WIND™

Certification of Avionics Applications on Multi-core Processors: Opportunities and Challenges

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Developers of avionics systems are increasingly interested in employing multi-core processors (MCPs). MCPs are especially suited to the lower size, weight, and power (SWaP) consumption requirements of avionics systems. However, MCPs pose many more system implementation and certification challenges than do typical single-core or multiple discrete processor solutions. This paper is intended to provide guidance on the certification challenges of multi-core solutions, as well as an update on the work at Wind River® to develop commercial off-the-shelf (COTS) RTCA DO-178C DAL A certification evidence packages for VxWorks® 653 Multi-core Edition platform.

TABLE OF CONTENTS

THE CHALLENGE OF MULTI-CORE CERTIFICATION

Multi-core processors have delivered significant performance gains for general purpose enterprise applications over the last decade. However, their use in safety-critical avionics systems poses some unique challenges that have slowed adoption and deployment in this market. Avionics applications have specific requirements, in particular application isolation and determinism. In addition, developers need to ensure that multiple applications running on a single processor do not interfere with another application's performance, and that each will execute its designated tasks in the proper sequence at all times. Multi-core semiconductor manufacturers designing MCPs for the commercial market tend to optimize their processors for performance, not safety and isolation. Avionics system designers, therefore, need to expend considerable resources to ensure that selected processors are suitable for a safety environment.

Business Challenges

From a business perspective, avionics program managers need to address two key principles when undertaking certification for safety-critical applications:

- **Managing overall program risk:** The increasing complexity of embedded software in new avionics systems due to increased functionality, combined with the complexity of the development of new hardware platforms and system integration, presents a real challenge to avionics program and engineering managers. The adoption of multi-core processor architectures increases system complexity significantly, and the challenges of multi-core certification therefore increase program risk dramatically. Avionics suppliers will seek to minimize this risk at all levels of a new program, and one of the ways they can achieve this is by using a COTS software platform that has been designed from the outset for DO-178C DAL A/ED-12C DAL A certification on multi-core processor architectures.
- **Affordability:** In an era of increasingly constrained program budgets, the cost of undertaking safety certification on multi-core processor architecture is likely to be an important consideration. The use of an ARINC 653–compliant platform running on multi-core processor architecture provides the potential for hosting multiple applications at multiple DO-178C/ED-12C development assurance levels (DALs) on the same common processing platform. This approach to consolidation can help eliminate multiple line replacement units (LRUs), reducing hardware costs and the impact of hardware obsolescence, thus providing long-term benefits for a program.

  In addition, the use of a COTS DO-178C certification approach and COTS certification packages for an ARINC 653–compliant RTOS can also drastically reduce a program's DO-178C certification costs by amortizing the cost of certification of the RTOS across multiple programs, instead of an individual program having to bear the full nonrecurring engineering (NRE) costs. An ARINC 653–compliant RTOS that employs a modular architecture and supports the use of independent build link and load (IBLL) enables avionics suppliers to modify or enhance an application that is part of an already certified system and only retest and recertify the components that have changed, thus dramatically reducing the recertification costs of a platform.

Technical Challenges

From an architectural perspective, MCP designs vary widely in their suitability for avionics applications due to the impact of different architectural design features on application isolation and determinism. In some cases, shared resources on the device, such as the use of a single memory controller or one bus for multiple cores, raises the risk of "resource contention."

Uncertainty about the selection of multi-core processors for avionics projects presents a challenge for developers. The European Aviation Safety Agency (EASA) and the FAA have not yet published formal policies or guidance on multi-core certification. However, EASA's MULCORS research report and the FAA Certification Authorities Software Team's CAST-32A study (November 2016) outline issues that could impact the safety, integrity, and performance of MCP-powered avionics systems. Developers may refer to these studies when planning safety-critical multi-core avionics projects in order to reduce certification risk.

Avionics developers need to pay attention to two key tenets when seeking certification for safety-critical applications:

- **Core deactivation:** Even if expected processing requirements do not exceed that of a single core, developers of avionics systems might consider using a multi-core processor to ensure adequate capacity to meet future processing requirements. Similarly, some projects may call for four-core and eight-core processors, which are now relatively common. In either scenario, project teams will need to be able to use certain processor cores and deactivate the unused cores. The ability to deactivate

individual cores and demonstrate deterministic operation in safety-critical applications may depend on detailed technical information from the semiconductor manufacturer. Some manufacturers may make this information publicly available, while others may only provide certain levels of information under nondisclosure agreements. Core deactivation is an important requirement for obtaining DO-254 certification of airborne electronic hardware. Developers will need to ensure that the selected semiconductor manufacturer will provide access to the required information, even if they do not formally support DO-254 certification.

