SCALABLE COMPUTING: PRACTICE AND EXPERIENCE
Volume 9, Number 1, pp. 77–82. http://www.scpe.org
ISSN 1895-1767

AIRBORNE SOFTWARE: COMMUNICATION AND CERTIFICATION

ANDREW J. KORNECKI*

Abstract. This paper discusses the distributed nature of airborne software intensive systems. The concept of fly-by-wire, the issues of safety, component communication, and certification are on the forefront of modern airborne applications. Since the communication between variety of on-board systems and subsystems is of paramount importance, the paper discusses the properties of new bus standard based on the Ethernet protocol gaining recognition and widespread use in large commercial aircraft. Avionics Full Duplex Switched Ethernet (AFDX) addresses quality of service, determinism, and reliability required in an aircraft environment. AFDX has reduced the cost of aircraft data networks, increased network capability, and supported determinism required by the airborne system certification guidelines system.

Key words. avionic bus architecture, airborne software certification, software safety

1. Introduction. When the Wright brothers took the first flight in December 1903, the flying controls were moved by mechanical strings. With progress of aeronautical technologies, the flight-control surfaces have been moved by hydraulic devices fed by hydraulic lines that run through the airplane. A fly-by-wire (FBW) system is a computer-based flight control system that eliminates the mechanical and hydraulic links between the cockpit controls and the airplane moving surfaces. Pulleys, cranks, wires and hydraulic pipes are replaced by much lighter electrical wires. The Lunar Module in 1969 was the first flying machine to use FBW concept. This concept was subsequently applied on the F9 Crusader in 1972 and then successfully implemented in all military aircraft. Obviously, FBW requires communication between distributed aircraft subsystem and components. We discuss the distributed nature of airborne systems, the issues of safety, recent directions in bus communication between airborne subsystems, and certification.

2. Fly-By-Wire. Fly-by-wire defines not only an electrically-signaled control system. Today, FBW identifies computer-configured controls with a computer system processing the pilot's inputs in accordance with software programs and producing outputs controlling the aircraft control surfaces or engine. Computers allows for fast processing compensating for the lack of natural aerodynamic stability e.g. in modern military aircraft. The FBW systems save weight and thus 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 facilitates multiple aircraft configurations increasing aerodynamic efficiency and providing better performance. However, this may result in the aircraft becoming unstable over part of the range of speed and altitude conditions. FBW systems overcome this by including high-integrity automatic stabilization of the aircraft to compensate for the loss of natural stability and provide the pilot with good control and handling characteristics.

Since commercial introduction of fly-by-wire systems by Airbus 320 and then Boeing 777, demand on data transmission between avionics subsystems has increased exponentially. Modern aircraft include large number of systems consisting of sensors, transducers, actuators, alerts and warnings, electrical and hydraulic power control, information management system, interfaces and other digital electronics. Direct connections with ground and satellite communication, links to convey weather and traffic data place additional burden on the number of systems in modern aircraft. Reliability and timely delivery of those communications are essential to safety of the aircraft operations.

3. Software Safety Issues. Software for high integrity digital FBW systems can account for between 60% and 70% of the total development cost of the complete FBW system. It is due to the size and complexity of the software required to implement the flight control functions and the problems associated with establishing the safety of the software. The software functions 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.

The FBW system must be no less safe than the mechanical control systems, which it replaces. 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 $1 \times 10^{-6}/hour$. The mean time

*Embry Riddle Aeronautical University, Daytona Beach, FL 32114, USA (kornecka@erau.edu).

between failures (MTBF) of a single channel FBW system is about 3,000 hours. The FBW 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.

FIG. 3.1. *Cockpit view of modern aircraft (B777)*

4. Communication and Bus Standards. Aeronautical Radio, Inc. (ARINC) was chartered to serve as the airline industry's single licensee and coordinator of radio communication outside of the government. ARINC took on responsibility for all ground-based, aeronautical radio stations and for ensuring station compliance with FRC rules and regulations. Currently, ARINC Standards specify the air transport avionics equipment and systems used by more than 10,000 commercial aircraft worldwide [2].

