Why Dissimilar Redundant Architectures Are a Necessity for DAL A

Read About

Introduction

It's estimated that there are more than 100,000 airplanes flying worldwide each day. In 2017, the Federal Aviation Association (FAA) reported that, at any given moment, Air Traffic Control is supporting an average of 5,000 aircraft in 29 million square miles of controlled airspace. The number of aircraft flying above our heads (and homes) on a daily basis increases significantly when you consider the growing prevalence of drones and other unmanned aircraft for both commercial and military uses.

The critical systems responsible for an aircraft's safe flight are understandably subject to stringent safety regulations, to which their adherence must be proven before an aircraft is deemed airworthy. Ultimately, an aircraft's certification is authorized by the regulatory body for aviation safety in its country of origin. These agencies include the FAA, the European Aviation Safety Agency (EASA) and Transport Canada. Multi-lateral agreements exist

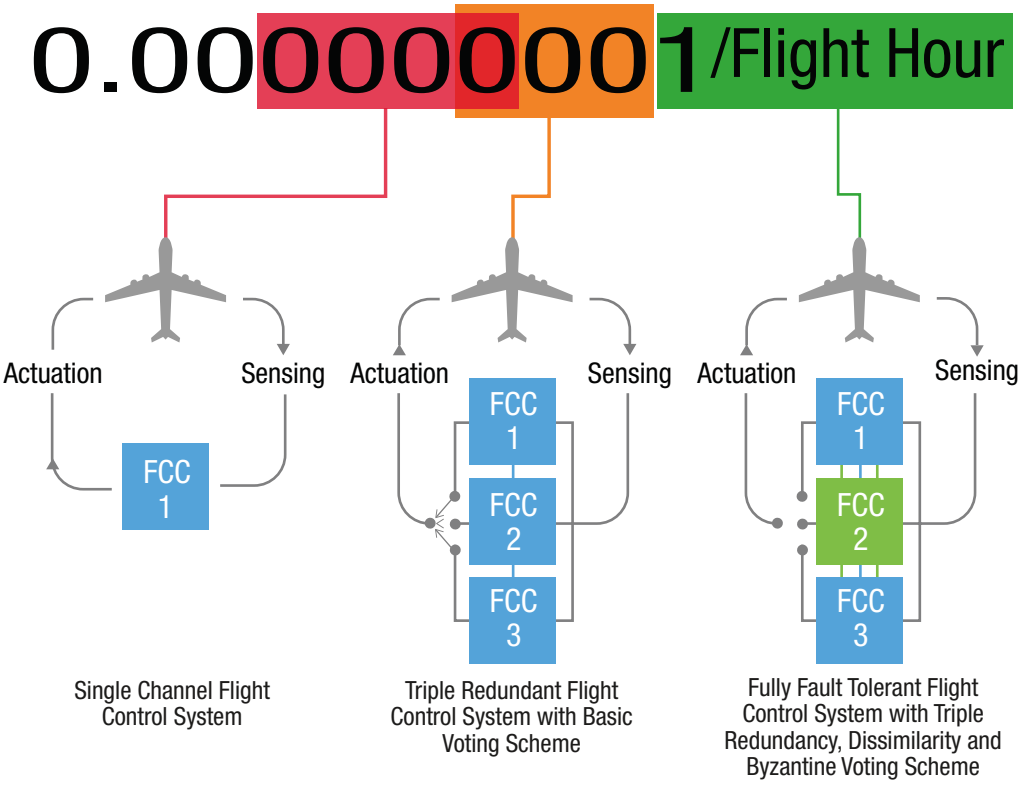

Figure 1: Achieving <1 in 10^{-9}/Flight Hour
Probability of Failure with a Dissimilar Redundant Architecture

between many certification agencies worldwide, meaning once a system has been safety certified in one country, the certification can be valid in other countries (pending the completion of some paperwork).

