TECHNOLOGY WHITE PAPER

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

CURTISS-WRIGHT

DEFENSE SOLUTIONS

Read About

Safety certifiable multi-core vs single core

Safety certification challenges of multi-core processors

CAST-32 mitigation strategies

How to select a multi-core processor for safety certification

Info

curtisswrightds.com

Email

ds@curtisswright.com

Introduction

Safety certifications involve strict sets of guidance documents ensuring a high degree of safety in airborne electronics. Originally created for the commercial aviation industry, safety certification is now increasingly required on airborne military platforms. The need for size, weight, and power (SWaP)-optimization in deployed applications along with fast time to market has led to the use of COTS modules. However, COTS modules often employ highly integrated, multi-core processors with many more features than previous generations of single-core counterparts. This complicates the safety certification process significantly, as the shared resources inside multi-core processors can be more difficult to identify and verify. How can COTS modules meet the mandatory safety certification requirements? We examine the challenges and solutions to certifying multi-core computers for use in military embedded airborne platforms.

COTS in Avionics Platforms - Multiprocessor vs. Multi-core

Traditionally, embedded airborne platforms were custom-built, self-contained units. These modules were designed with well-known single-core processors, which made verification of their internal mechanisms for safety certification less complicated. Because of their transparency, these units could be certifiable up to the most stringent level available - Design Assurance Level A.

In recent years, however, the push for lower cost, SWaP-optimized systems has resulted in the use of multi-core processors in embedded airborne platforms. In contrast to their single-cored predecessors, multi-core processors are highly integrated, with 1-8 or more cores, giving avionics applications a power-saving processing boost.

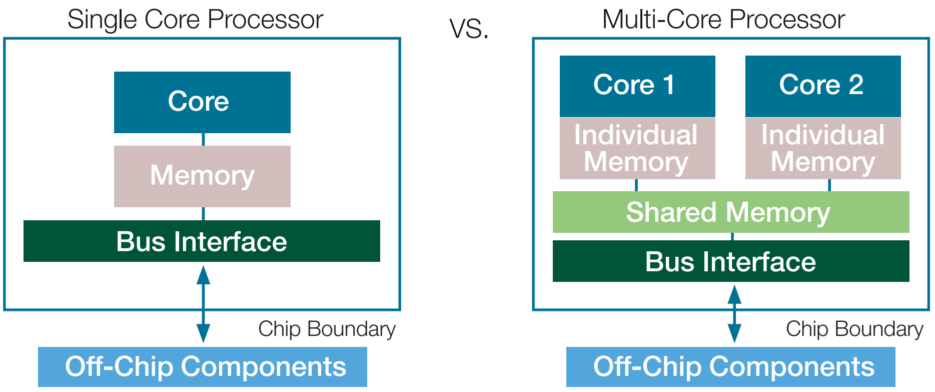

Figure 1: Single Core Processor vs. Multi-core Processor

Multi-core applications generally require less hardware to provide the same, and more, functionality than single-cored systems. In addition to performance benefits, multi-core processors offer a long-term solution to the anticipated upcoming obsolescence of single-core processors in the electronics market. Note: Many COTS vendors (Curtiss-Wright being one) also offer long term support (longevity of supply) and pin-compatible technology insertion for their products, protecting the customer from what can be an expensive upgrade as technology advances.

While COTS multi-core processor modules offer performance, time to market, and reduced risk benefits to the user, they also present unique challenges for safety certification. The highly-integrated nature of multi-core processors means they are not easily evaluated or verified. Multi-core architecture may be difficult to access, additional features could cause a loss of data integrity, and multi-core processors in general were not designed for compliance with the existing safety certification verification processes. With the trend towards using multi-core COTS modules in airborne platforms, how will the challenges of verification and the necessity of safety certification be rectified?

Multi-core Certification Considerations

The use of multi-core processors in safety-/mission-critical systems has been intensively discussed in the Avionics community over the past five years. Several reports such as the *CAST-32 Position Paper, MULCORS – Use of Multi-core Processors in Airborne Systems*, and *COTS-AEH – Use of Complex COTS in Airborne Electronic Hardware – Failure Mode and Mitigation* have been developed by industry partners and authorities (FAA, EASA) worldwide in an attempt to offer viable solutions to the issue of multi-core DO-254 certification. The CAST-32 paper in particular was seen by the industry as too prescriptive. In the future, a less prescriptive guidance document may be written for individual projects; however the overall concerns and objectives as stated in the CAST-32 paper remain valid.