The flight control, navigation, display computers, and any other equipment on board have to communicate with each other. In early systems, a dedicated wire, i. e. point-to-point connection, was required for each separate component that needed to exchange information with any other. For example, three components exchanging data with each other required a total of six data lines. Bus architecture provided a better solution to integrate the various system components. ARINC 429 defines unidirectional communication bus protocol between a transmitter and up to 20 receivers connected by a two-wire data bus. ARINC 429 has been serving aviation very well and it is used in a majority of commercial aircraft designed before mid-80. However, further advancement of computing capabilities and the need for a multi-transmitter protocol with higher transmission rate to accommodate large number of data in triple-redundant Boeing 777 flight control system led to creation of ARINC 629 based on the Digital Autonomous Terminal Access Communication (DATAC) development work of Boeing and NASA [3]. Each transmitting component's data was coded and broadcast in a synchronized order and each computer or component could be programmed to retrieve only the needed information. The increased data rate and ability to connect more terminals were an added value. However, the proprietary nature of the design hindered widespread use of this standard.

5. Ethernet Solution: AFDX. In the early 90's when Airbus began research for the development of the A380 model, extensive time and resources was put towards implementing new technologies that were reliable and safe without imposing production delays and budget overruns. This resulted in the creation of Avionics Full Duplex Switched Ethernet (AFDX) based on the existing Ethernet technology while requiring less wiring, reducing weight, lowering cost, and increasing communication speeds.

The Ethernet IEEE 802.3 standard with abundance of COTS components, maturity, and the standardization would serve reduction of both cost and development time. However, Ethernet cannot provide aircraft data networks with the required by safety/time critical aviation system "guarantee of service" [4]. Although the data rate is higher than established avionics buses, the potential for transmission collision and related need for re-transmission is significant enough to prevent its defined use in an avionics system. Additionally, a collision could cause time delays exceeding defined time constraints and effectively preventing the transmission from ever reaching its destination—thus "leading to non-deterministic behavior" [5].

Avionics Full Duplex Switched Ethernet (AFDX) extensions to the IEEE Standard 802.3 (Ethernet) address quality of service and reliability required in an aircraft environment. AFDX provides much higher data rates than existing avionics. Both Airbus and Boeing are developing currently aircraft that use AFDX. ARINC 664 Part 7 defined AFDX as a standard.

Each system to be connected to the aircraft bus includes a dedicated End System, which is a gateway to connect each avionic system Line Replaceable Unit (LRU) via the AFDX Switch to the network for the purpose of receiving or transmitting. The End System can accommodate multiple subsystem partitions embedded within each avionics system.

