EasyChair Preprint

№ 10164

Fault-Tolerant Systems Based on Distributed IMA Technology

Mohamed Elmahdi

May 15, 2023

Fault-tolerant Systems based on distributed IMA Technology

Dr.-Ing. Mohamed Elmahdi[1]

[1] LAMBDA AeroTech Aviation Consultancy LLC, P.O.Box 96990, Dubai, UAE
mohamed.elmahdi@lambda-aerotech.com

Abstract. The architecture of most present aircraft control systems is based on the principle of the "federated, centralised avionics architecture". Federated avionics architecture means that each system consists of standalone and self-contained avionics; different systems cooperate in a loosely controlled way with each other. Centralised avionics architecture signifies that a centralised avionics computer performs the whole functions assigned to the system. On the basis of the "federated avionics architecture" principle, new aircraft functions require their own dedicated new avionics resources. With regards to aircraft systems in their totality, this will result in a high number of standalone avionics resources leading to increased weight, volume, and life cycle cost.

On the contrary, the "Integrated Modular Avionics" (IMA) provides a solution approach, where the functions of different systems share a number of standardised avionics resources. IMA proves to be efficient, particularly when it shows a distributed character with following specific attributes: 1) an integrated distributed acquisition and generation of signals for different systems by distributed input and output resources, and 2) the integration of the control functions of different systems into common powerful core computing resources.

This paper presents the validation's results of the implementation of a safety critical aircraft function – the secondary flight control function – on an integrated, distributed avionics architecture.

Keywords: Fault-tolerant system, Safety Assessment, Integrated Modular Avionics IMA, avionics, secondary flight control, high lift.

1 Architectures of the avionics control systems

1.1 Federated centralised avionics architecture

Up to the 1990s, aircraft system design – regardless of the safety criticality of the system – followed the "federated centralised avionics architecture" principle [1, 2]. Each system owns its dedicated private avionics resources, which means that each aircraft function runs on a dedicated computer – may also be redundant – connected to its dedicated sensors and actuators [3] as illustrated in Fig. 1. Thereby, most federated systems are centralised.

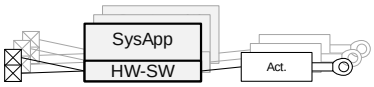

Fig. 1. Federated centralised avionics architecture of one aircraft system

With respect to the steady growth of the new functions to be implemented in any new type of commercial aircraft, this approach led to an exponential growth of avionics hardware and software per aircraft and finally it met its natural limit when the weight and volume of the "black boxes" hit the envelope restrictions of the aircraft. Another burden became obvious, the huge number of different "black boxes" charged the balances of the airlines with life cycle cost, especially with maintenance cost for world-wide computer spare provisioning and handling [1, 2].

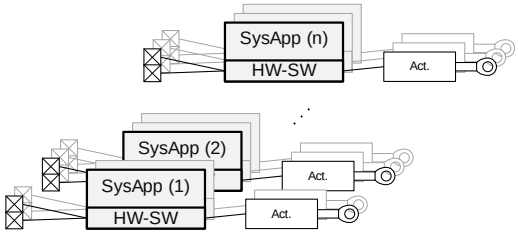

Fig. 2. Federated centralised avionics architecture of n aircraft systems

1.2 Integrated distributed avionics architecture

On the contrary, "Integrated Modular Avionics" [1, 2, 4] applied in the non-safety-critical avionics systems enables sharing of the resources between functions of different aircraft systems. This means that a) the system dedicated avionics resources are replaced by standardised generic powerful resources, and b) the dedicated communication medium is replaced by a standardised communication medium. ARINC 653 [5] specifies an Application Programming Interface API that enables the independent development of the SW applications form the HW; and consequently, the sharing of the HW resources between functions of different aircraft systems. On the other hand, ARINC 664 [6] specifies a standardised means for the communication; the so-called AFDX "Avionics Full Duplex switched Ethernet".

The integrated distributed characteristic enables the optimisation of the avionics resources; this means: a) HW resources can be minimised due to the resources sharing, b) input/output resources and core computing resources can be optimised regarding redundancy degree and dissimilarity needs independently of each other.

