WHITE PAPER

A Low-risk, COTS Approach to Building Safety Certifiable Processing Subsystems

How to affordably decrease safety critical processing subsystem development time and program risk using DO-178 / DO-254 certifiable off-the-shelf building blocks.

www.mrcy.com

JANUARY 2017

mercury systems™

Introduction

As processing systems are being designed to assist and in the case of autonomous, unmanned aerial vehicles (UAVs) replace humans, and as military platforms increasingly require flight safety assurance for government permission to operate within commercial aerospace, safety certification is becoming ever more critical and widespread.

Developing processing subsystems that have the required safety certification for these rolls is complex, time consuming and has the potential to be expensive. The traditional approach to developing these subsystems has been to design them from scratch, which has resulted in project delays and an overall high execution risk. There is a need for an efficient, reliable and cost-effective path to develop safety critical processing subsystems which is inherently low risk.

For non-safety equipment, system engineers leverage COTS (Commercial off the Shelf) items to accelerate the development and lower the risk of projects. Now these COTS building blocks are available for safety applications with the introduction of Mercury Mission System's Avionics Series that are designed from the ground up with safety built-in. Avionics Series processing building blocks are designed to DO-254 (hardware) and DO-178 (software) processes and are provided with artifacts to support system certification, saving time, cost and minimizing risk while developing safety critical processing systems.

"There is a need for a fast, reliable and cost-effective path to develop safety critical applications which is inherently risk adverse"

Safety Off-The-Shelf

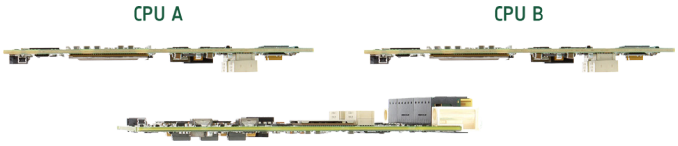
Mercury Mission Systems' Avionics safety certifiable COTS building blocks or SRUs (Shop Replaceable Units) are engineered to the Radio Technical Commission for Aeronautics (RTCA) DO-254 / DO-178 design process. They are delivered with certification artifacts that support their successful certification of the aircraft. A significant part of these certification artifacts are re-used across multiple programs, reducing cost and development time. Leveraging proven safety certifiable COTS building blocks has proven to reduce program risk and development schedules, right up to the highest, most critical safety certification levels.

Top-Down Approach to Safety at the System Level

Mercury's Avionics certifiable building blocks use a COTS model to identify the processing requirements of each building block. Each building block efficiently addresses a fundamental processing sub-function. Through subsequent integration of these interoperable building blocks, complex safety certifiable processing subsystems are quickly and affordably designed. We leverage a top-down approach that addresses how each individual building block will work together, without compromising safety. Specific mechanisms, such as time synchronization, specific bus topology and segregation. are all designed within a pre-defined, interoperable and proven safety ecosystem. This holistic design approach removes the inefficiencies of the traditional safety design doctrine and instead builds in inherent safety that is scalable, highly interoperable and proven.

Each Mercury safety certifiable processing building block is designed in compliance with DO-178 / DO-254 building safety in with an overall system level perspective. Our Avionics Series safety certifiable building blocks address most avionic systems requirements including avionic I/O to control actuators and gather data from sensors, processors to assess the situation, make decisions, give commands and video processing to capture, overlay, encode, decode, stream and display visual data.

Reducing the Total Cost of Ownership



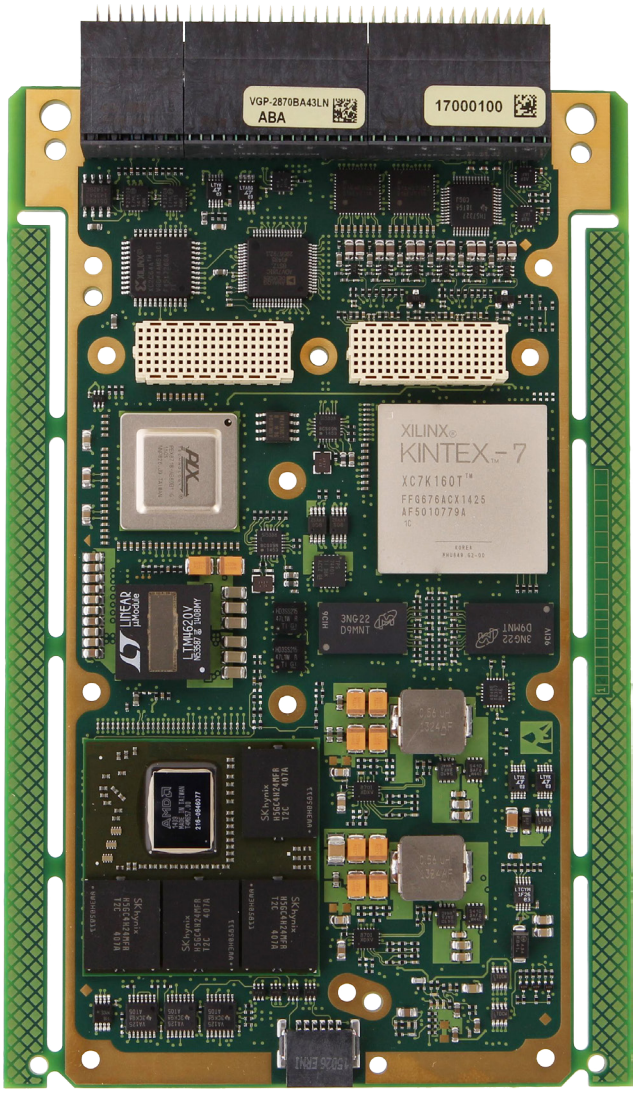
An important aspect of developing safety certifiable building blocks is the ability to support long services lives. There should be robust provision for future technology insertions that fully consider the implications of safety recertification. As an example, a safety certified processing solution may be initially designed with processor A and later upgraded to processor B for higher performance or perhaps greater power efficiency. To lower the overall cost of ownership, the tech insertion should be performed without having to repeat the whole certification process.