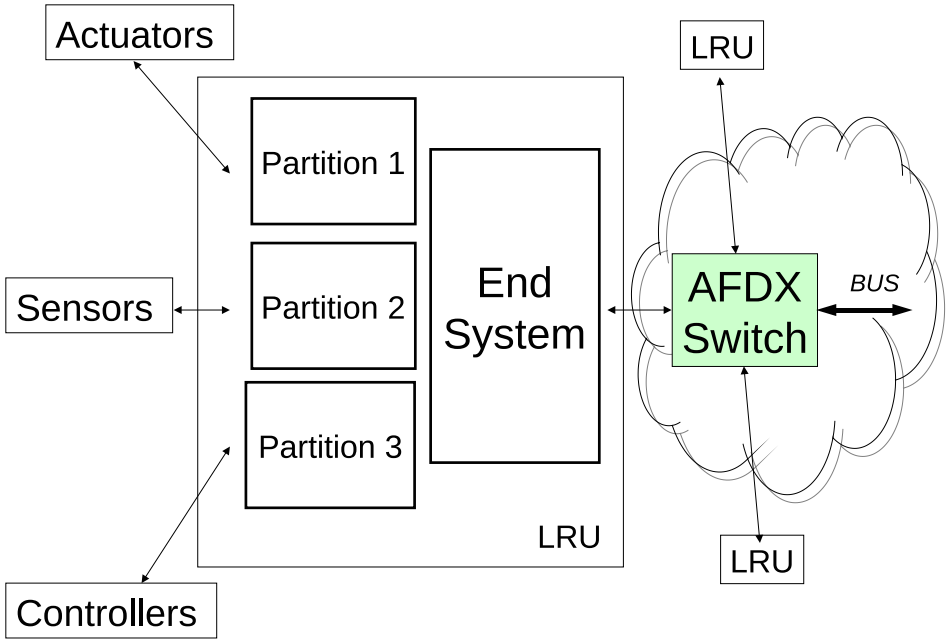

FIG. 5.1. *Avionic Computer System Line Replaceable Unit with three partitions [5]*

To prevent the issues of non-determinism AFDX implements a full-duplex switched Ethernet "... in which the maximum amount of time it would take any one packet to reach its destination is known" [5] thus implementing collision free deterministic system. To achieve this, each subsystem is connected to a switch via two twisted pairs, one dedicated for transmission and one to reception. The AFDX switch implements scheduling protocol controlling the allocation of transmission packets and assuring determinism of the bus operation.

While use of full duplex protocol prevents collisions, it does introduce inaccuracy of packer transmission timing i. e. jitter due to the delay introduced by one packet waiting for another to be transmitted. To maintain system determinism the jitter must be controlled.

AFDX switches play a critical role maintaining and loading configuration tables defining the system and subsystem. Additionally, switches can be cascaded to form larger hierarchical network. The main functions of AFDX switch are:

- Set up a point to point connection network between a sender and one or more receivers
- Establish communication between subscribers on the network
- Monitor and control bandwidth checking and maintaining data frame integrity

Virtual Links (VL) are the channels with unique identifiers which carry messages from source through the switch to the destination. Together with a switch, they effectively create virtual point-to-point network composed of a single source

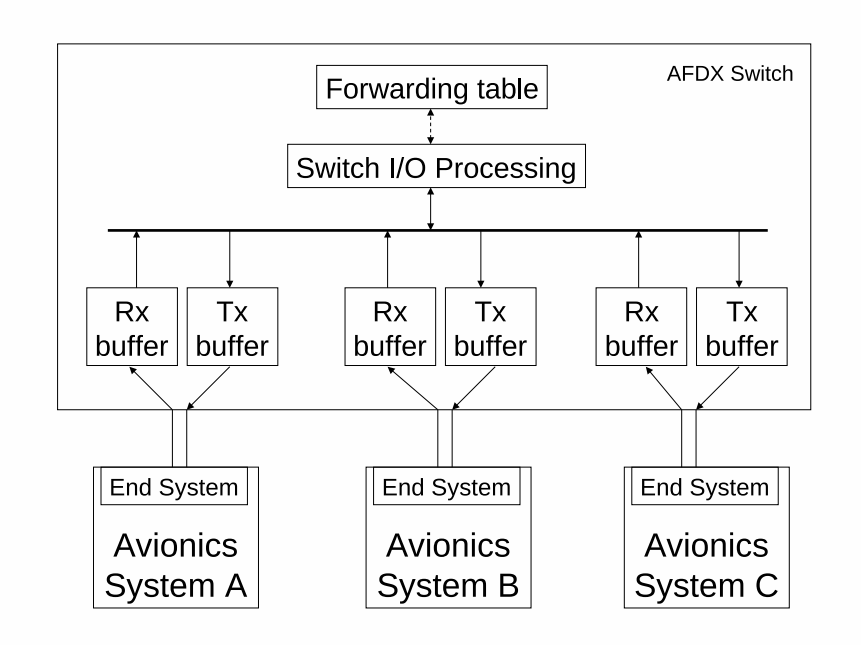

FIG. 5.2. *Full Duplex AFDX Switch Connection with three LRU's [5]*

and delivered to one or more specific receivers. Even though there can only be once source for each VL, it is permissible to originate more than one VL from each source creating a point-to-point connection to one or more destinations. More than one VL can be transmitted at the same time through the physical Ethernet link.