A new design milestone for the avionics architectures of the safety critical aircraft systems is achieved in a patent [7] published by Airbus Operation GmbH. The avionics architecture described in the patent shows a distributed integrated character with following attributes: (1) an integrated acquisition of signals of different systems by distributed common modules, i.e. remote data concentrators "RDCs" and remote electronic units "REUs", and (2) the integration of control functions of different systems

into common computing modules. The RDCs, the REUs and the computing modules communicate via an AFDX network.

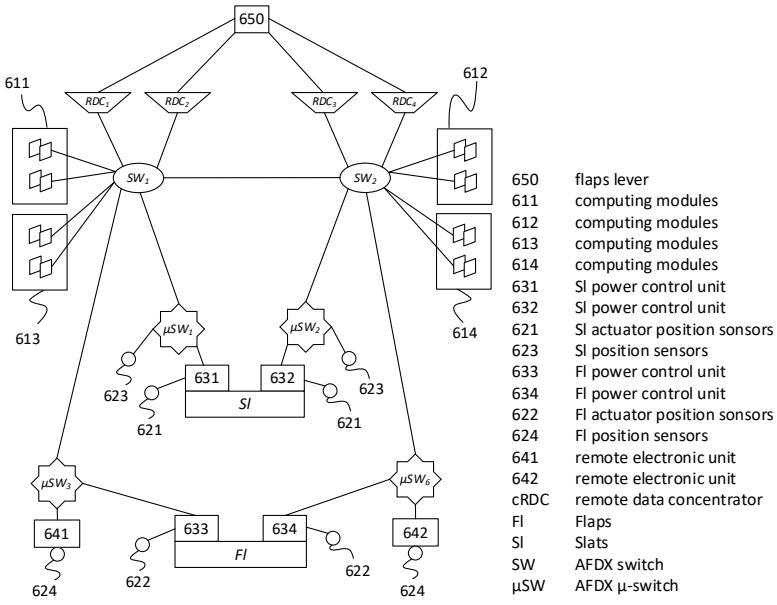

Fig. 3. Integrated flight control system according to Airbus patent [7]

The avionics platform based on the distributed integrated architecture shall run the primary flight control function as well as a plurality of control functions of other systems, for example the secondary flight control function, propulsion control function, brake control function of the landing gear, steering control function, and control function of the hydraulic circuits. Fig. 3 illustrates an example of a secondary flight control system architecture that can be implemented in the aircraft control system according to the patent.

2 The High Lift System (HLS): An example for validation

2.1 HLS current avionics architecture (federated, centralised)

A thorough look at the present avionics architecture of the high lift control system of an Airbus transport aircraft – the A320 exemplary [8] – shows that it is designed in accordance with the classical “federated centralised avionics architecture” principle. Particularly for the high lift control system, the high lift functions run on centralised redundant so-called Slats/Flaps Control Computers – SFCCs – which are specialised to perform the high lift functions.

The system owns its dedicated avionics computers, dedicated sensors, dedicated motors, and dedicated brakes; it operates in a loosely controlled way with other systems. Fig. 4 illustrates the federated architecture of an Airbus high lift control system.

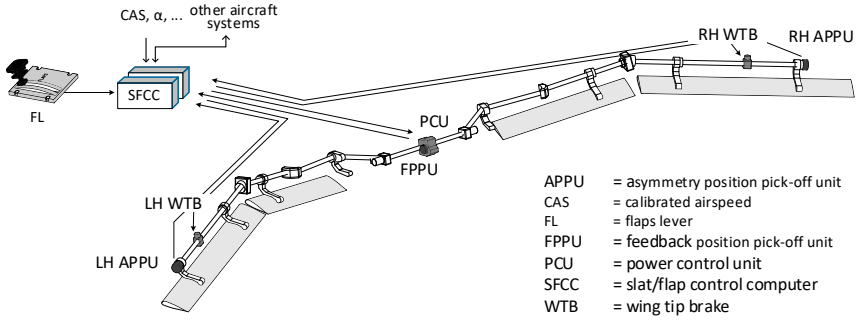

Fig. 4. Federated centralised high lift control system [9]

2.2 HLS future avionics architecture (distributed, integrated)

In the future avionics architecture of the high lift control system, the functions hosted in the conventional SFCC well be distributed over several IMA resources. Remote Data Concentrators RDCs collect the pilot input over the Flap Lever. The RDCs generate AFDX [6] messages, which contain the current FL-position, and send it to the Core Processing Modules CPMs via the AFDX network.

