Civil Certification of Multi-core Processing Systems in Commercial Avionics

David Radack, Principal Software Architect
Rockwell Collins
Cedar Rapids, IA
Dave.Radack@rockwellcollins.com

Harold G. Tiedeman, Jr, Fellow
Rockwell Collins
Cedar Rapids, IA
Harold.Tiedeman@rockwellcollins.com

Paul Parkinson, Principal Systems Architect
Wind River
Swindon, United Kingdom
Paul.Parkinson@windriver.com

Introduction

Many years ago, the first certified civil avionics software systems were monolithic, hosted on single core processors. Rockwell Collins provided industry leadership in developing and certifying a multi-partitioned operating system that allowed multiple functions of varying design assurance levels (DALs) to safely execute on a single processor. This technology is mature and certified in operational service on dozens of aircraft types, including both civil and military aircraft. Today, Rockwell Collins is again providing industry leadership by certifying a multi-core processing platform that robustly executes multiple functions with mixed DAL assignments on multiple cores within a single system-on-chip (SoC) processor.

This step is the next logical evolution of processing systems, improving processing system performance and efficiency through increasing levels of integration within single devices. This integration has recently included the incorporation of multiple processing cores within the same processor device. Through an iterative trade study and experimentation process, Rockwell Collins chose to pursue certification of multi-core processing with the Freescale/NXP QorIQ® Power Architecture processors: first, with the P3041; and finally, with the T2080. These processors provide a significant level of performance increase, while not significantly increasing power consumption and providing valuable features to support safe and deterministic integration across all cores.

What is unique about Multi-core Processors

The introduction of multi-core processor (MCP) architectures has provided performance gains for enterprise general-purpose applications; it has also presented some unique challenges for their use in safety-critical avionics systems. Avionics applications often have specific requirements, including, but not limited to, application isolation and determinism. These are not the primary considerations of semiconductor manufacturers when designing MCPs for the commercial market, which typically push for best average performance.

Research undertaken by academia, the avionics industry and safety certification authorities has found that there is variation between MCP designs. These variations can affect their suitability for use in avionics applications due to the impact of architectural design features on application isolation and determinism. For efficiency, MCP designs include shared resources on the device, such as a single memory controller or shared bus used by multiple cores (providing a risk of resource contention), and shared use of Level 2 caches between cores (Figure 1). As a result, the execution of multiple applications simultaneously on different cores may result in multi-core interference. This complicates the analysis of behavior and worst-case executing timing (WCET) of applications.

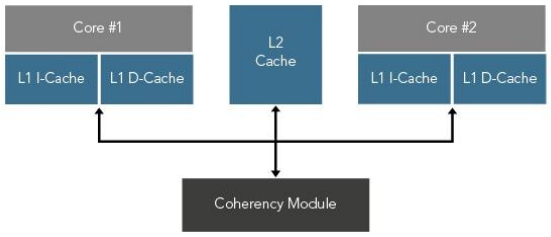

Figure 1. Notional multi-core cache architecture with shared L2 cache

The increased levels of integration on MCP system-on-chip (SOC) designs provide more components integrated into the device, which simplifies board layout design and can help reduce the physical footprint. However, this can increase the complexity of on-chip interactions, as multiple processor cores share peripheral interfaces. Hardware analysis of these interactions is dependent on the availability of proprietary design information from the semiconductor manufacturer; if this is not available, it may be impossible to completely understand the device's behavior.

Relationships and industry involvement

Rockwell Collins addressed these multi-core challenges in our certification approach through a series of strategic actions integrated into the process.

1) Worked closely with OEM, civil, and military certification authorities to help them understand these issues and our approach to address each one.

2) Established strategic proprietary relationships with operating system (OS) and SoC vendors, partly through contributions to the Multi-Core For Avionics (MCFA) working group.

3) Aligned our certification plans with the certification considerations described in the EASA multi-core certification review item (CRI) and FAA CAST-32A position paper.

4) Engaged internal experts who first certified multi-partitioned systems to make the leap to multi-core systems.

5) Recruited the team in the certification office and our on-site program certification liaisons to help guide our efforts.