- **Multi-core interference:** Using MCPs in safety-critical avionics applications requires the ability to manage contention between cores for shared resources. In particular, developers need to consider whether potential interference paths will result in actual interference channels. Wind River, for example, conducted research to measure inter-core disruption on the QorIQ P4080 processor resulting from shared caches and memory controllers. The benchmark results demonstrate the potential interference paths for a specific processor architecture but do not necessarily reflect the actual interference channels that will occur in an avionics system, as this depends on the characteristics of the applications. Multi-core interference analysis, therefore, cannot be performed on the underlying operating system in isolation but needs to be undertaken at the system level, including the application. In single core, the results degrade in a predictable manner as the data sizes increase.

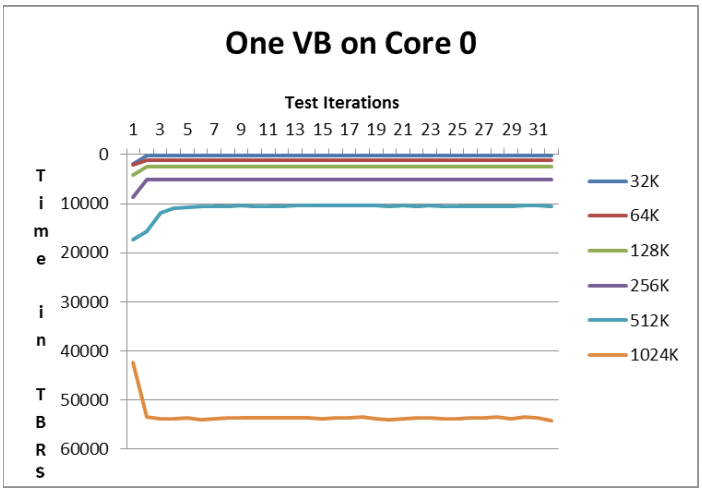
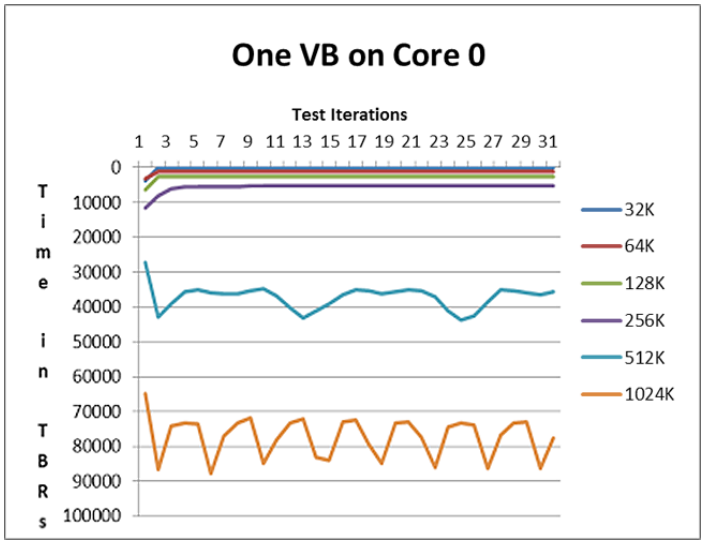


Figure 1. Cache perturbation results: P4080 unicore



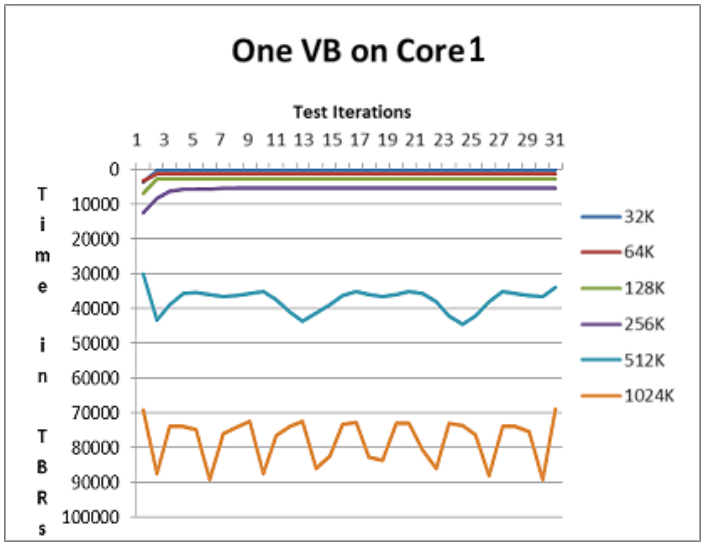


Figure 2. Cache perturbation results: P4080 dual-core and single memory controller

In dual core (same memory controller), the results become unpredictable once the data size overflows into the L3 cache starting at 512 KB.