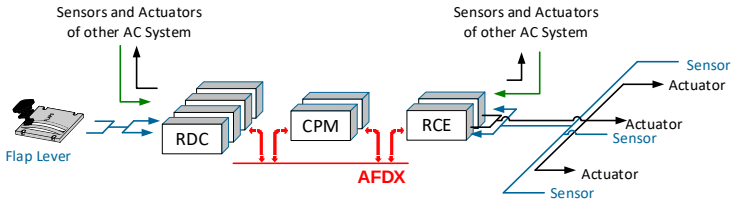

Fig. 5. Distributed, integrated, future high lift control system

The CPMs are located in a cabinet in the avionics bay. Based on the received position, the CPMs compute a target command and send it to the Remote Control Electronics RCEs via the AFDX network. The RCEs, which are located in the middle fuselage close to the PCU, drive the motors to the new target position. Beside the motor sequencing control, the RCEs have the view over the actual flap (slat) position by means of the system sensors, consequently it performs the system monitoring functions. The integrative character of the IMA resources RDC, CPM and RCEs enables the sharing of the resources with other systems e.g. primary control system, cabin pressure control system, etc. in addition to the high lift system.

2.3 HLS requirements

Quantitative safety requirements. Within the scope of the Functional Hazard Assessment FHA, the aircraft system functions will be analysed to identify potential functional failures and classify the hazards associated with these failure conditions [10]. The FHA outcome is shown Table 1.

Table 1. Quantitative safety requirements of the high lift system

System Subsystem	Failure Condition	Classification	P({undesired Event})/FH
Slats & Flaps	(1) Loss of system operation	Major	$< 1*10^{-6}$/FH
Flaps subsystem	(2) Overspeed	Catastrophic	$< 1*10^{-9}$/FH
	(3) Unacceptable asymmetry between RH and LH flats positions	Catastrophic	$< 1*10^{-9}$/FH
	(4) Uncommanded movement	Catastrophic	$< 1*10^{-9}$/FH

Qualitative requirements. Three monitoring functions are implemented in the high lift system to avoid catastrophic events assigned to the failure conditions (2, 3, and 4). The flaps overspeed monitoring prevents the flaps being extended or retracted with high speed. The flaps unacceptable asymmetry monitoring prevents the right- and left-hand flaps entering an unacceptable asymmetrical position. And the flaps uncommanded movement monitoring is implemented to prevent flaps uncommanded movement.

Table 2. Qualitative safety requirements of the high lift system

Monitoring	Detection	Threshold	Reaction
Overspeed	APPUs	Any flaps transmission speed higher than $v_{overspeed}$	WTBs and POBs
Asymmetry	APPUs	Any flaps position difference higher than $\Delta_{asymmetry}$	WTBs and POBs
Uncaommanded Movement	FPPUs	Any flap movement increasing the distance to the target position since a new target position by more than Δ_{UCM}	WTBs and POBs

Here it is useful to remark that the monitoring functions and requirements are demonstrated and verified only for the flaps subsystem – the slats subsystem is equivalent.

3 Verification of the HLS future avionics architecture

3.1 Safety Assessment - Verification of the quantitative requirements

Definitions and mathematical basis. The safety assessment is performed in compliance with the Aerospace Recommended Practices ARP 4754 and ARP 4761 [11, 12]. Fig. 6 shows a generic state diagram [9], which is applied to all system items to get a unique description of the behaviour of each individual system component. Thereby:

- An item is in the state z(t) = "c" (correct): If it behaves for all $0 \leq \tau \leq t$ correctly according to its specification.
- An item is in the state z(t) = "f" (failed): If it is not in the state z(t) = "c".
- An item is in the state z(t) = "f_p" (failed – passive): If it is in the state z(t) = f, and if it is in a predefined condition all the time when it does not behave correctly.
- An item is in the state z(t) "f_o" (failed - out of control): If it is the state z(t) = "f", and it is not in the state "f_p".

