

Research on Architecture Design and Safety Analysis of Avionics Architecture Databus Network for Commercial Aircraft

Yiqing Quan

Shanghai Aircraft Design and Research Institute, No.5188 Jinke Road, Pudong District, Shanghai, China

quanyiqing@comac.cc

Keywords: ARINC664; AFDX; IMA; Safety; Switch; FTA

Abstract: The commercial aircraft is designed to be larger and lighter for transporting more passengers or cargo. As a result, avionics systems shall be highly integrated and efficient avionics architecture. The author will provide an Integrated Modular Avionics (IMA) architecture with Avionics Full-Duplex Switched Ethernet (AFDX) network for avionics architecture design and propose the means of safety analysis.

1. Introduction

This article is about avionics architecture and databus network, which provide means of communication access between all avionic systems by using standard protocols, which achieves the high level of integration and considerable reduction of equipment and cable weight. The IMA provides a platform of sharing resources, such as electrical powers, processors and I/O interfaces. AFDX is used in this AADN, which features high speed and deterministic data transfer (transmission and reception) between the connected avionic systems by AFDX switches. The architecture design and safety analysis are proposed in detail below.

2. Background

With the rapid development of the aviation technologies, avionics systems are increasingly advanced, which contributes to bringing more convenience to operation of flight crew and providing airlines with more reliable guarantee. However, thousands of hundreds of avionics components are brought into the systems, which lead to more complicated and huger systems and also producing incredibly increasing weight of cables. Obviously, a new generation of avionics architecture shall be developed to integrate the whole avionics system perfectly. In the meanwhile, the certification and safety of systems shall be ensured to meet.

As a result, the Avionics Architecture Databus Network(AADN) with IMA comes into the world, which currently plays a significant role in the avionics system for safe journey. This new avionics architecture provides a real time communication between avionics systems and even can be extended to support other systems, such as fuel system, engine system, etc. Taking advantage of IMA architecture, the avionics systems have higher level of integration and more effective reduction of components and cabling weight. Besides, it is easier for airlines to maintain or update AADN. All these improvements provide better performance and safer flight.

3. Design Methodology

The process of system development must conform to system development life cycle model which is proved. There are various life cycle models of systems development. The V-Model and the Waterfall model have been used widely in aircraft design. Especially, the V-model is actually an improved tool of the Waterfall model. [1] The avionics members have decided to adopt this proved system development life cycle model described by ARP4754 famously used in the field of the

aerospace industry. The procedure followed by the Avionics Team is a V-sharp design life cycle model [2], see Fig.1.

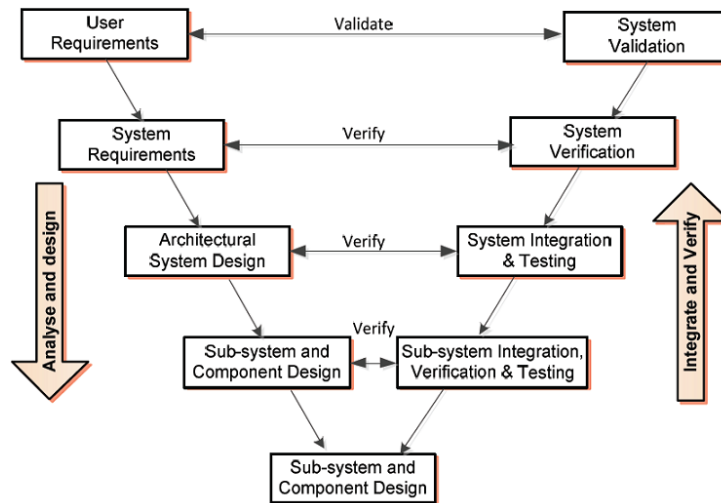


Fig.1 Basic V-Model

4. AADN System Design and Architecture

This chapter aims to demonstrate all the AADN system design and architecture in detail. System interface design will be introduced firstly followed by functional architecture design base on the redundancy design. Then IMA hardware and software design will be shown respectively. Finally, the complete AADN network architecture is achieved and PSSA is carried out in the next chapter to show the reasonability and reliability of avionics architecture.