Selecting the right processor

Rockwell Collins undertook a multi-disciplined trade study for the selection of the processor. This trade study evaluated historical support for civil certification and associated risk, available service life, availability of DO-178C DAL A RTOS, and architectural features such as virtualization support, on-chip network performance, and the type and independence of peripheral controllers. Initially the team selected the Freescale/NXP P3041 SoC, but the subsequent availability of the NXP T-series processors resulted in a re-evaluation of this decision. The team's selection of the NXP T2080 SoC took into account data collected from the P-series processors and the architectural improvements found in the T-series parts. Its advantages include better core performance, including e6500 core integer and floating-point performance, dual-threading at no additional power, internal SoC features, and a reset of the clock on product availability. The T-series SoC improves upon P-series multi-core design features including interference reducing performance in the SoC interconnect fabric, networking support, and additional IO controllers.

Most important requirements for a safety critical operating platform

Rockwell Collins defined the following requirements for a safety-critical virtualization platform for the T2080 multi-core platforms:

1) *Multiple guest operating system support*
A most important requirement was support for hosting multiple guest operating systems (GOS) consolidated in a single platform. This open system architecture feature is particularly important to enable Rockwell Collins and its customers to reduce system integration costs. This attribute is critical to preserve investments in millions of source lines of code (SLOC), design assurance evidence, and decades of application software development.

2) *Single platform for DO-178C applications spanning the spectrum of design assurance levels (DAL)s*
To enable Size, Weight, and Power (SWaP) efficient processor utilization, the virtualization platform must support DAL A through E, co-existing on a single multi-core processor. This feature allows existing applications to be hosted, without concern for the behavior of other applications, executing in other partitions, and extending that onto all cores of the SoC.

3) *Efficient Virtualization Support*
Rockwell Collins desired a very thin, highly configurable platform that took advantage of virtualization and configuration features of the hardware.

4) *Open standards APIs*
Customers required support for open standards such as POSIX, ARINC 653 and FACE™.

5) *Flexible Business Model*
The business model needed to support a product line approach, having an open licensing model to support multiple different products (multi-function displays, control display units, mission computers, etc.) and multiple customers with no additional licensing overhead required.

6) *Support DO-178C Certification*
The perceived DO-178C certification risk needed to be low, allowing an incremental certification step from our existing multi-partition OS approach.

Selecting the right OS platform for multi-core certification

In 2002, Wind River® started developing VxWorks® 653 based on the VxWorks real-time operating system (RTOS) to enable the development and deployment of ARINC 653-compliant applications using an Integrated Modular Avionics (IMA) software architecture.

This approach has enabled multiple applications, which had previously been deployed using a federated architecture comprising many separate Line Replaceable Units (LRUs), to be migrated into an IMA architecture comprising a reduced number of common computing platforms. The adoption of IMA has enabled an overall reduction in SWaP requirements, reducing aircraft weight and providing options and operational benefits in relation to fuel load and payload.

VxWorks 653 enables different types of applications to run within individual partitions – including ARINC 653 APEX processes, POSIX threads, VxWorks tasks, and/or Ada tasks. Wind River has also created commercial-off-the-shelf (COTS) DO-178 certification evidence packages for VxWorks on multiple specific processor architectures in response to customer and market requirements. These COTS certification evidence packages have increased affordability by enabling the cost of DO-178 certification to be amortized across multiple customers and programs.

Wind River actively participates in the ARINC 653 committee and contributes to the evolution of the ARINC 653 software standard. Wind River is also an active member of the Future Airborne Capability Environment (FACE™) Consortium, and VxWorks 653 was the first operating system to achieve conformance certification for the FACE Operating System Segment (OSS) Safety Base Profile. Wind River's support for open standards enables the development of portable applications and enables interoperability across a wide range of industries, processors, and application platforms.

In 2014, Wind River began the development of the *VxWorks 653, Multi-Core Edition*, to support multi-core processor architectures. The development program had the following high-level goals:

- *COTS RTCA DO-178C DAL A certification evidence*
- *Support of multiple DALs on multiple cores*
- *Perform fault isolation and containment (health monitors)*
- *Perform static configuration and enforcement as per ARINC 653*
- *Enable IMA role-based development and delivery as per RTCA DO-297*
- *Robust partitioning of application and OS environments for ease of updates and reduced certification burden*

These high-level goals enable the VxWorks 653 multi-core platform to support a broad range of customer use cases in both avionics and non-safety-critical environments.

