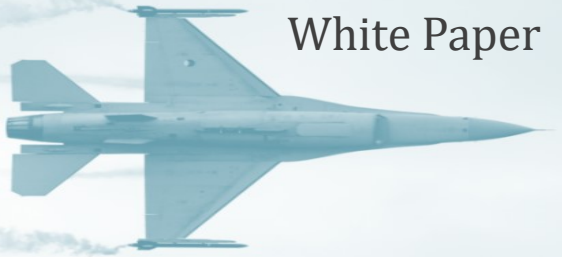


Solving Airplane Safety Requirements with Design Diversity

Introduction

Modern systems are virtually synchronous and utilize redundant units that execute the same software with the same inputs., In order to achieve an acceptable level of safety at the full platform (airplane) level, these require mitigation against the real concern of simultaneous failures in the redundant units. This white paper discusses the simultaneous failures that may occur due to common mode failures and how these can be mitigated through design diversity to meet the numerical safety requirements of the airplane.

Fail-Safe Design Concept

The Part 25 airworthiness standards are based on a Fail-safe Design Concept with section AMJ/AC 25.1309-1A[1] setting certain objective safety requirements based on this design concept. A key aspect of the Fail-safe Design Concept is that an analysis should be prepared that demonstrates the system and its installation can tolerate failures to the extent that major failure conditions (i.e. those having adverse affects to essential functions) are improbable and catastrophic failure conditions (i.e. those having adverse affects on critical functions) are extremely improbable. The analysis should give special attention to the use of design techniques that would prevent single failures or other events from adversely affecting more than one redundant system or more than one system performing operationally similar functions (e.g. primary and back-up flight displays). This paper focuses on redundant systems and the risks of common mode failures amongst them. The techniques described herein are only required for certain types of aircraft hazards associated with catastrophic events as determined by a Functional Hazards Analysis.

Redundancy and Simultaneous Failures Problem

A technique commonly used to meet numerical safety requirements is the use of multiple redundant hardware. Common mode failures need to be considered for multiple redundant systems as a failure common to two or more systems simultaneously is not acceptable since it defeats the intended purpose of redundancy. Common mode failures may be the result of requirement errors or omissions, design flaws, manufacturing problems, installation faults, application errors, etc. Some analysis conclusions attempt to show that common mode failures are improbable; however, these analyses usually fall short of proving this point and are not typically accepted by certification authorities:

1: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25_1309-1A.pdf

1. A failure condition result from a single failure mode of a device that is shown to be extremely improbable
2. Service experience showing that the failure mode has not yet occurred (even though the service experience may be extensive, it is not considered enough)
3. Flight-crew or ground-crew checks that occur before flight (these are of no value if a catastrophic failure mode could occur without any warning during flight)

Addressing Airplane Susceptibility to Common Mode Simultaneous Failures Associated with Catastrophic Events

Airplane susceptibility to common mode failures can be addressed by designing systems for both physical and functional separation. This provides separation from structural damage, lightning strikes, thermal management and other environmental conditions, a common mode reason that may result in a common mode failure.

Because of this, redundant systems should be physically separated as much as possible; they should either be situated in different physical locations within a single equipment bay or ideally in multiple equipment bays.