4.1 System Interface Design

The author assumes that there are 13 subsystems in the avionics systems. The primary task of Avionics Architecture Data bus Network (AADN) System is to integrate all the 13 subsystems into one network, which contributes to reliable data communicating among avionics systems according. Fig.2 shows the System Interface Design.

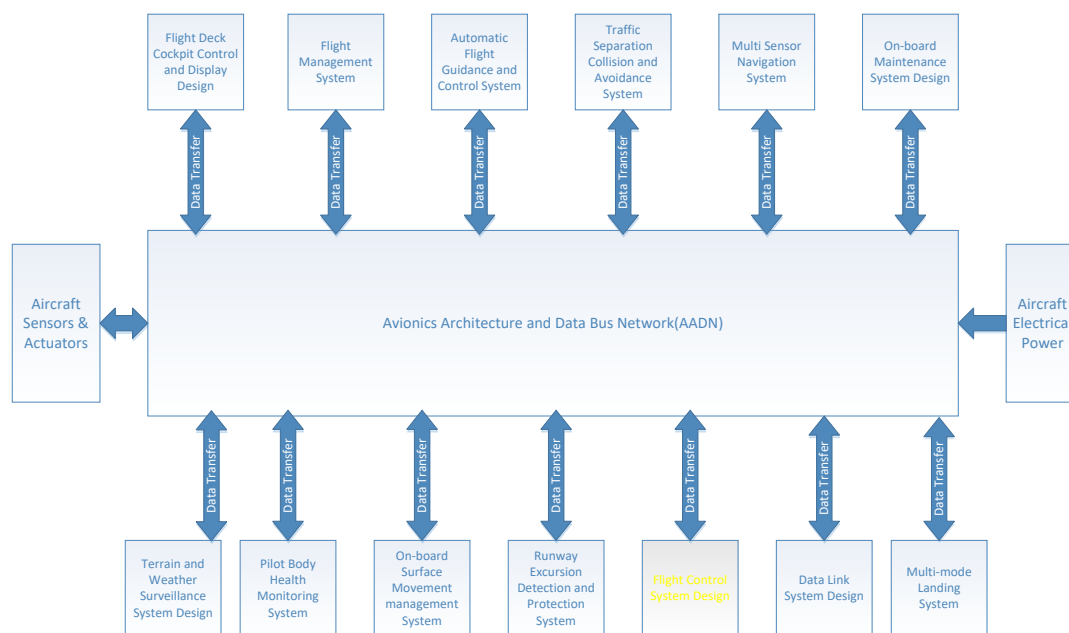


Fig.2 System Interface Design

This interface has the capability of connect with all the other avionics subsystems and also

provides the interface with sensors and actuators required, which achieves highly integrated data communication in avionics systems.

4.2 Functional Architecture Design

Fig.3 shows the functional architecture in IMA Cabinet.

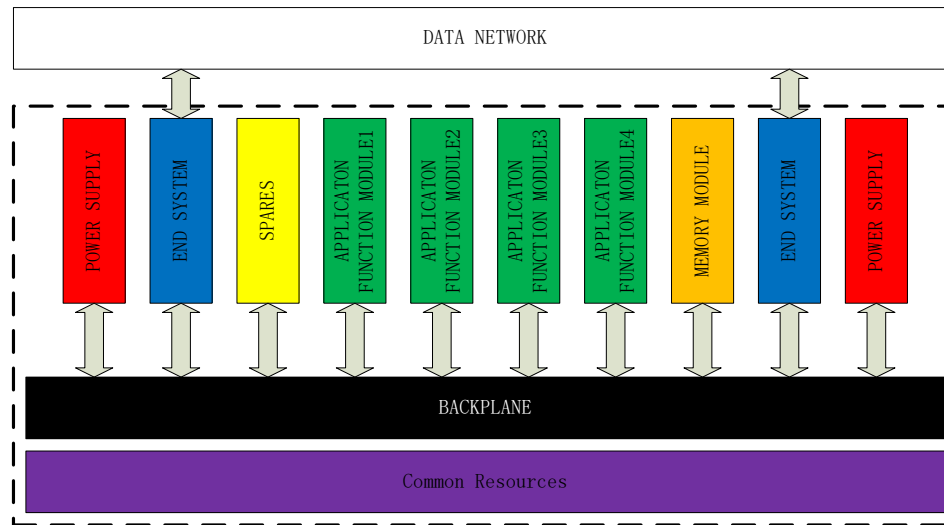


Fig.3 IMA Cabinet

This functional diagram shows the internal modular architecture in an IMA cabinet. Except the backplane, common resources and I/O module, there are five primary modules, power supply modules, end system modules, processors (Applications) modules provided by the subsystems suppliers, memories modules and spares module integrated into this cabinet.