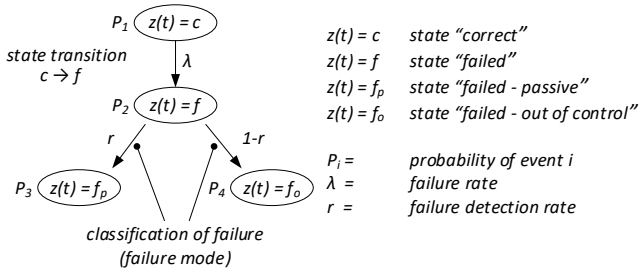

Fig. 6. Failure Mode Model – Classification of failure [9]

The referenced high lift system of Airbus A320 consists of two subsystems, the slats subsystem $z_{S-subsys}$, and the flaps subsystem $z_{F-subsys}$. The HL functions assigned to a subsystem are realised by means of two, redundant, segregated channels $z_{S(F)-channel}$. In order to relate the state of each particular system component z_{comp} to a unique state of the whole high lift system $z_{HL-sys} \in \{c, f_p, f_o\}$, the function G_{FTA} is defined by Fault Trees as follow:

Fault Trees. Four separate fault trees are derived for the key safety failure conditions: "Loss of Slats and Flaps Operation, Flaps Overspeed, Flaps Asymmetry and Flaps Uncommanded Movement". Following is the fault tree of the first key failure condition "Loss of Slats and Flaps Operation", i.e. the high lift system state $z_{HL-sys} = f_p$:

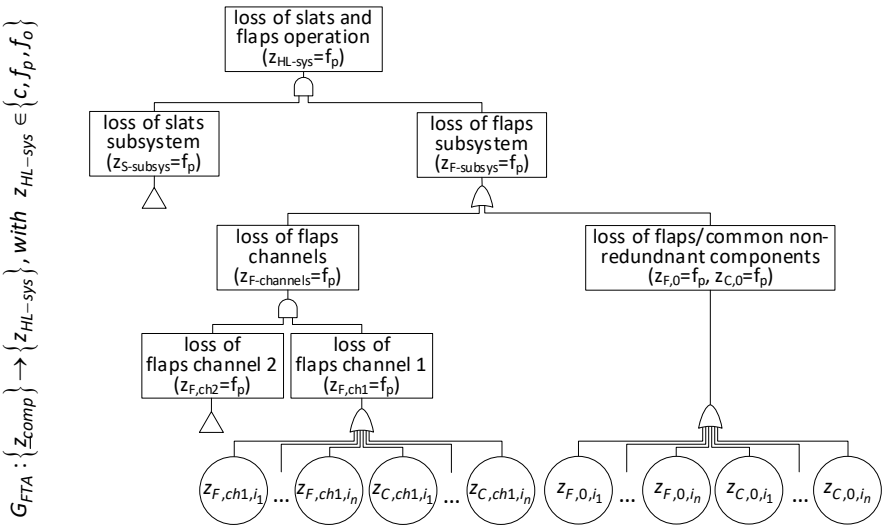

Fig. 7. Fault Tree: Loss of Slats and Flaps Operation

Fault trees of the system state $z_{HL-sys} = f_o$ – the remaining three failure conditions – are worked out in [9]; technics of the FTA and definitions of used symbols are in [12].

In conclusion, probabilities of the failure conditions achieved in the FTA meet the safety requirements of the high lift system under following considerations:

Table 3. Derived quantitative safety requirement for the IMA components

Component of the distributed IMA	maximum allowed failure rate	
	F_p	F_o
Remote Data Concentrator	$5*10^{-4}$/FH	$2{,}23*10^{-5}$/FH
Common Computing Module	$3{,}1*10^{-2}$/FH	$2{,}5*10^{-10}$/FH
Remote Electronic Unit	$3{,}1*10^{-2}$/FH	$2{,}5*10^{-10}$/FH
AFDX	$1*10^{-3}$/FH	$5*10^{-10}$/FH

3.2 Systems demonstrator- Verification of the qualitative requirements

Demonstrator Setup.