The vertical axis indicates time in ticks measured by the PowerPC 64-bit Time Base Register (TBR), and the horizontal axis indicates the number of iterations of the benchmark that were performed.

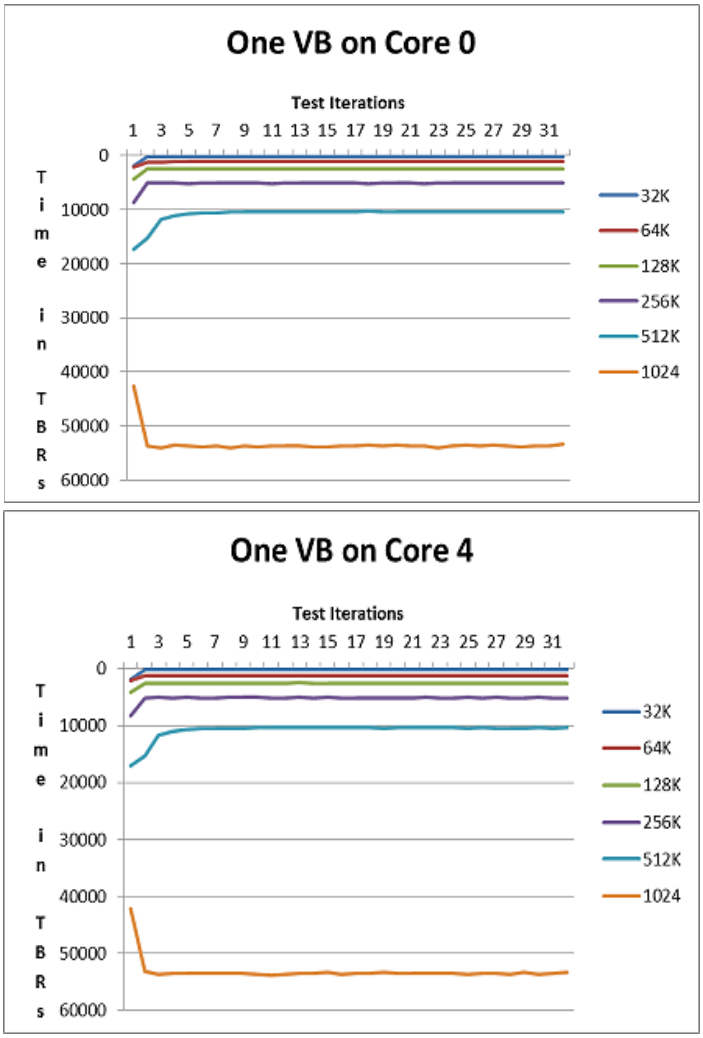


Figure 3. Cache perturbation results: P4080 dual core and separate memory controllers

CERTIFICATION OF AN ARINC 653 RTOS ON MULTI-CORE PROCESSOR ARCHITECTURE

ARINC 653 is the leading industry open standard for space and time partitioning in safety-critical applications in an integrated modular avionics (IMA) environment. Systems based on ARINC 653 have been widely deployed in commercial and military aircraft. Until recently, published ARINC guidance did not address the use of ARINC 653 in multi-core processor avionics systems. In view of strong market demand for support for multi-core, however, the AEEC APEX Subcommittee undertook the updating of ARINC 653 Part 1, Supplement 3 (ARINC653P1-3) to support the use of MCPs. Wind River collaborated closely with Tier 1 suppliers, system integrators, and other commercial off-the-shelf software suppliers in this industry effort.

The evolution of the standard resulted in the publication of ARINC653P1-4 in 2015 to support the use of MCPs. A key provision states that an application developed to run on a single core processor under ARINC653P1-3 should also exhibit the same behavior when running on one core on a multi-core platform under ARINC653P1-4. This preserves the investment of previously developed ARINC 653 applications when migrating to multi-core platforms.

ARINC653P1-4 also includes the ability to run an instance of a partition across multiple cores (known as a multicore partition). ARINC653P1-4 does not include the ability to support multiple partitions on each processor core but states that this capability may be added in a future update of the standard (currently planned for ARINC653P1-5 in about 2019). This concurrent execution capability will provide the potential for many scheduling configurations. However, the system integrator will need to ensure that the configuration of specific applications on a particular IMA platform will provide deterministic behavior, and that potential interference paths are reduced to the minimum number of interference channels.