In each IMA cabinet, two power supply modules are configured to avoid the single point failure. End systems establish the interface between IMA and AFDX networks and also provide the network management. Applications are provided by the subsystems suppliers and host in the processing card (application functional module), which is convenient to upgrade or replace. Various applications (processing cards) in the IMA cabinet can communicate with each other through backplane. Spare modules are generally reserved for back up. The Backplane provides medium of communication between avionics function hosted in it. Specially, Partitioning is generally used in order to help segregate mixed-criticality applications in IMA.

Due to the definition of catastrophic level of system failure classification, AADN shall be capability of redundancy both in components and network. Four IMA Cabinets are connected into the AFDX network as Fig.4. This figure is used to show the redundancy concept and each IMA consists of power suppliers, end systems, common resources and so on with different colours. Various applications of avionics systems are allocated into four cabinets respectively.

According to specification of AFDX, at least two networks (channels) called Network A and Network B, are required for redundancy. This architecture averages the output of redundant networks so that all the networks are functional all of the time and faulty network will be disconnected in the event of failure. When the data are sending out, end systems will replicate the data and send them to both two networks, A and B. The receiving end system then will carry on checking and running redundancy management. Fault, lost and slowest data from the networks will be eliminated. Therefore, the high reliability of communication is based on redundant transmission (Dual Redundancy).

Dual redundancy in the switched network and four IMA cabinets are designed for Avionics Architecture Data bus Network (AADN) as Fig.4. This figure is used to describe the detailed architecture and connection in the entire AFDX/IMA. In an IMA cabinet, applications from different subsystems can transmit the data through the IMA backplane.

In the whole AFDX network, various applications can exchange the data in the end systems of

IMA cabinets and then data will be connected into network by AFDX switches, which achieves data communication among all the avionics systems.

Noticeably, Remote Data Concentrator Unit (RDCU) is not only developed for sensors, actuators such as antennas, but also used for data transformation between different data buses (ARINC 429, ARINC 664 P7 etc.) or types of data (analogue data, digital data etc.)

In conclusion, this network can ensure deterministic data transmission and reception and avoidance of single failure.