The upgrade of a certified system without re-certification is not trivial. Whereas I/O such as ARINC 429 and MIL-STD-155 have been largely static in terms of upgrades for generations, processors are much more dynamic. Mercury's safety building blocks enable easier tech refreshes by mounting often refreshed technology (e.g. processors) on mezzanine platforms. Such an approach enables tech refreshes to be recertified at a mezzanine level rather than at a more complex system level.

Safety by Design

The most important aspect when designing safety certifiable COTS building blocks is that safety must be built-in by design, from the start. In other words, the design process of a safety certifiable COTS building block must follow DO-254 / DO-178 process respectively for hardware and software. It is extremely difficult, if not impossible, to build-in safety retroactively if the design has not started out with safety considerations in mind.

There are a number of design considerations that need to be taken into account right from the start when developing COTS safety processing building blocks, including:



Determinism

Safety critical products must have a deterministic behavior. Determinism is more important than pure performance. A system can be optimized to transmit a data packet in a minimum amount of time, but if it is a minimum amount of time in 99% of the cases and a very long time in the remaining 1%, that would compromise the strict order in which operations are performed. Potentially a decision could be made based upon outdated information which can lead to dramatic consequences in safety critical applications.

Component Selection

Components are selected carefully. The complexity of components must be reduced to a minimum. For example, components with a state machine will be privileged over components with a CPU executing a firmware. In any case, certification evidences must be available for the selected components. This requires working closely with suppliers to understand their plans and roadmaps to support certification.

Fault Tree Analysis

Fault tree analysis is obvious but crucial to know which part of a system contributes in which way to the probability of errors.

Error Detection

Equally important to avoiding errors is the system ability to detect errors when they do occur. If errors cannot be avoided, they must be detected so they can be overcome by system redundancy to increase safety.

An example of this is witnessed when a display projects Hazardously Misleading Information (HMI). If a display stalls and displays misleading information, the operator must be informed that it is stalled in order not to rely false data (e.g. false altitude level while in reality the aircraft is already changing its height.

Data Requirement List

Developing processing subsystems for flight safety certification is more than hardware and software. A major part of the safety development effort is required to document the process. These documents, called artifacts or Data Requirement List, are required to prove to a certification authority that the overall system has been designed according to a process, which leads to a safe system. As a result, all of the system requirements need to be documented: - these requirements need to be traced throughout the system development. Any change to these requirements also needs to be documented and traced, as well as the consequences of these changes.

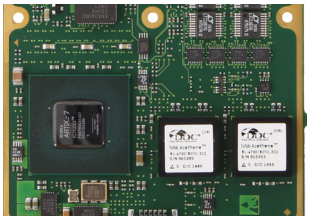
Quality Management

A well-developed quality management system has to be in place. It must be able to monitor the safety development process and deal with changes that may be subsequently required.

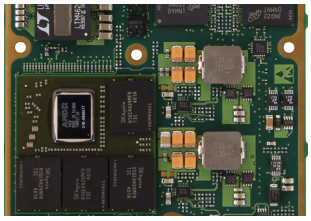
Relying on the Right Partner

There are two other essential ingredients required for low risk safety processing certification - expertise and experience. Engineers with the skill and experience reduce safety design development risk.

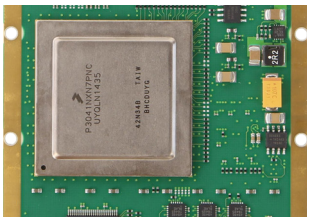
Mercury has decades of experience designing boards and systems deployed in applications certified up to the highest level of design assurance, DAL-A, for both DO-254 and DO-178. Years of products in service in safety critical programs have shaped our development process when it comes to designing products supporting safety critical applications. All this expertise and experience is built into our series of safety certifiable COTS building blocks dedicated to computing, avionic I/O and video. We have designed these building blocks with a top-down approach and are using them in ROCK-2: our modular full-featured safety certifiable packaged COTS system.



AVIO-2353
Safety Certifiable 3U OpenVPX™
avionic I/O Board



VGP-2870
Safety Certifiable 3U OpenVPX™
video I/O graphics processor



MFCC-8558
Safety Certifiable NXP QorIQ ™ T2080
processor XMC

ROCK-2A
Development platform for Safety
Certifiable applications

ROCK-2
Safety Certifiable packaged COTS system

3268.00E-0117-wp-safety

mercury systems™

INNOVATION THAT MATTERS™

MERCURY MISSION SYSTEMS INTERNATIONAL S.A.
Avenue Eugène-Lance 38, PO Box 584
CH-1212 Grand Lancy 1 • Geneva – Switzerland
+41 (0)22 884 51 00

CORPORATE HEADQUARTERS
201 Riverneck Road • Chelmsford, MA 01824-2820 USA
(978) 967-1401 • (866) 627-6951 • Fax (978) 256-3599