There are several considerations and challenges with multi-core processors that must be overcome to enable DO-254 certification. The importance of addressing these challenges is not lost on the military and defense industry. Currently, DO-254 certification efforts for multi-core systems focus on processors with only two cores. The following are some of the known challenges to the safety certification of COTS multi-core solutions and the possible strategies that can be used to mitigate them.

Determinism and Predictability

Deterministic behavior is a key requirement in safety certification. The MULCORS Study states that, “a system is deterministic as soon as its behavior is ruled by a set of identified laws” which must be compatible with safety certification requirements.[1] That is, to be deterministic enough for safety certification, a system must be extremely predictable. Complex multi-core technology may introduce a variety of non-deterministic system behaviors such as increased latency, jitter, decreased throughput, and one or both cores may experience lockout from shared resources. Because much of the verification in the safety certification process requires that modules meet an acceptable level of Worst Case Execution Times (WCET), these behaviors may result in a module’s ineligibility for certification.

Challenge: Shared Resources

While single-cored systems traditionally used dedicated hardware for one application or function, multi-core systems allow cores to share different resources such as memory, system level cache, and interconnect. Although memory sharing lends itself to better performance, it is possible for the memory bandwidth to experience a bottleneck, thus preventing applications from obtaining the data they need, and affecting WCETs. Software operation can also be impacted if one core locks out software running on another core from accessing shared memory. Similarly, two cores sharing the same cache may lead to data integrity issues. In fact, multi-core studies have discovered increased WCETs for one core’s software when the other core repeatedly accesses shared cache.[2]

Since a processor interconnect controls each core’s access to the shared memory and cache, it too is a key element in assessing deterministic behavior. Because interconnect is not typically developed by the COTS module vendor, it may have additional functionality and features that cause predictability issues such as jitter during data transfer, incorrect transaction orders, or services provided to the wrong requester. Not only that, as interconnect designs are highly competitive in the electronics market, manufacturers of interconnect may not always provide the required documentation, making it difficult, if not impossible, to analyze the interconnect for DO-254 certification.

Finally, multi-core processors have many more features that are configurable with registers and pins than single core processors. Some of these can be improperly set, changed, or even deactivate necessary components of the system. This can change the way the multi-core processor operates and cause unwanted interruptions. In addition, multi-core processors may have dynamic features such as energy-saving that are programmed to change the processor’s operation without any outside intervention. This is a concern for DO-254 certification, as these features can alter processes inside the cores, or even shut down parts of the processor, causing non-deterministic behavior during flight.

Mitigation Strategies: Shared Resources

There are several approaches a system designer can use to mitigate the effects of shared resources:

- Configure Resource Management. For example, a processor's shared cache can be divided and dedicated to cores to minimize access and data integrity issues. There are also multi-core architectures that do not use shared cache, but have dedicated cache for each core, which can eliminate this issue.
- Schedule Access to Resources. This method allows the processor scheduled access to a resource where no other interruptions can occur.
- Monitor the Access to Resources. System engineers can monitor how much a resource is used, and then grant or restrict access based on a pre-determined limit.

Since verifying shared resources is not currently part of the DO-254 certification procedure, several reports suggest mandatory 'safety net' solutions whereby applicants test and provide risk mitigation strategies that can be designed and implemented into multi-core processors, allowing them to be properly verified:

- Whether or not the multi-core processor has shared memory, and providing proof that the applicant has implemented and tested proper safety net methods of providing uninterrupted memory access for both cores
- Whether or not the multi-core processor has shared cache, providing data on the most detrimental effects the shared cache could have on the software, and demonstrating proof they have implemented a safety net strategy to lessen issues with the shared cache
- Detailed descriptions of how interconnect will be used and managed in the platform, the maximum capacity of the interconnect that will support deterministic behavior as well as evidence that the processor will not exceed this capacity while in flight, and proof that the WCETs will not exceed what is permitted for the safety certification process
- The exact settings that will be used for all types of features available on the multi-core processor, as well as proof these chosen settings will ensure both cores operate in a deterministic fashion. The applicant should also provide tested safety net mitigation strategies to deal with consequences should any of these settings be changed during flight

Challenge: Interference Channels and Hypervisors

The challenge of interference is related to shared resources. When multiple cores share cache, memory, and interconnect, the applications running on each of the cores are not executing independently. Applications are, in effect, 'coupled' at the platform level, and open to various possible hardware and software interference channels. For example, studies have shown the many additional features available in a multi-core processor can cause interference between applications operating simultaneously, and residing on different cores.[3]

These additional features can include not only shared memory, caches, and interconnect, but also operating systems with software or hardware hypervisors. A software hypervisor can enable virtualization that allows several operating systems to operate on separate cores. A hardware hypervisor enables multiple cores and multiple operating systems to work together, and helps control access between them. In addition, if malicious software attempts to access and/or overwrite configurations, the hardware hypervisor blocks it. However, hypervisors can cause unintended interference actions to occur, and are difficult to fully verify.