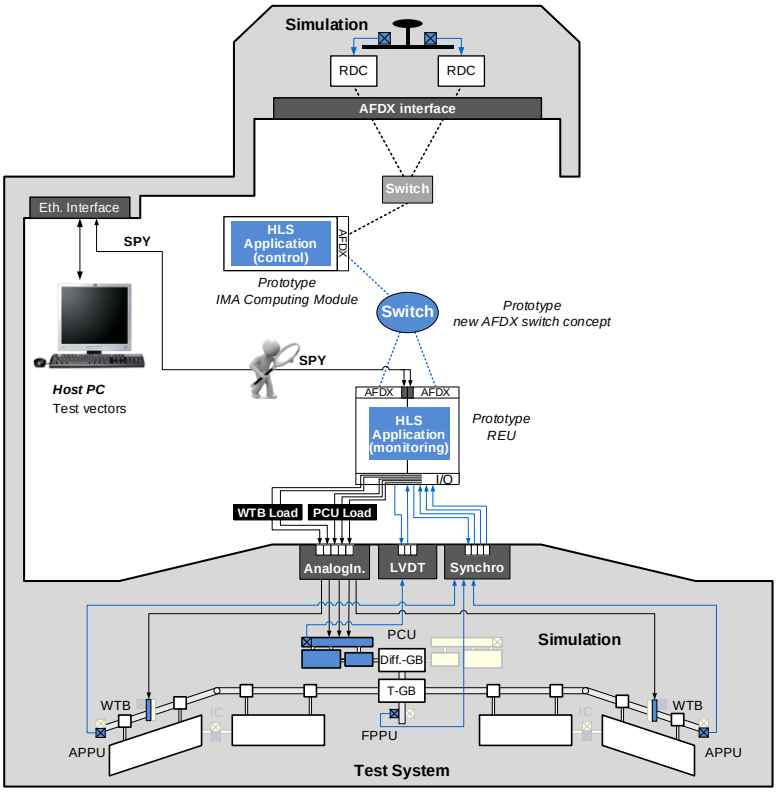

Fig. 8. HLS demonstrator using IMA prototype HW resources

The system demonstrator is built up to verify the timing and data transport delay requirements of the critical system monitoring functions: overspeed, asymmetry, and

uncommanded movement. For this purpose, a single channel of the flap subsystem is demonstrated as Hardware-in-the-loop. IMA prototype HW resources are used for demonstration. Fig. 8 illustrates the demonstrator setup. Details of the test cases and test results are included in [9].

Verification results. In conclusion, qualitative requirements i.e., the timing and data transport delay requirements will be fulfilled under the following IMA specific design restriction and considerations:

Failure detection rate. To achieve the high failure detection rate requirement derived from the safety assessment, redundant architecture of the computing resources is required. In this research n-duplex architecture is applied and analysed. Thereby, duplex means that two lanes are working closely together forming one IMA computing resources. Each lane consists of its own controller, IO interface and communication interface.

Process scheduling. The HLS application process is implemented as a Minor Frame "MiF". MiF is a term used in IMA-technology describing a time window of fixed duration, which will be periodically repeated and contains the scheduling of the processes. To fulfill the restrict timing requirements of the HLS, following MiF design, illustrated in Fig. 9, is proposed for the RCE. Well known that the RCE performs the safety critical HLS monitoring functions:

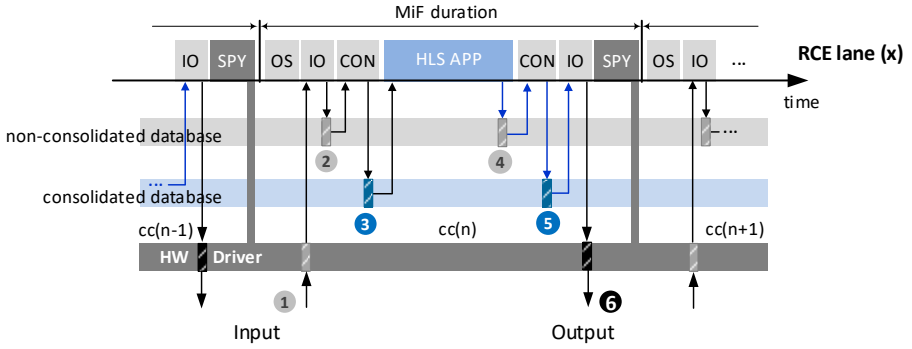

Fig. 9. Minor Frame of one RCE lane

The Operating System "OS" process runs the basics functions of a lane, such as power-on, intialisation, health monitoring, etc. The Input-Output "IO" process is responsible for reading and writing of information from and into all HW interfaces. The Consolidation process "CON" consolidates the database of both RCE lanes to ensure a consistent view in both lanes. The HLS APP performs all HLS specific processes. The SPY process is for verification and integration purposes and can only be activated in the lab mode.