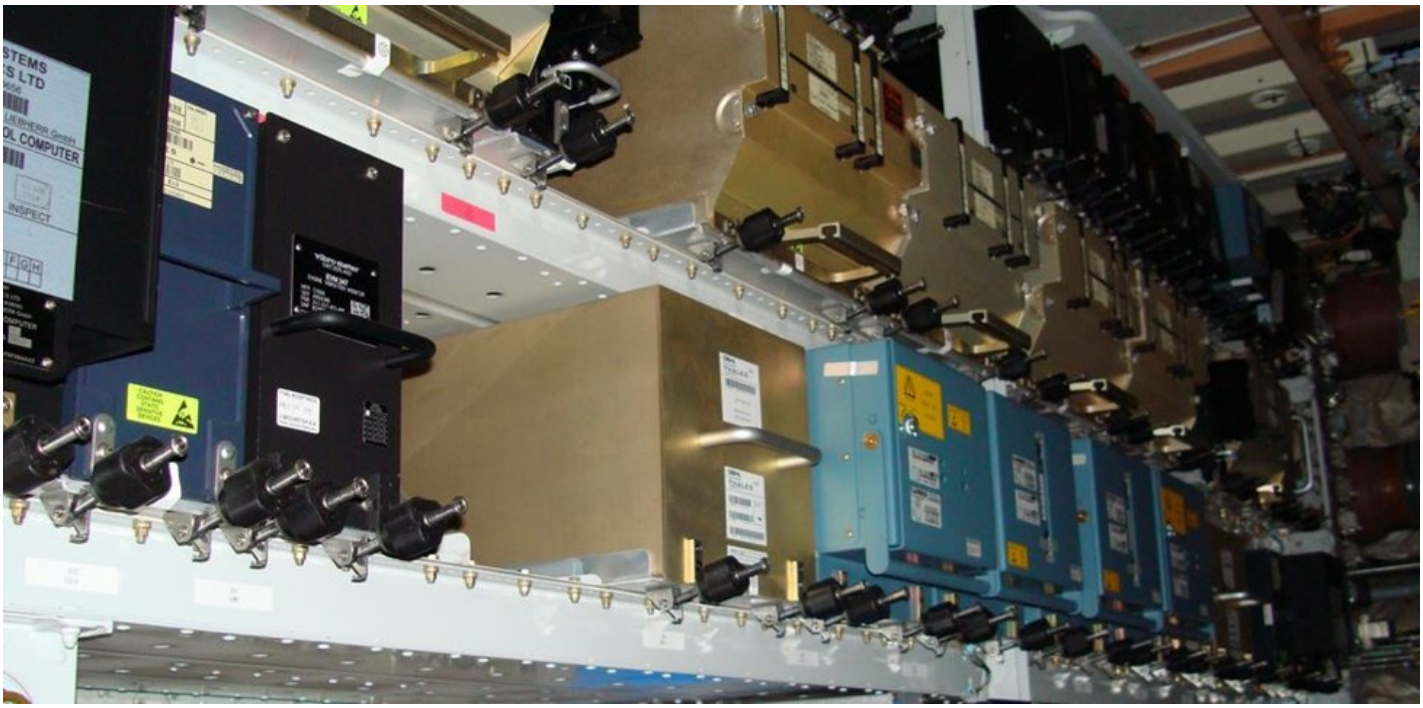


Figure 1: A320 Equipment Bay[2]

2: Taken from https://www.flickr.com/photos/8353822@N02/with/2254309681/

Functional separation of triple redundant hardware is aligned to the left, center and right positions. For example, in a Primary Flight Display (PFD) there are redundant display systems driving the left and right positions with identical looking displays (pilot and co-pilot positions) along with standby flight instruments in the center.