All these interference issues can lead to non-deterministic behavior such as data latency, data integrity loss, denial of access to data or peripherals, and problematic WCETs. There are currently no DO-254 certification guidelines to verify interference channels or hypervisors, and the number and complexity of these issues makes it extremely challenging to document all the possible execution scenarios.

As illustration of this challenge, interference channels have been observed during testing. Below is an example from *Leveraging Multi-core Computing Architectures in Avionics.*[4]

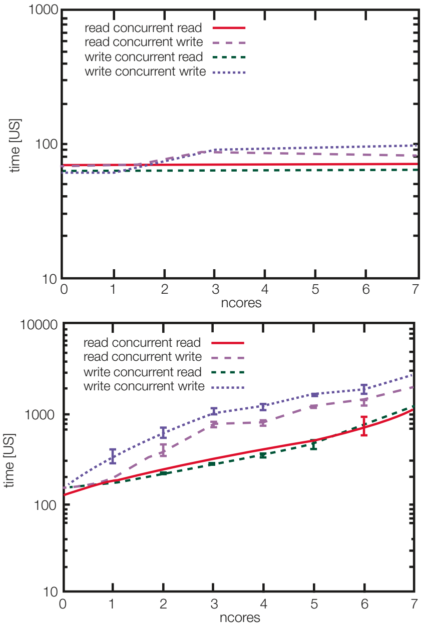

Figure 2: Dependency of read and write on read and write accesses from other cores for SRAM and DDR3 Memory

Mitigation Strategy: Interference Channels and Hypervisors

Apart from disabling one of the processor's cores (which would negate the module's SWaP benefits), the CAST-32 paper suggests the applicant can mitigate interference channel issues by providing DO-254 certification authorities with the results of a functional interference analysis, detailing any possible interference channels or features that are unique to multi-core processors. With this, the applicant must also provide a mandatory safety net mitigation strategy tailored to each interference channel identified, including methods of deactivating each interference channel.

To meet software hypervisor requirements, it is suggested that applicants clearly demonstrate how they are going to comply with the certification authority's guidelines, and show how they have tested their hypervisor strategies. To meet hardware hypervisor requirements, applicants need to demonstrate how they will verify the hypervisor's functionality, and provide proof that the hypervisor has been successfully verified.

Transparency of Design

Challenge: Lack of Publicly-available Data

Many of today's multi-core processor manufacturers are reluctant to make all the details of the inner operations of their processors publicly available. Given the inherent transparency of the verification process, the absence of this data makes certification impossible. To add to this complication, these are very complex devices, and as much as the processor manufactures attempts to verify against all possible use cases, there may still be latent faults in the device. Manufacturers must provide errata on design issues in their modules to be able to identify issues and creates fixes. However, all the errata for a given product may take years to be discovered and collected. This causes a problem for DO-254 certification in that, although the applicant may be very forthcoming and thorough in their application documentation, they may not even be aware of certain design issues that will affect safe operation of the module.

Mitigation Strategy: Lack of Publicly-available Data

In the case of architectural transparency, system designers need to choose processors made by manufacturers who are open about the inner workings of their architectures. Processors without this clarity of operation generally have a reduced chance of being accepted for safety certification, especially as the DAL level increases.

Mitigating errata, on the other hand, is a more complicated endeavor. The CAST-32 paper suggests that applicants should:

- Provide a detailed errata analysis on known issues (either from the manufacturer or from the applicant's use of the processor), and document how these issues may affect processor function and whether they have implemented the recommended resolution provided by the device's manufacturer
- Demonstrate the maturity of their chosen processor – how long it's been used in the field, frequency of new errata, the different applications is has been used with, etc.
- Provide proven, tested safety net mitigations for each of the known errata
- Provide strategies on how to mitigate newly discovered errata in the processor, should the need arise

Software

Challenge: Software Development and Verification

On traditional single-cored processors, software is restricted to operating on one core only, with a designated memory allocation, and any dynamic software features are either disabled or restricted. This configuration ensures the processor produces the desired deterministic behavior. With a multi-core processor, however, several types of software architectures may be used in parallel, in real-time, and on separate cores. Depending on the architecture type, a single operating system may be capable of dividing various software functions into threads that can execute in parallel on separate cores.[5] This capability calls into question the software's aptitude for partitioning, and consequently, for deterministic behavior.