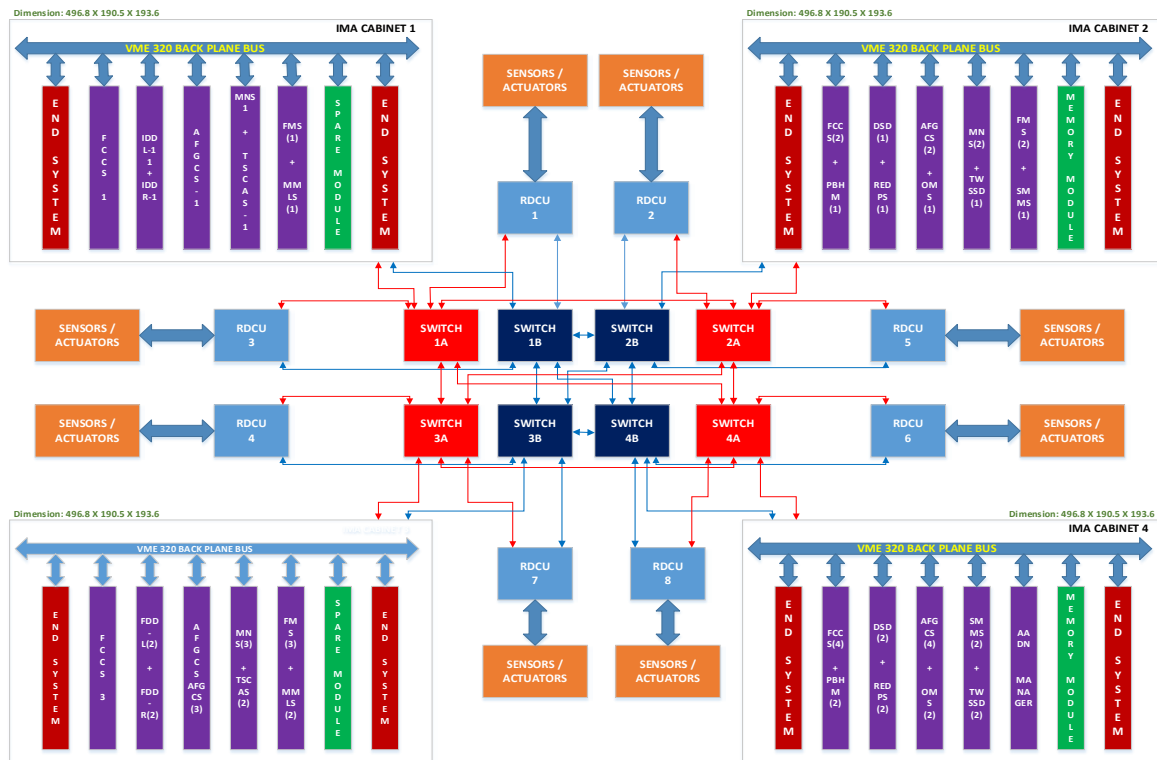


Fig.4 AADN Functional (Network) Architecture

5. System Safety Analysis

After developing the system architecture and fault hazardous analysis (FHA), the safety targets for the subsystems shall be calculated and then from the system level to component level (hardware and software). It is an iterative analysis during all the development process starting from the requirements capture, then architecture design and safety targets allocation, to system safety assessment (SSA) for verifying whether the design targets have been fulfilled. This author gives a top-down fault tree analysis (FTA) of AADN in the chapter.

5.1 FTA of AADN Network

According to the system level FHA, loss of AADN network is catastrophic for failure condition (failure probability less than 10^{-9}) and this top event can be divided into three sub-events, loss of IMA, loss of data communication and loss of RDCU respectively. See Fig.5.

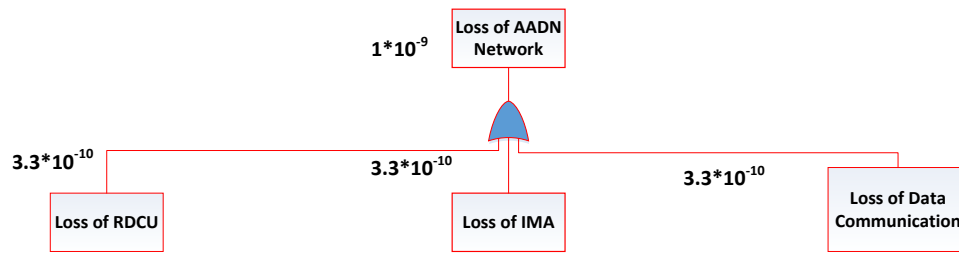


Fig.5 FTA of AADN Network

5.2 FTA of Data Communication

There are two networks (channels) for dual system redundancy, in each of which consists of two end systems with Tx and Rx functions, switch and data bus. See Fig.6.

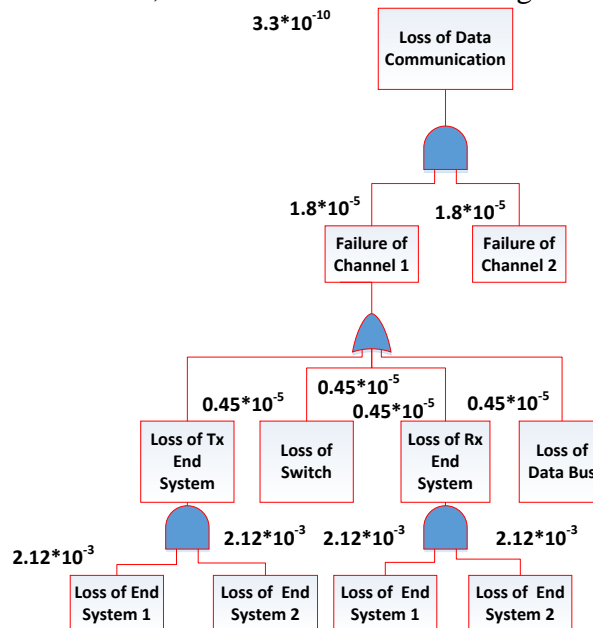


Fig.6 FTA of Communication Data

5.3 FTA of IMA

The primary components in IMA are power supplier module, backplane and processor card. In addition, loss of end systems have been calculated in the communication network. Fig.7 shows FTA of IMA.