Agencies such as the FAA issue Technical Standard Orders (TSOs) that prescribe the Minimum Performance Standards (MPS) aircraft parts and materials must comply with in order to be certified for flight. New equipment manufactured after the release of a TSO must meet these requirements. These MPS (and the TSOs that reference them) are written in accordance with guidelines from independent organizations, such as EUROCAE, SAE International, ARINC and the Radio Technical Commission for Aeronautics (RTCA).

Design Assurance Levels and Acceptable Probability of Failure

SAE International is a global association that develops engineering standards for a variety of industries such as aerospace, where its Aerospace Recommended Practice (ARP) guidelines play a critical role in the aircraft design and safety certification process. One of SAE's most prominent sets of standards is ARP4754A, which details Guidelines for Development of Civil Aircraft and Systems. In designing these guidelines, SAE has examined the computing systems required to control modern aircraft (such as flight control computers, autopilot, navigation systems and landing gear controls) and evaluated the safety criticalities that would result from a malfunction in one of these systems. These criticalities range from no effect, which would be expected from the failure of a non-essential system like in-flight entertainment, to catastrophic for safety-critical systems that would prevent an aircraft from operating safely or landing should the system break down.

Depending on the safety criticality its malfunction would bring upon the aircraft, each system is assigned an acceptable probability of failure. For example, for flight-critical systems that would result in catastrophic loss of life – the highest level of danger – it must be demonstrated that the probability of failure is lower than one in one billionth (10^{-9}) per flight hour. The acceptable probability of failure per flight hour increases slightly for systems that pose lower threats of danger in the event of a glitch.

A system's potential for danger in the event of an error and the associated acceptable probability of failure dictate its Design Assurance Level (DAL) that must be met in order to be certified for flight. This means that the key computing elements of a system, such as the single board computers (SBCs), graphics cards and operating systems built into a flight control computer or flight display, must all endure stringent testing to prove they can meet the required DAL.

TABLE 1 Design Assurance Levels (DALs) and Acceptable Probabilities of Failure

DAL	Danger Level	Probability of Failure	Systems Affected
A	Catastrophic: failure results in preventing the aircraft from continuing safely and/or landing	<1 in 10^{-9}/flight hour	Flight control computers, fly by wire, full authority digital engine control, flight displays, air data systems
B	Hazardous: failure results in serious or fatal injuries to the aircraft occupants	<1 in 10^{-7}/flight hour	Autopilot, autothrottle, ice protection, standby flight displays, instrument landing system, landing gear control
C	Major: failure results in discomfort or injuries to the occupants	<1 in 10^{-5}/flight hour	Navigation systems (such as GPS), yaw damper, environmental control systems
D	Minor: failure results in causing come inconvenience to the occupant	<1 in 10^{-3}/flight hour	Flight data recorder, data acquisition system, cabin lighting
E	No effect	n/a	In-flight entertainment

Standards for Hardware and Software Design

Along with SAE, RTCA is another organization that serves as an advisory to the FAA, providing technical guidance on various facets of air transportation. RTCA has developed several documents that guide the development of avionics hardware and software, establishing Minimum Operational Performance Standards (MOPS) in accordance with the DALs outlined in Table 1.

Two examples of RTCA documents adopted as standards by the FAA are DO-254 (Design Assurance Guidance for Airborne Electronic Hardware) and DO-178C (Software Considerations in Airborne Systems and Equipment Certification). When it comes to embedded systems, these two documents are key for system designers as they evaluate the hardware components, operating systems and applications that they will use in their safety-certifiable systems.

For instance, an SBC that is designed for use in a flight control computer (which, as noted in Table 1, can cause a catastrophic failure in the event of a malfunction) must be certifiable to DAL A in accordance with DO-254 and provide drivers for DO-178C safety-certifiable operating systems and applications. Similarly, a video capture and processing card providing the graphics in a flight display system would need to be demonstrably certifiable to DAL A.

To meet certification requirements, the system designer must present an assortment of artifacts, meaning data collected from a wide array of tests as outlined in the DO-254/DO-178C documents.