There is currently no certification guidance material that details the development process for software on multi-core processors. Because of this, there is also no industry-wide standard on how to properly verify software used on multi-core processors. Without a tried and true standard, there is a chance that the applicants' approach for verifying two cores will not be sufficient to ensure deterministic behavior during flight.

Mitigation Strategy: Software Development and Verification

To avoid the dynamic allocation of threads to different cores, system designers can implement an Asymmetric Multiprocessing software model. This allows each core to run an independent instance of the operating system, locking tasks or threads into a single core.

In addition, to properly verify software installed on multi-core processors, the CAST-32 paper suggests that system designers should integrate and test the software with the desired hardware first, then individually integrate each application for additional testing with the operating system. After this is complete, the overall system operation may be verified. This gradual approach is a current industry standard method of verifying software operation on single core processors that can also be applied to multi-core processors, providing that all software is integrated and tested on both cores. This testing method facilitates system designers finding the source of any errors that occur, allowing them to remedy any issues and ensure the processor exhibits the required deterministic behavior.

The following are some other mitigation strategies system designers should consider to help software on a multi-core processor become successfully certified:

- Provide details on the development and verification of all software installed on a given multi-core processor to demonstrate that all software together can operate deterministically.

- Provide proof that each individual software application that will run on the multi-core processor meets the current DO-178 requirements.

- Provide results from testing of software's access to shared memory, as well as any interfaces between software applications.

Technology Considerations

Some recent processors utilize technologies with gate lengths below 30 nm. These technologies need to be analysed for wear-out mechanisms and SEU/MBU sensitivity. A careful technology analysis must be performed before implementing such devices in high reliability or safety critical applications. On the other hand, new technologies offer lower power consumption, so this trade-off should be taken into consideration.

COTS Assurance Considerations

The AFE 75 Project[6] done by the Aerospace Vehicle System Institute examines COTS assurance methods. With both commercial and military segments of the airborne electronic hardware (AEH) market increasingly dependent on COTS components, sub-assemblies, and in some cases even systems, the aerospace industry needed consensus on methods to assure COTS-based system safety and airworthiness in Airborne Electronic Equipment (AEE). This includes criteria that assure that those methods are used properly in design, production or support. The AFE 75 project evaluates the current challenges posed by the use of COTS electronics modules in aerospace vehicles, as well as addresses major characteristics of the COTS electronics market, namely:

- The rapidity with which it changes

- The regular emergence of new issues that can affect AEE safety and airworthiness

Device Uprating

Device uprating (i.e. when a component is used beyond the manufacturer's stated operating limits) is often overlooked, but is a concern for safety critical applications. With regards to COTS modules, the AFE 75 project states: "Typical wear-out mechanisms in semiconductors are gate-oxide wear-out, electro migration and hot-carrier injection. These mechanisms can, to some extent, be accelerated by uprating. These and other wear-out mechanisms can be non-progressive and hence non predictable in time or in failure mode. Some unshrinkable parameters prevent the power supply voltage from proportionally scaling with the physical devices. Therefore, the process of technology scaling impacts the noise and voltage uprating for each new generation of COTS in a non-linear fashion."[7] The AFE 75 Project's position is that device uprating in safety critical modules should be avoided if possible. If it cannot be avoided, it should be done following the guidance given in IEC/TR 62240:2005.[8]

Additional Considerations for COTS Digital Airborne Electric Hardware Components

The guidelines and considerations given in the AFE 75 Project document apply especially for multi-core processors that are classified as highly complex COTS microcontrollers. These considerations were written to aid in the use of the components in certifiable systems. However, the following aspects should also be applied for mission-critical systems in airborne applications (i.e. Design Assurance Levels between DAL-C and DAL-D):

Device Data

To aid in the safety certification process of a COTS module, there should be identification and archiving of specific data corresponding to each COTS device. This should include, at the very minimum, the user manual, datasheet, device errata sheet, and installation manual (including the hardware/software interface and the explanation of activation/deactivation of COTS functions).

Usage Domain Aspects

Safety certification applicants must list the usage domain of each COTS module for the application, as well as demonstrate that the module is operated within the limits/recommendations established by the manufacturer. For example, the usage domain should identify[9]:

- Used functions (e.g. description of each function, configuration characteristics, mode of operation, control and monitoring during normal/abnormal operation)
- Unused functions
- The means used to deactivate functions
- External means to control any inadvertent activation of unused functions, or inadvertent deactivation of used functions
- The means to manage device resets
- Power-on configuration
- Clocking configuration (e.g. identification of the different clock domains)
- Usage conditions (clock frequency, power supply level, temperature, etc.)