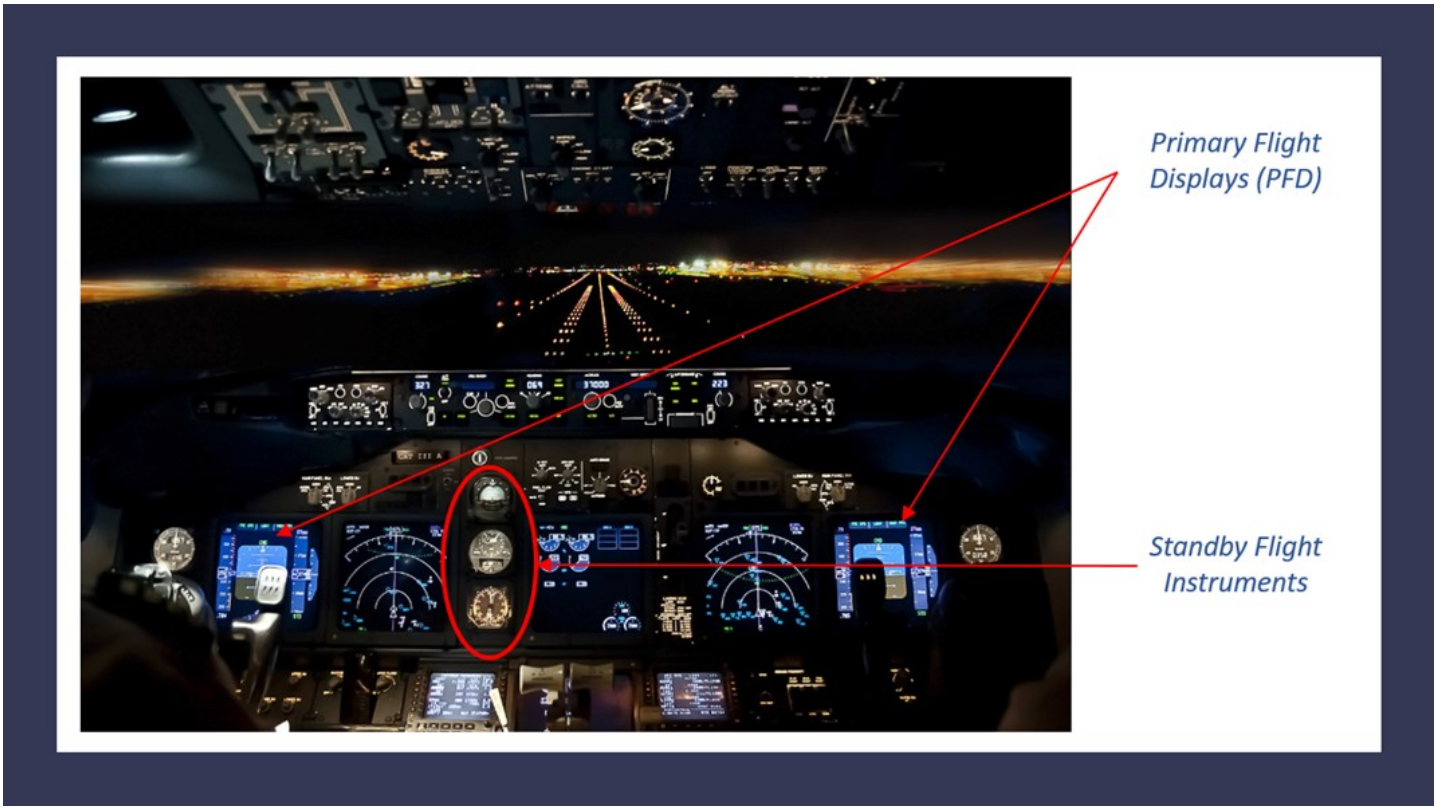
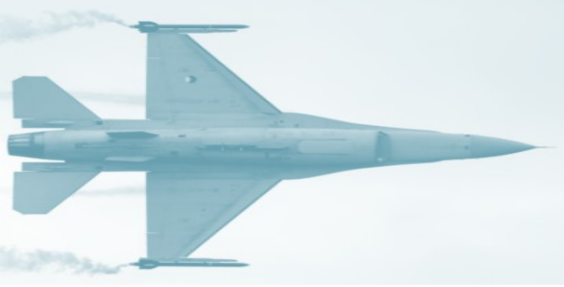


Figure 2: Typical Cockpit Flight Instrumentation

Moving from the airplane level to the system level, common mode failures may occur from the use of complex and highly-complex Commercial Off The Shelf (COTS) electronic components (devices). This typically leads to requirements for dissimilar hardware to avoid the potential for common mode failures. In the example of cockpit flight displays, the hardware used for standby instrumentation in the center position is typically different to that used by the PFD in the left and right positions.