WIND RIVER VXWORKS 653 RTOS MULTI-CORE REQUIREMENTS

For earlier releases of the VxWorks 653 real-time operating system, targeting single-core operation, requirements were defined in the software requirements specification (SRS) contained in the VxWorks 653 2.x DO-178B Level A certification evidence package for the respective processor architecture. For VxWorks 653 3.x Multi-core Edition, Wind River defined specific high-level goals for use in multi-core architectures. The product needed to:

- Support DO-178C Design Assurance Level (DAL) A avionics platform certification
- Support multiple DALs on multiple cores
- Perform fault isolation and containment (health monitors)
- Perform static configuration and enforcement in accordance with ARINC 653
- Enable role-based development as per RTCA DO-297

These goals were addressed and accomplished through the product design and certification strategy.

In order to achieve the high-level goals of support for safety certification of multiple applications at different DALs, VxWorks 653 Multi-core Edition RTOS needed to support isolation of applications running individual partitions through spatial, temporal,

resource, and multi-core partitioning. The RTOS design also needed to minimize the potential for multi-core interference paths where possible.

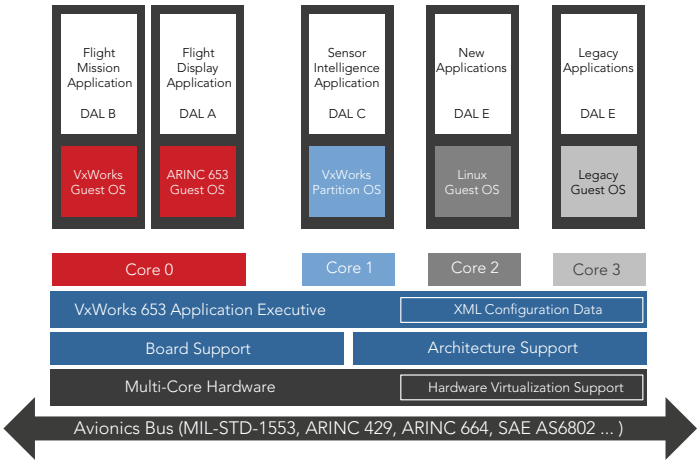


Figure 4. VxWorks 653 Multi-core Edition

DO-178C DAL A CERTIFICATION STRATEGY FOR VXWORKS 653 ON QORIQ

Since 2000, Wind River has developed and released COTS DO-178 certification evidence packages that organizations could use to support their platform and system certification programs. When COTS MCPs started to become widely available, customers asked Wind River to provide DO-178C certification packages on MCP processors, using multiple cores. Following publication of the EASA MULCORS research report and FAA CAST-32A position paper, Wind River developed its Plan for Software Aspects of Certification (PSAC) for VxWorks 653 3.x Multi-Core Edition on QorIQ T2080 at DO-178C DAL A.

Wind River released the COTS certification evidence package for VxWorks 653 Multi-core on the advanced PowerPC multi-core processor in June 2017, meeting the rigorous RTCA DO-178C and EUROCAE ED-12C DAL A requirements. This release adds the certification evidence package needed to comply with the FAA's safety requirements—designs, tests, reviews, source code, build files, test results, annotated object-level code coverage, and tool qualification data.

Wind River has worked with a lead customer and the FAA on an avionics program to gain early feedback from DO-178C audits on the design and certification approach, as well as guidance on application of CAST-32 guidelines from the certification authority. This approach presented lower technical risk, increasing the probability of successful completion of certification in shorter overall timescales.

FUTURE CHALLENGES

Although ARINC653P1-4 does not currently support concurrent execution of partitions, it indicates that this may be supported in a future update of the standard. This would enable more applications to be hosted on ARINC 653 systems, enabling further consolidation of avionics LRUs onto IMA common computing platforms.

The DO-178C certification of an ARINC 653 RTOS on other MCP architectures could present different requirements, as other architectures have different initialization sequences. For example, Intel® processors use a BIOS or Intel Firmware Support Package, which might require optimization in order to meet the AC2511-B startup time requirement for an avionics flight display and undergo DO-178C certification.

Finally, as ARM®-based system-on-chip (SoC) devices increase in processing performance, these may become an attractive option for an IMA platform, especially if DO-254 certification artifacts are provided by the semiconductor manufacturer.

CONCLUSION

The avionics market is currently undergoing a significant transition from single-core to MCP architectures, driven by demands for greater system functionality and the semiconductor product lifecycles that primarily target the much larger commercial market segments. Advances made by semiconductor manufacturers now give developers a much broader range of viable processor choices for avionics applications than were previously available. By working in close collaboration with application developers, system integrators, and certifying bodies, Wind River is helping the avionics community address certification obstacles in order to fully realize the benefits of multi-core solutions.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.