Wind River chose a Type-1 (native) hypervisor-based approach because it provides the ability to control multiple processor cores via lightweight supervision that doesn't adversely impact system performance. The hypervisor-based approach also utilizes full hardware virtualization assist that is available on many modern multi-core

processors. This VxWorks 653 robust virtualization platform is validated on the latest Arm, Intel, and PowerPC architectures.

The hypervisor enables operating systems to run as unmodified virtualized guests at lower processor privilege levels. This provides the ability to host previously developed applications and third-party OS on the multi-core platform, enabling consolidation of applications onto a common processing platform (Figure 2). This reduces program migration and platform lifecycle costs when compared to using multiple traditional federated line-replaceable units (LRUs). This approach enabled Rockwell Collins to host multiple guest OSs on VxWorks 653, thereby enabling reuse of previously-developed and certified applications.

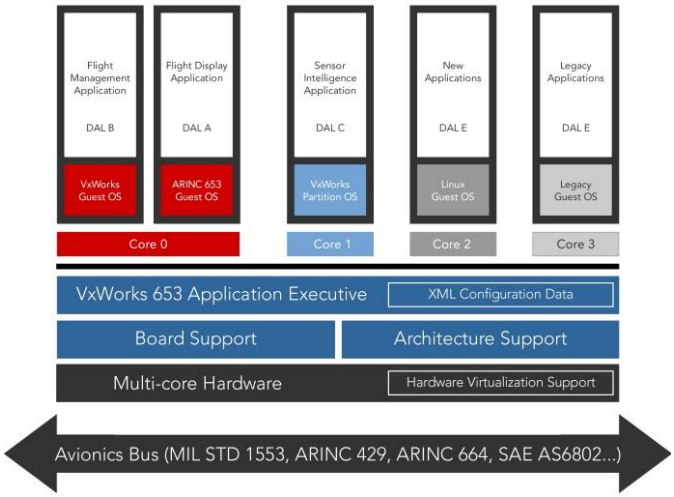

Figure 2. VxWorks 653 Multi-Core Edition architecture

The VxWorks 653 Platform also enables IMA role-based development according to RTCA DO-297 through a process known as independent build link and load (IBLL). This provides the ability to configure and initialize an IMA platform using a single configuration vector (CV). This approach enables platform providers, application developers and system integrators to collaborate according to role separation, and also reduce the impact of change, as system and partition configurations can be changed without rebuilding, re-testing, and re-certifying the entire application or platform. This approach significantly reduces the impact-analyses burden when upgrading and modifying an existing system, and can therefore dramatically reduce the cost of incremental certification and the total cost of ownership (TCO) over the life of the platform.

CAST-32A compliance

The Federal Aviation Authority (FAA) and European Aviation Safety Agency (EASA) have not yet published official policy or guidance on the use of multi-core processors, as research into use of multi-core processors in avionics systems is ongoing. However, the FAA Certification Authorities Software Team has published Position Paper CAST-32A guidance for multi-core processors in 2016. This CAST-32A paper was written by representatives from certification authorities in North and South America, Europe and Asia. CAST-32A defines a number of objectives that must be met by an avionics developer using a multi-core processor.

Table 1 provides an overview of CAST-32A by paraphrasing the objectives and providing some interpretation on the rationale for each.

CAST-32A objectives address system-wide safety concerns, which therefore means that CAST-32A compliance is not the sole responsibility of the hardware supplier or operating system supplier. Instead, the domains of hardware, operating systems, platform software, application software, and system integration are all intimately involved with CAST-32A compliance. This requires a coordinated approach to ensure all aspects of the CAST-32A objectives are appropriately satisfied.

In order to reduce DO-178C multi-core certification risk, Wind River has collaborated with Rockwell Collins on an FAA Program of Record for the development of the COTS DO-178C DAL A certification evidence for VxWorks 653. This approach has provided early validation of the VxWorks 653 software architecture and proposed approach to multi-core certification, through Stages of Involvement (SOI) audits covering the DO-178C process.