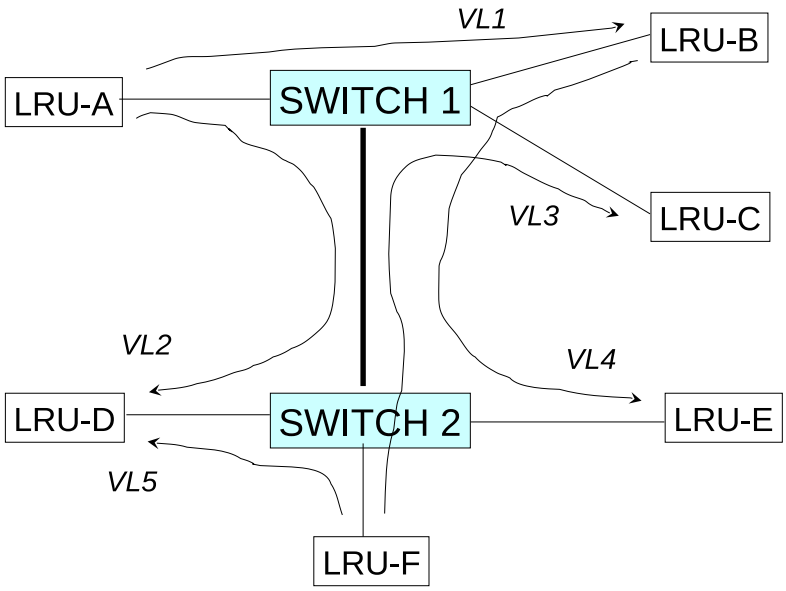

FIG. 5.3. *Virtual Links between six LRU's in a system with two switches*

Each VL has a well defined transmission time, which guarantees [4]:

- Reserved path into the switched network topology
- Reserved bandwidth into the global AFDX network
- Global time scheduling between End Systems

- Known maximum latencies and jitters
- Access delay to the network
- End-to-end delivery, without acknowledgements nor retries

The bandwidth control is achieved by the timing constraints associated to each VL. Every VL is allocated a predefined Bandwidth Allocation Gap (BAG) representing the minimum time interval between the starting bits of two successive AFDX frames (assuming no jitter) and defined in the configuration tables. The BAG values are predetermined for each Virtual Link and the End System allocates the data frames to each BAG to regulate the traffic. The scheduler calculates the maximum jitter for a BAG to accommodate all frames within a given VL. Certainly, to maintain deterministic network, the total bandwidth of all created VL cannot exceed the maximum available bandwidth of the network. When VL is transmitted, AFDX scheduling takes place considering each VL parameters i. e. BAG and the Largest Ethernet Frame. By limiting the rate at which Ethernet frames can be transmitted on a specific VL and by limiting the size of the Ethernet frames, the scheduler can maintain a deterministic network. The scheduler must also coordinate the multiplexing of all transmissions to maintain the total jitter introduced below acceptable levels.

6. Certification. In highly regulated industries such as aerospace, nuclear, medical and transportation it is critical to assure the system safety [6]. In civil aviation industry, a rigorous certification process follows the guidelines of the Radio Telecommunication Committee for Aviation (RTCA) [7]: DO-178B for software and DO254 for hardware. DO-178B was developed by the avionics industry to provide software considerations for aircraft systems including software controlled computing devices. DO-254 provides hardware deployment guidelines for systems including microprocessors, or other complex electronic devices (FPGA, PLA, ASIC, etc.), are deployed in aircraft equipment designs. Both document place significant emphasis on the design/development and verification process to assure product safety and thus constitute guidelines for the design/development assurance. For validation and testing there is an additional need to conform to environmental qualification, as per DO-160D, and need for rigorous and complete testing of variety of failure recovery situations. The system safety considerations, due to lack of well-established metrics, are most difficult to evaluate. Two automotive industry standards [8], SAE ARP 4754 and SAE ARP 4761, give fundamental guidelines to the system safety considerations.