Analysis of the component manufacturer errata sheets

DO-254 certification evidence should show:

- How the component manufacturer captures and maintains the list of errata and publishes it
- That the rate of occurrence of new errata from the component manufacturer decreases as a function of time. This is a criterion to determine the maturity of the component

Product Service Experience (PSE)

DO-254 certification applicants should document the following in their applications:

- The target market for each COTS module
- The specific environments (e.g. civil aircraft, military aircraft, space, telecom, automotive, medical, etc.) in which the operating experience of each module was gained and the related number of operating hours
- The total time that the component has been used (i.e. the number of execution hours and the usage duration in years)

For mission-critical components, the product service experience is noted as “sufficient PSE” if the following criterion is met. If the criterion is not met, then the product service experience is noted as “Low PSE”)

- [Hours in aircraft applications + safety applications + other applications] >105h

Performing this analysis requires a close exchange with the module manufacturer. Support for this exercise and willingness to disclose the required information must be agreed upon with the module manufacturer. Some manufacturers currently participate in the Multi-core for Avionics (MCFA) working group. Those manufactures know the requirements from the Avionics industry and commit to delivering portions of the required data. Module manufactures without this commitment should be excluded from use in Avionics equipment.

Multi-core SBCs: Number of Activated vs Deactivated Cores

The semiconductor industry is promoting increased computing performance by increasing the number of active cores being used. Considerations such as shared resources and software architectures prevent increased computing power from mitigating safety certification concerns, especially in the worst case scenarios.

Selecting a Multi-core Processor for Safety Certification

With the varied considerations and requirements for hardware and software DO-254 certification, it's important to choose a multiprocessor wisely. Not only are all the elements discussed above important, but the manufacturer and availability of documentation play key roles in easing the certification process.

When selecting a multi-core processor for safety certification, system designers should consider:

- Dealing with a manufacturer who has a proven, long term track record in the military and defense industry, and who will be willing and available to assist in any way during the entire certification process
- The availability of required documentation from the manufacturer
- Using an architecture that has the open, documented details on its inner operations and design as required by safety certification authorities
- The lifespan of the hardware and software, obsolescence issues, and the long term availability of component repair
- The availability of required information on WCETs, interconnect, shared memory and cache, peripherals, etc. for that multiprocessor

Author

Rick Hearn,
Product Manager,
Safety Certifiable Solutions,
Curtiss-Wright Defense Solutions

Conclusion:

Moving Toward Your Safety Certification

There is much debate surrounding the use of multi-core processors in safety certifiable applications. Several organizations have closely examined the challenges of multi-core processors and the associated mitigation strategies that would facilitate their successful safety certification. This white paper has provided some insight and guidance on the major issues at hand. Curtiss-Wright has years of hands-on experience with DO-254 certification of COTS graphics and single board computer modules. We not only provide you with the hardware and software your applications need, we also guide you through the DO-254 certification process. Using COTS modules in your DO-254 certified application not only speeds your time to deployment and reduces your program risk, but also reduces the cost of developing critical aviation applications on manned and unmanned platforms. Let Curtiss-Wright's 25+ years of experience as a supplier of embedded electronics ease your path to a successful certification process.

Learn More

Video: DO-254 Certifiable Computer Modules

White Paper: COTS and Safety Certifiability in the Military and Aerospace Industry

Safety Certification: DO-254/DO-278B

Product: VPX3-150

Product: VPX3-718

References

1. European Aviation Safety Agency (2012). MULCORS – Use of Multi-core Processors in Airborne Systems. Germany

2,5. Certification Authorities Software Team (CAST) (2014). Position Paper CAST-32. Multi-core Processors

3. Airbus Defence & Space. Open Architecture Platforms for Avionics Applications: Challenges in Safety Critical Systems and Possible Solutions

4. Multi-core Processors, COMPLETED May 2014 (Rev 0)J. Nowotsch and M. Paulitsch. Leveraging Multi-Core Computing Architectures in Avionics. 9th European Dependable Computing Conference (EDCC), pp. 132-143, 2012. doi:10.1109/EDCC.2012.27

6,7,9. AFE 75 Project: COTS AEH. Issues and Emerging Solutions Final Report, Version 1.0b. Federal Aviation Administration. 07 Oct, 2014. Retrieved April 25, 2016, https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/AFE75_COTS_AEH.pdf

8. Process management for avionics – Use of semiconductor devices outside manufacturers' specified temperature range IEC/TR 62240:2005