These artifacts must demonstrate that any unused hardware functions or software features are discarded or disabled in such a way that they can't impact the performance or safety of the system itself. As well, they must prove that any disabled hardware function will remain off and can't be accidentally turned on again. Prior to testing, any unneeded or undesired software features should be completely removed in order to reduce the number of lines of software code that need to be tested for certifiability, as any additional line of code that isn't needed for the application will add unnecessary burden to the certification process.

As an alternative to conducting the rigorous and time-consuming tests to develop DO-254/DO-178 artifacts, hardware and software components can be purchased from vendors with experience and expertise in safety-certifiable programs. These products are delivered with the full set of artifacts demonstrating certifiability, resulting in a significant reduction in the time and cost of certifying the complete system.

Regulations for Unmanned Aerial Vehicles

There are an increasing number of use cases – both commercial and military – to deploy large drones, weighing upwards of 600lbs, in civil airspace. Operating without a pilot to account for unforeseen issues, unmanned aerial vehicles (UAVs) are understandably subject to additional safety requirements. Whereas a pilot in an aircraft can see and avoid potential safety threats while in flight, a UAV must have the proper systems onboard to detect these threats and compute a method of avoidance. In lieu of a pilot's vision, a UAV must use surveillance sensors to "see". And, in the absence of a pilot's judgement, a UAV must rely on mathematical expressions to maintain safe flight.

To ensure today's UAVs are equipped to fly without an onboard pilot, two TSOs have been released specifically for unmanned aircraft. TSO-C212, in accordance with DO-366 (UAV Air-to-Air Radar), provides standards for the UAV's scanning radar that serves to detect other aircraft while in flight. The complementary TSO-C211 invokes DO-365 (UAV Detect and Avoid Systems) and outlines requirements for an onboard system capable of computing an avoidance maneuver should an intruder enter the UAV's flight path. All UAVs weighing more than 55lbs, flying in controlled airspace above 400ft and out of view of their operators should be certified to DO-365.

Unmanned Aerial Systems (UAS) have a separate set of DALs and failure probabilities to adhere to based on their kinetic

TABLE 2 DALs and Acceptable Probabilities of Failure for UAS

DAL	Kinetic Energy in Ft-Lbs	Probability of Failure
A	≥50,000,000	<1 in 10^{-9}/flight hour
B	≥6,000,000 to ≤ 49,999,999	<1 in 10^{-8}/flight hour
C	≥800,000 to ≤ 5,999,999	<1 in 10^{-7}/flight hour
C	≥25,000 to ≤ 799,999	<1 in 10^{-6}/flight hour
D	≥530 to ≤ 24,999	<1 in 10^{-5}/flight hour
E	≤ 529	<1 in 10^{-4}/flight hour

energy at ground impact. The calculations behind these DALs are detailed in TSO-C213 (Unmanned Aircraft Systems Control and Non-Payload Communications Terrestrial Link System Radios).

The functionality for both air-to-air radar and detect and avoid systems are typically executed from the same computing module or system. While size, weight and power (SWaP) optimization is a priority with any aircraft, ultra-small form factors for these types of embedded computing devices are of particular interest to UAV designers. After all, UAVs can be designed to log extensive continuous flight hours that would not be requested of a human pilot, meaning the ability to dedicate extra onboard space to additional fuel sources is a significant advantage.

Military Adoption of Commercial Standards

When a commercial aircraft is approved for flight by the FAA or another regulatory body, its designer is issued a type certificate that signifies the airworthiness of the manufacturing design. Military aircraft, on the other hand, do not receive a type certificate; instead, the aircraft designer is given so-called design authority when its aircraft has been proven to meet its certification requirements.

U.S. and Canadian military agencies now generally accept artifacts that align to commercial standards, such as DO-254 and DO-178C, as certification evidence. For example, DO-160 has come to be recognized in place of MIL-STD-461 and MIL-STD-810 for environmental conditions and testing. Similarly, ARP4754 and ARP4761 are together accepted as a safety assessment in place of MIL-STD-882.

Occasionally, military aircraft will be subject to additional testing for challenges commercial aircraft are not expected to encounter, such as corrosive gas or gunfire. The latest “C” revision of MIL-HDBK-516 provides certification guidance for military aircraft and encompasses both MIL- and RTCA standards.