Table 1 CAST-32A Objective Overview

Objective	Why It's Important
MCP_Planning_1: Plans identify MCP SW architecture (including dynamic and IMA aspects)	Provides the overall system design context for the certifying authority
MCP_Planning_2: Plans provide a high-level description of how MCP shared resources and dynamic features will be used and how the applicant intends to allocate and verify the use of shared resources	Shows the applicant has thought through critical multi-core issues that could impact the execution of the application software
MCP_Resource_Usage_1: The applicant has determined and documented the MCP configuration settings	MCP's are extremely complex and likely have configuration settings that could negatively impact system safety
MCP_Resource_Usage_2: The applicant has planned, developed, documented, and verified a means that ensures that in the event of any of the Critical Configuration Settings of the MCP being inadvertently altered, an appropriate means of mitigation is specified	Configuration settings could be inadvertently modified by software errors or single event upsets in ways that result in undefined behavior if not mitigated
MCP_Resource_Usage_3: The applicant has identified the interference channels and has verified the means of mitigation of the interference	Interference channels are a source of jitter and performance degradation and may have significant, negative impact on the determinism of the processing system
MCP_Resource_Usage_4: The applicant has identified, allocated, and verified the available resources of the MCP and of its interconnect are sufficient to meet the demands of the integrated software	MCP shared resources could be oversubscribed by the full collection of hosted software, resulting in degradation of expected functionality
MCP_Software_1: Verification that all the hosted software components function correctly and have sufficient time to complete their execution when all the hosted software is executing in the intended final configuration	Software applications running simultaneously on different cores impact each other's execution timing and need to be integrated together to understand the impacts to operational behavior
MCP_Software_2: Verification that the data and control coupling is correct during software requirement-based testing	Data and control coupling across cores is more complex than coupling across partitions on a single-core processor and may result in unintended behavior if not verified to be correct
MCP_Error_Handling_1: Identification of the effects of failures that may occur within the MCP and plan, design, implement and verify means by which to detect and handle those failures in a fail-safe manner	The high level of integration of device functions and peripheral interfaces typically found within multi-core SoC designs drives a need for more built-in-test and monitoring for desired behavior
MCP_Accomplishment_Summary_1: The applicant has summarized in their SAS, HAS or other deliverable documentation how they have met each of the objectives of this document	Provides a reference for the evidence developed to build assurance that the MCP system design is appropriate for safety critical use

The DO-178C certification process involved defining the compliance of VxWorks 653 against CAST-32A objectives in the Plan for Software Aspects of Certification (PSAC), and where partial compliance is claimed against an individual objective, the responsibility of the platform provider for applying for full credit is defined. The Wind River DO-178C certification evidence package provides guidelines on how to configure and operate the VxWorks 653 environment in a deterministic manner in order to mitigate the potential multi-core interference channels identified in the Robust Partitioning Analysis (RPA) and Software Vulnerability Analysis (SVA). In addition, a set of requirements-based tests are used to verify robust partitioning capabilities on the customer avionics platform.

Military airworthiness authorities are also finding the same multi-core safety concerns and certification considerations are applicable to their domains. Rockwell Collins has been meeting with US Army AED/SED/AATD and US Air Force airworthiness agencies since 2013 to discuss multi-core issues related to safety certification, and Rockwell Collins has received positive comments from each organization regarding our CAST-32A approach. Rockwell Collins has incorporated feedback from the airworthiness agencies to optimize our methods and techniques over time.

Multi-core Certification Approach

Rockwell Collins has a multi-faceted approach to attaining safety certification with a multi-core processor. The main engineering effort is in complying with the certification considerations and objectives published in the FAA CAST-32A position paper. The first steps of CAST-32A compliance lay out the plan for meeting its objectives. Formal documents such as the DO-178C Plan for Software Aspects of Certification (PSAC) and the DO-254 Plan for Hardware Aspects of Certification (PHAC) capture this plan. A clear and concise matrix is used to allocate the ten CAST-32A objectives to the various hardware, software, or system integration activities and/or artifacts that will provide compliance evidence.