Time synchronisation between both RCE lanes. The OS process is responsible for of the time synchronicity between both RCE lanes. The time synchronisation between the lanes is a prerequisite to have a consistent view in both lanes. This is required to achieve a high failure detection rate.

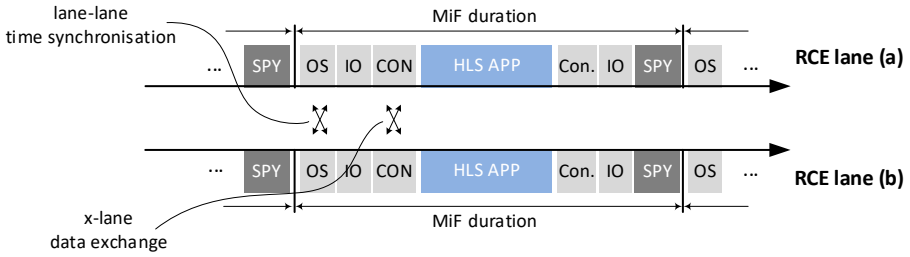

Fig. 10. Time synchronisation and data consolidation between REU lanes

4 Statement of validation

In conclusion, the key validation statement is that the distributed, integrated avionics architecture shows compliance with the requirements of the high lift system – a safety critical system. Thereby, components requirements and architectural attributes requirements derived from the safety assessment and from the experimental verification shall be considered in the system design.

References

1. P. Bieber, F. Boniol, M. Boyer, E. Noulard and C. Pagetti: New Challenges for Future Avionic Architectures, Journal Aero-space Lab Issue 4, 2012.
2. Henning Butz: Open integrated modular Avionics (IMA): State of the Art and future Development Road Map at Airbus Deutschland, Department of Avionic Systems at Airbus Deutschland GmbH, Proceeding of the 1st International Work-shop on Aircraft System Technologies, 2007.
3. Marco Di Natale, Alberto Sangiovanni-Vincentelli: Moving From Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools, Proceeding of the IEEE, Vol. 98, No. 4, 2010.
4. Christopher B. Watkins, Randy Walter: Transitioning from fed-erated avionics architecture to integrated modular avionics, 26th Digital Avionics Systems Conference, DASC '07, IEEE/AIAA, 2007.
5. Airlines Electronic Engineering Committee: Avionics Applica-tion Software Standard Interface ARINC Specification 653-1, Aeronautical Radio Inc., Maryland, United States, 2003.
6. Aeronautical Radio Inc.: Aircraft Data Network Part 7, Avionics Full Duplex Switched Ethernet (AFDX) Network, ARINC Specification 664P7, Maryland, United States, 2005
7. (AIRBUS OPERATIONS) Marc Fervel, Arnaud Lecanu, Antoine Maussion and Jean-Jacques Aubert: Aircraft Control System with Integrated Modular Architecture, Patent Application Publication, Pub. No.: US 2012/0109424 A1, United States, 2012.
8. AIRBUS: A320 Flight Crew Operating Manual, VOL I, 1.27.50: FLIGHT CONTROLS FLAPS AND SLATS
9. M. Elmahdi: Distributed Architecture of an IMA-based Hight Lift Control System, Ph.D. thesis, Institute of Aircraft Systems, University of Stuttgart, Verlag Dr. Hut, 2016.
10. European Aviation Safety Agency EASA: Certification Specifications for Large Aeroplanes CS-25, 2007.
11. SAE International: Certification Consideration for Highly-Integrated or Complex Aircraft Systems, SAE ARP 4754, 1996.
12. SAE International: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE ARP 4761, 1996.
13. M. Armbruster: Eine fahrzeugübergreifende X-by-Wire Plattform zur Ausführung umfassender Fahr- und Assistenzfunktionen, Ph.D. thesis, Institute of Aircraft Systems, University of Stuttgart, 2009.