Overcoming the DAL A Challenge

For avionics systems requiring DAL A certification, adhering to the <1 in 10^{-9} probability of failure is no easy feat. Take, for example, a flight control computer that relies on multiple air data computers and their collected inputs from sensors such as air speed sensors, altitude sensors, accelerometers, and gyroscopes in the roll, pitch and yaw axes. The flight control computer is responsible for reading data from these systems and calculating outputs to drive actuators for various aircraft components (for example, rudders, elevators and propulsion systems) in order to keep the aircraft in straight and level flight. Communication between these sensors and the flight control computer occurs at a high frequency, creating a controlled feedback loop.

Relying on a single computer to manage this loop would fall short of meeting the acceptable <1 in 10^{-9} probability of failure rate. The pitfall of a single channel flight control system is that any single point of failure in that chain can cause the entire system to malfunction. And, no matter how reliable your electronics are, unpredictable external factors can still cause a malfunction. For instance, if a UAV strikes a bird in flight and one of its probes becomes blocked, this can result in one of two major classes of errors: the probe can become completely inoperative or it can begin transmitting Hazardous Misleading Information (HMI) to the flight control computer. Either type of error can potentially prevent the flight control computer from properly calculating the desired output for any of the aircraft components under its control, and can ultimately lead to a disaster. For this reason, redundancy is critical in DAL A systems.

Introducing Redundancy and Basic Voting

A triple redundant system is a fault tolerant form of redundancy that incorporates one active system primarily controlling the aircraft and typically two additional systems on standby in case the main active system faces any sort of failure. The standby systems run in parallel to the main, active flight control computer throughout flight, running their own algorithms using their own independent sensors and air data computers. A basic voting scheme is employed to compare outputs and dictate which of the two standby systems will take over in the event of a failure in the active system. The voting logic establishes a majority when there is a disagreement, and the majority will deactivate the output from the device that disagrees.

However, a redundant architecture is not necessarily guaranteed to meet the <1 in 10^{-9} failure probability per flight. For safety certification purposes, a system designer is responsible for demonstrating that their aircraft can withstand the complete loss of the main active system, and a redundant architecture built with similar channels is susceptible to common mode failures that can cause all channels to fail in the same way. Common mode failures can be unpredictable and unpreventable, like a lightning strike, electro-magnetic interference, a fire or an

explosion. Software bugs are another form of common mode failure that are hard to protect against; because complex aviation applications are built from tens of thousands of lines of code, it's realistically impossible to test for and prevent every possible software bug or combination of events.

Furthermore, the basic voting scheme employed in this scenario is typically incapable of viably arbitrating between the two standby systems should they offer conflicting directions. For this reason, a more complex scheme is required.

Strengthening Redundancy with Dissimilarity and Complex Voting

Dissimilar redundancy can mitigate common mode failures by using two or more different processor types with dissimilar software, and/or a backup system that uses different sensors and controls from the main active system. By running different operating systems and applications on dissimilar hardware, system designers can add an extra layer of protection against software bugs that would impact the different hardware architectures in similar ways.

Moreover, a DAL A certifiable redundant architecture requires a more intelligent voting system to decide which standby system's directions should be followed in the event that they conflict with those of the other standby system. A Byzantine voting scheme, derived from the Byzantine Generals' Problem concept, is an advanced method of examining each flight control computer using a complex analysis of various parameters and probabilities in order to determine which of the multiple systems in a redundant architecture is providing the most accurate instructions.

Examples of Highly Redundant Systems

A prime example of a highly redundant system can be found in NASA's Space Shuttle fleet. The computers in the Space Shuttle control flight and mission functions, and have been designed to handle several levels of component failure without compromising mission success. This high level of fault tolerance is achieved through five computers, four of which run identical software. The fifth is an independent backup computer running different software to protect against generic software problems that may impact the quad-redundant set.