System development proceeds in parallel with the multi-core specific activities, which can offer feedback to the system requirements for multi-core specific features that need to be implemented to satisfy determinism concerns. Five critical analysis activities are performed to address a majority of the CAST-32A objectives. These analysis activities are:

1) Configuration Analysis
2) Interference Channel Analysis
3) Partitioning Analysis
4) Shared Memory Analysis
5) Errata Analysis

The Configuration Analysis establishes the critical SoC configuration settings that determine the processing capability available for applications. These settings can affect the operation of the processing cores, the resources allocated to each core, the operation of SoC peripherals, and the SoC utilization of shared resources. The usage domain for the system is taken into account while establishing the appropriate configuration settings in order to achieve determinism and maximize performance. Changes to these critical settings could change SoC behavior such that software executing on the SoC may no longer meet its requirements. The Configuration Analysis also describes a strategy to protect the system from inadvertent modification of these configuration settings.

Resource sharing creates the potential for interference that may affect the software applications executing on one of the processing cores. Interference Channel Analysis is what quantifies the interference impact. Starting with the configuration settings identified in the Configuration Analysis, the processing environment is reviewed and sources of interference are identified. Rockwell Collins developed tests to exercise each type of interference and to measure the impact of that interference on an application's execution time. Specialized tools are used to generate interference levels higher than would be seen in normal operation. The intent is to expose the software to potential fault situations from

other applications in order to ensure appropriate levels of system function availability. The results characterize the worst-case execution time for a given application. This in turn is necessary for the system integration process to allocate processing resources in the software execution schedule.

Partitioning Analysis verifies the time, space, and resource partitioning of the software architecture. There are potential situations where an event related to one application may consume part of another executing software application's allocated processing time. For example, an interrupt may be triggered during an application's execution frame. The time spent handling that interrupt must be well understood and bounded in order to ensure the executing application is still able to meet its deadlines. Partitioning Analysis identifies and measures any event that affects execution time. Resulting information is used for scheduling during the system integration process.

Shared Memory Analysis identifies all uses of system shared memory and ensures that the software architecture results in robust behavior. The shared data structures are analyzed to show deterministic communication is provided. Potential software problems such as race conditions, data starvation, deadlocks, and livelocks are avoided through this analysis.

The Errata Analysis studies the multi-core processor errata to determine the maturity of the platform, as well as to address any reported problems with the SoC. Hardware and software engineers review the errata data provided by the processor vendor. For each erratum applicable to the usage domain of the product, mitigation actions are determined and implemented.

The results from this set of analysis is captured in an artifact we call the Determinism Analysis Document (DAD). The DAD provides the basis for system level analysis performed by applications developers and integrators. It is used to develop a system level configuration which guarantees deterministic behavior.

Some CAST-32A objectives are satisfied through system functionality, such as Health Monitoring and Built-In-Test. In these cases, the related hardware or software component artifacts such as requirements, or design data, are updated with multi-core specific functionality and verified through requirements-based verification.

Rockwell Collins captures CAST-32A objective evidence in the DO-178C Software Accomplishment Summary (SAS) and the DO-254 Hardware Accomplishment Summary (HAS). Again, a matrix is provided as the mechanism to present the data. In this way, the PSAC/SAS and PHAC/HAS provide the bookends for the CAST-32A compliance.

Summary

Rockwell Collins and Wind River efforts in the certification of the T2080 processor are nearing completion. Rockwell Collins has obtained concurrence from our internal certification liaisons that the multi-core certification plans and accomplishments in SOI 3 (verification and validation review) meet the necessary objectives for CAST-32A. Operating system suppliers, including Wind River, have completed their requirements for SOI 4 (final certification review). Rockwell Collins will submit System SOI 4 for TSO later this year, with FAA acceptance expected in early 2019.

Rockwell Collins is also developing integration guides and toolkits to support third party software integration and certification. The cornerstone of this support is the Determinism Analysis Document (DAD), tailored to a customer's avionics platform and usage model. The third party tools include excitation, measurement, and analysis software and methods. These provide customers with the ability to achieve system level objectives related to CAST-32A and multi-core certification of the processing platform executing application software.