The initial selection of the specific measurable criteria to help in assessment of the data buses is proposed in the CAST paper [9]: safety, data integrity, performance, design/development assurance, and validation/testing approaches. Data integrity and performance can be demonstrated by specific array of tests. In the process, the allowed error rate per byte should be defined and means to recover from the errors should be provided. The load analysis and related bus capacity should be also specified. The extreme cases of bus loss, shortening, and opening should be considered in the analysis and tests. Each specific data bus may have details that need to be addressed by a particular method discussed in advance between the applicant and the appropriate certification authority.

7. Conclusions. Avionics Full-Duplex Switched Ethernet (AFDX) has defined the future of aircraft data networks. Based on a mature technology with extensions to meet fly-by-wire systems' needs, AFDX has reduced the cost of aircraft data networks, increased network capability, and supported determinism required by the airborne system certification guidelines system. AFDX has increased the reliability of avionics systems, while reducing implementation time and cost. The concept and implementation underwent full certification scrutiny and as such has gained stamp of approval for the safety critical applications.

Acknowledgement. The author would like to acknowledge ERAU MSE graduate student Leonard Matos whose term paper was instrumental in collection of the presented material.

REFERENCES

[1] A. J. KORNECKI, K. HALL: *Approaches to Assure Safety in Fly-by-wire Systems: Airbus vs. Boeing,* Proceeding of the Eight IASTED International Conference on Software Engineering and Applications (SEA 2004), ISBN: 0-88986-427-6, MIT, Cambridge, MA, November 2004 http://faculty.erau.edu/korn/papers/SEA04Kornecki_436-021.pdf

[2] *ARINC Aeronautical Radio Inc.,* https://www.arinc.com/cf/store/catalog.cfm?prod_group_id=1&category_group_id=3
[a.] ARINC Specification 629 Part 1–5—Multi-Transmitter Data Bus, Part 1—Technical Description,
[b.] ARINC Specification 664 Part 7, Aircraft Data Network, Avionics Full Duplex Switched Ethernet (AFDX) Network.

[3] D. C. E. HOLMES: *Global System Data Bus Using the Digital Autonomous Terminal Access Communication Protocol,* IEEE/AIAA 7th Digital Avionics Systems Conference and Technical Display, Fort Worth, Texas, 13–16 October 1986, pp. 227–233, 1986.

[4] CREATIVE ELECTRONIC SYSTEMS S. A.: *CES White Paper on ADFX,* 2003, http://www.ces.ch/documents/downloads/afdx_white_paper.pdf

[5] CONDOR ENGINEERING: *ADFX Protocol Tutorial,* Condor Engineering, Inc., 2005, http://www.acalmicrosystems.co.uk/whitepapers/sbs8.pdf

[6] A. J. KORNECKI, J. ZALEWSKI: *Avionics Databus Safety Criteria and Certification,* Proceedings of ESREL'05 Conference, Advances in Safety and Reliability, Gdańsk, Poland, June 2005, ISBN-0415383404, pp. 1149–1155 http://faculty.erau.edu/korn/papers/ZalewskiKorneckA4.pdf

[7] RTCA Radio Telecommunication Committee for Aviation, Inc., http://www.rtca.org/downloads/ListofAvailableDocs_WEB_OCT%202007.htm

[a.] RTCA/DO-178B. Software Considerations in Airborne Systems and Equipment Certification. Washington, DC, 1992.

[b.] RTCA/DO-254. Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC, 2000.

[c.] RTCA/DO-160D, Environmental Conditions and Test Procedures for Airborne Equipment, Washington, DC, 1997.

[8] SAE Society of Automotive Engineers,

[a.] SAE ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, 1996, http://www.sae.org/technical/standards/ARP4754

[b.] SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996, http://www.sae.org/technical/standards/ARP4761

[9] CAST Position Paper CAST-16. Databus Evaluation Criteria, 2003. http://www.faa.gov/certification/aircraft/av-info/software/CAST/cast-16.rtf

Edited by: Marcin Paprzycki
Received: Nov 20, 2007
Accepted: Nov 21, 2007