Airbus provides further examples, with its A320 leveraging five dissimilar computers running four dissimilar software packages. As well, the Airbus A330 and A340 employ three flight control primary computers, two flight control secondary computers, plus two redundant flight control data concentrators. Each computer utilizes two independent channels and detects failure by comparing the channel commands to preset thresholds. Ultimately, these planes only require one active computer to safely fly.

Similarly, the Boeing 777 is designed with a high level of redundancy. The 777 features three primary flight computers with dissimilar processors that each transmit data through an independent channel, resulting in three unique control paths. This Boeing method is referred to as triple-triple redundancy.

There is much debate and uncertainty about how much redundancy is too much redundancy, as the increase in a system's reliability with the addition of each redundant computer is not a one-to-one ratio. Particularly where size, weight and power optimization are high priority, the sacrifices made for minimal gains in reliability are important to consider.

Building a Fault Tolerant Redundant Architecture

To help system designers build redundant architectures with lower risk of common mode failure, Curtiss-Wright's selection of safety-certifiable Commercial Off-the-Shelf (COTS) modules includes SBCs powered by Intel®, Power Architecture® and Arm® processors.

These DO-254 certifiable boards are built with drivers to support DO-178C certifiable software from experienced vendors, such as Green Hills Software®, Wind River®, Lynx Software Technologies® and Sysgo®. Take, for example, Curtiss-Wright's Power Architecture-based VPX3-152. Designed to meet DO-254 DAL A requirements, the VPX3-152 offers a board support package for Green Hills Software's INTEGRITY-178 tuMP, an operating system that has provided the software foundation for various DO-178 DAL A certified programs and is supported by all Curtiss-Wright DO-254 certifiable SBCs. Together, the VPX3-152 and INTEGRITY-178 tuMP operating system support a variety of applications for safety-critical airborne electronics, such as Harris® Corporation's FliteScene® Digital Moving Map software.

Authors

Rick Hearn

Senior Product Manager

Curtiss-Wright Defense Solutions

Paul Hart,

Chief Technology Officer

Curtiss-Wright Defense Solutions

Lisa Sarazin,

Marketing Portfolio Manager

Curtiss-Wright Defense Solutions

As well, Curtiss-Wright's VPX3-1220, a DAL C safety-certifiable SBC featuring the 7th Generation Intel "Kaby Lake" Xeon processor, supports Lynx Software Technologies' LynxOS178 real-time operating system and LynxSecure Safety Bundle, which integrates key security capabilities onto Intel multicore systems. The LynxSecure Safety Bundle features LynxSecure, a secure-by-design separation kernel hypervisor. This provides assured separation, meaning only software in the LynxOS-178 partition needs to achieve DO-178 certification even though the software resides on the same processor as non-critical applications with no safety requirements. The availability of DO-254 artifacts for the VPX3-1220 coupled with the FAA Reusable Software Component artifacts of LynxOS-178 significantly reduces the time and cost for integrators to certify systems deployed on military and commercial manned and unmanned aircraft.

Bringing a third processor architecture into the mix, Curtiss-Wright offers the VPX3-1703, the industry's first safety-certifiable 3U OpenVPX Arm SBC. Pairing the NXP Layerscape LS1043A Arm quad-core A53 processor with advanced I/O capabilities, the VPX3-1703 brings new levels of performance at low power to programs with DO-254 certification requirements up to DAL A.

This broad array of processor architectures and software support enables system designers to build dissimilar, highly redundant architectures with COTS modules that are designed to work together. Each Curtiss-Wright DO-254 certifiable SBC is delivered with an artifacts package to support the required DAL, significantly reducing the cost and time involved in bringing a certifiable system to market.

Learn more

Products: Curtiss-Wright DO-254/178 certifiable SBCs

Read: Curtiss-Wright strategic partners

White Paper: Accelerate Time-To-Market With Safety-Certifiable Airborne Electronics Hardware

White Paper: Understanding Your Safety-Certifiable COTS Options: A Closer Look at the Subsystem Level

White Paper: Overcoming the Challenges of DO-254 Certification in Multi-core COTS Modules