One approach to avoid common mode failures is to select systems from different suppliers. In the cockpit flight displays example, the supplier for the standby instrumentation would be different to the that of the PFD. On the surface this would appear to provide a dissimilar software/hardware architecture as the two systems would be architected and developed independently. However, it is not known if both systems suffer from a similar implementation error. That is, a common hardware failure may result in a loss or false (but believable) operation due to the use of the same hardware device, same (but incorrect) understanding of the requirements and other reasons that may result in a common implementation error. Credit may be taken for software and AEH Programmable Logic Devices (PLDs) on these targets when development follows ED-12C/DO-178C or ED-80/DO-254 process guidelines applying rigor to find errors in the designs. However, the COTS device has no assurance that it is free from errors; for DAL A, and sometimes DAL B, service history will not address the concern of loss of both parts (i.e. each system) at the same time for a critical or essential function of the airplane. Part of achieving design diversity is looking for different manufacturers and architectures. In the case of a PLD, the same mask and die will be used on several variants of the same family of parts and therefore will not be enough to achieve dissimilarity. That is, it would not be feasible to prove that two parts from a single manufacturer are fully dissimilar. How far one may need to go to address the safety requirements with dissimilarity will vary depending on the certification authority and the assigned certification authority personnel. The easiest path to convince a certification authority that the safety requirements have been achieved is to use different manufacturers for the PLD, CPU, GPU or any complex COTS part - for example, a PLD solution from Microsemi® and Xilinx® and a CPU solution from NXP® and Intel®.

Case Study: Fly-By-Wire Controls

In the mid 1980's, the original Airbus A320 ran fly-by-wire controls on pairs of dissimilar single board computers with independently written software that cross-checked each other. The fly-by-wire systems are redundant for fail-over and for functional separation of primary flight controls (two Thomson-CSF computers based on the Motorola 68010 for elevator and aileron) and alternate controls (three SFENA/Aerospatiale computers based on the Intel 80186 for spoilers and horizontal stabilizer); if either fails the other can still control both pitch and roll. This illustrates how two different manufacturers were used, where each used a different processor technology and worked to different functional specifications. There are two software packages written for each system type, one for the control system and one for the monitoring system. If the monitoring verification fails, the system pair (control/monitor) is declared faulty and a fail-over approach is used. There is also a mechanical backup in the case of a complete electrical failure.

Boeing's original 777 fly-by-wire system is similar and is described in a white paper[3]. Interestingly, in section 3.3 of the referenced white paper, Boeing identified challenges with dissimilar software and abandoned that approach. Boeing discovered academic research that demonstrates how multiple versions of software developed independently can contain similar errors. Boeing's own experience is that the source of most of the errors are a result of erroneous or misinterpreted requirements. Close communication was needed between the system requirements engineers and the software engineers to eliminate these errors and this communication resulted in a positive side effect of improved system requirements. This close communication would have otherwise been precluded by a dissimilar software design approach to maintain software development independence. Boeing found that with a single software approach with high level of communication within the system requirements engineering team, the gain in total system integrity outweighed what would have been achieved with a dissimilar software design approach.

What about Software?

In general, AMJ/AC 25.1309-1A is not applicable to software and it references AMJ/AC 20.115D[4] to address acceptable means for assessing the software. Software is expected to be developed following ED-12C/DO-178C guidelines (or some acceptable alternate means process) and therefore the dissimilarity does not apply because disciplined, rigorous development assurance process is relied upon to limit the likelihood of development errors that could impact airplane safety. With dissimilar hardware, there is potential to take some credit with regards to certification for software that is inherently dissimilar to a degree given the different architecture and compiler.

The CAST-24[5] position paper discusses how the fail-safe concept and design techniques can be interpreted and addressed for software related development errors and complex electronic hardware.

Safety Certifiable Solution Building Blocks

Core Avionics & Industrial (CoreAVI) is the first to offer COTS-D products. COTS-D provides complete circuit board assembly design and qualification data along with ED-80/DO-254 evidence for a diverse range of single board computers and graphics modules, enabling customers to quickly and economically produce ED-80/DO-254 hardware with low risk and address dissimilar hardware requirements.

CoreAVI also provides safety critical OpenGL® and Vulkan® graphics drivers, video decode and video encode drivers for a diverse selection of COTS Graphical Processors (CGPs), and solutions for CGP monitoring to detect situations that may lead to the display of hazardously misleading information and handle mixed DAL applications. All of these solutions are available with ED-12C/DO-178C evidence.

Find Out More

To learn more about our solutions, please contact CoreAVI at Sales@CoreAVI.com.

3: White paper accessible at: https://citemaster.net/get/3096e588-8b87-11e8-8c74-00163e009cc7/yeh98_777-fbw.pdf
4: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-115D.pdf
5: https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/cast_papers/media/cast-24.pdf