5.4 FTA of RDCU

FTA of Remote Data Concentrator Unit is shown in Fig.8.

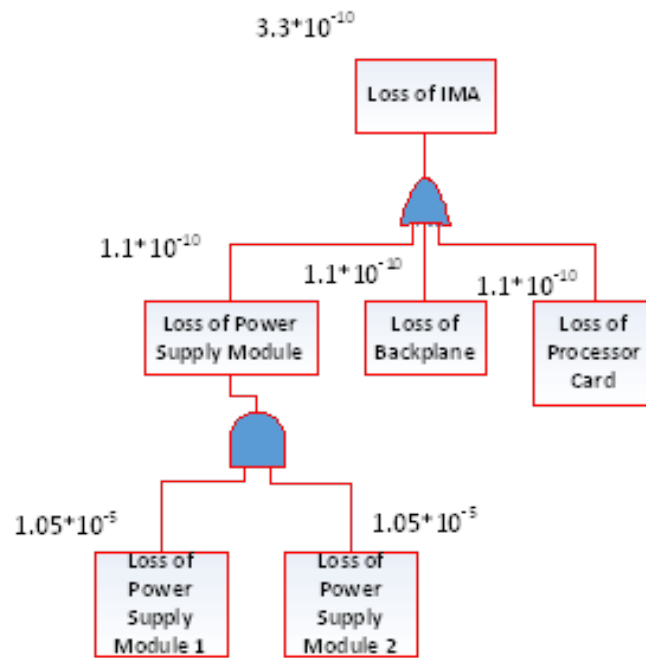


Fig.7 FTA of IMA

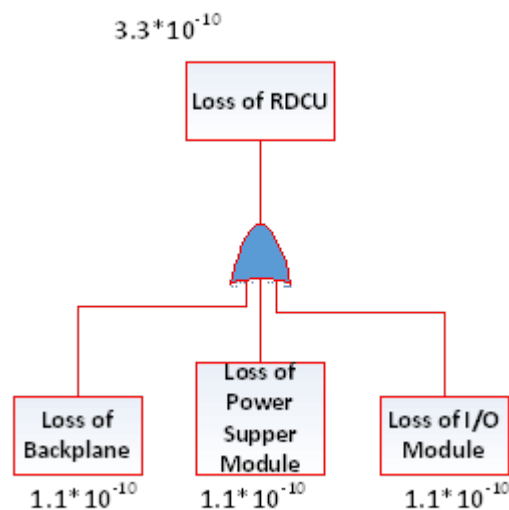


Fig.8 FTA of RDCU

6. Summary

Currently, avionics systems have been developing significantly while avionics architecture is designed to be highly integrated. Integrated Modular Avionics (IMA) with AFDX network is a trend for the avionics architecture design in the future. The author propose the AADN architecture design and the means of safety analysis.

In this article, four IMA cabinets are designed to host 13 subsystems applications, which achieve the integration of avionics architecture as high as possible. Each IMA cabinet has 10 slots for 2 power suppliers, 2 end systems, 5 applications and others for backup. COTS have been chosen for the IMA components. Application inside the IMA cabinet can transmit the messages with each other by VME backplane. The processing cards selected provide different computational capability for various applications. All the IMA design is in compliance with DO-297 and ARINC 653.

In the AFDX network, dual redundancy architecture is developed for ensuring the safety and reliability. AFDX switch and end system are chosen from COTS. All the design of AFDX network is compliance with ARINC 664 P7.

References

- [1] AR Dr. HuaminJia (2014). AVD Avionics System Design Manual(Unpublished).
- [2] ARP4754, certification consideration for highly integrated or complex aircraft systems, SAE, USA