and system checks, rigging and alignment checks, and pre-flight checks.

4.2. Human-Computer Interaction

The Boeing 777 utilizes a lateral control system, where the pilot commands operation via the yoke and the aircraft adjusts the flight control surfaces independently. One of the design goals of the 777 was that operation and response of the airplane should be familiar to the pilots, based on their past experience and training [9]. Other goals related to this were that the control functions shall only assist the pilot – the pilot shall retain ultimate control authority of the aircraft. Traditional tactile, aural and visual cues, using yoke controls, are provided to assist the operation of the autopilot and auto-throttle systems.

The issue of flight envelope protection in the B777 is one of "soft limits". The system provides crew awareness of envelope margins while not reducing pilot control authority. In this case, the aircraft can be stalled and it can exceed its maximum bank angle. The intention is to reduce the possibility of inadvertently exceeding the aircraft's flight envelope. These functions are: stall protection, overspeed protection, and bank angle protection.

5. Conclusion

The use of redundant architectures is common to both approaches. The five redundant systems of Airbus and the triple-triple redundancy of Boeing both achieve the goal of the system being able to survive at least two failures. Both have simple, reliable alternate control paths and employ dissimilar redundancy in their architectures.

Automated controls are highly regarded. However, some pilots believe that the lack of back-driving and cross-coupling of some control loops removes a feedback that crew uses to maintain situation awareness. In addition, some implementations of automated control have "smoothed the boundaries," effectively removing the feel that pilots use. Flight envelope protection is the primary difference between the two systems as it pertains to pilot interaction with the aircraft. As the velocity changes, the Boeing system requires the pilot to re-trim the aircraft to the new speed while Airbus aircraft provides this functionality and does not allow changes [5]. Boeing allows control functions to assist the pilot in avoiding or recovering from situations where the aircraft exceeds its operational boundaries. Airbus aircraft, using "hard-limit" FBW approach, provides this service automatically to the pilot. In short, Boeing provides "soft-limit" flight envelope protection where Airbus provides flight envelope limiting.

Aircraft with FBW flight control systems have accumulated millions of flight hours establishing the claim of the safety and integrity. The two views of the system, a design and maintenance standpoint and a usage standpoint, demonstrate that the argument of an implementation being "better" than other is a matter of preference and often, opinion. The preferences are often described in terms of the level of control that pilot can exercise over the aircraft. Both presented approaches achieve the same goal: a reliable, efficient, and most importantly, safe flight control system. Years of successful operation by Airbus and Boeing aircraft have supported the opinion that two very different FBW philosophies can result in a comparable level of safety assurance essential for airline operations.

References:

[1] R.P.G.Collinson, *Introduction to Avionics Systems* (Boston; London: Kluwer Academic, 2003).

[2] Understanding Airbus fly-by-wire technology, *Aircraft Technology Engineering and Maintenance*, no.36, Oct-Nov 1998, pp. 18-20, 22, 24

[3] N.Storey, *Safety Critical Computer Systems* (Addison Wesley Longman 1996)

[4] M.B. Tischler (editor), *Advances in Aircraft Flight Control* (London: Taylor & Francis, 1996)

[5] M.Mulder, A.Veldhuijzen, R. van Paassen, and S. Bennani, Fly-by-wire Control and Tunnel in the Sky Displays: Towards a Task-Oriented Control/Display System. *Proceedings of AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2002, AIAA 2002-4928

[6] Software Changes Being Made to Help Prevent Landing Mishaps, *Air Safety Week*, June 18, 2001

[7] B777 fly-by-wire, *Aircraft Technology Engineering and Maintenance*, no.42, Oct-Nov 1999, pp. 18-22

[8] K.Sabbagh, *21st Century Jet: The Making and Marketing of the Boeing 777* (New York, NY: Scribner, 1996)

[9] J.McWha, Development of the 777 Flight Control System, *Proceedings of AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2003, AIAA 2003-5767