A Commercial Solution for Safety-Critical Multicore Timing Analysis

White Paper

The MASTECS project is developing a commercial timing analysis solution designed to enable the safe use of multicore processors in the automotive and avionics domains.

MASTECS

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

RAPITA SYSTEMS
A DANLAW COMPANY

Collins Aerospace

MARELLI

Contents

1. A certification-ready Multicore timing analysis solution

It is now possible to take your multicore avionics or automotive project through certification thanks to a pioneering new multicore timing analysis approach.

The MASTECS project has played a pivotal role in commercializing a new generation of multicore solutions:

- Timing analysis software tools
- Tool qualification and documentation to support certification and safety assessments
- Expertise for consultancy services to support the analysis of multicore timing behavior

This technology works by combining cutting-edge software analysis tools, interference generators, documents, processes and expert engineering services to assure the timing behavior of complex multicore processors.

Assuring the timing behavior of multicore processors has been a significant hurdle in achieving certification within the aerospace and automotive industries. Barcelona Supercomputing Center and Rapita Systems have collaborated with industry partners Raytheon Technologies and Marelli to develop a solution that is driven by industry needs and is already being deployed in real-world, commercial projects.

In this white paper we will examine both how this advanced technology works and how you, like our industrial partners, can certify your multicore project using the solution.

Avionics systems are using more and more multicore processors

About MASTECS

The MASTECS project was created to develop a commercial timing analysis solution designed to enable the safe use of multicore processors in the automotive and avionics domains.

2. Solving the multicore challenge

Certification standards like DO-178C (aerospace) and ISO 26262 (automotive) have kept pace with changes in safety-critical hardware by providing generic and relevant guidance regardless of software architecture, programming language, etc.

One of the most significant changes in embedded computing systems in recent times has been the adoption of multicore processors. With a higher density of silicon, these systems offer increased performance per unit area, which is critical to meet the needs of modern embedded systems. Their use comes at a price, as unlike single core systems, they offer neither a deterministic environment nor predictable software execution times.

To verify that an embedded system is robust, it must be demonstrated that the hosted software components function correctly and have sufficient time to complete their execution when operating in their multicore environment.

Multicore systems are much more complex than their single core counterparts. To understand how to verify their timing behavior, we must first understand the unique challenges inherent in the analysis. We've listed some of these below:

- Resource contention and interference: The execution time of a task in a multicore system is affected by contention for shared resources and the interference this causes. To investigate the timing behavior of a multicore system, we need to take this interference into account.
- Multicore timing analysis can't be entirely automated: The complexity of multicore processors means that building a fully automated timing analysis solution is unrealistic. While tool support can automate most of the data gathering and analysis processes, engineering wisdom and expertise is needed to understand the system and direct tool usage to produce necessary evidence.
- Test on the real hardware: Multicore CPUs are complex and often their internals are hidden, making purely analytical models of limited use in understanding their timing behavior. As such, the only way to determine exactly how the processor and its components behave is to measure timing behavior on the system itself.
- Assumptions must be tested: To analyze the timing behavior of a multicore system, a customer will need to make some assumptions about things such as the interference channels in the system and their effects. Those assumptions, however, need to be empirically assessed through a focused test campaign and likely adjusted based on the obtained evidence.

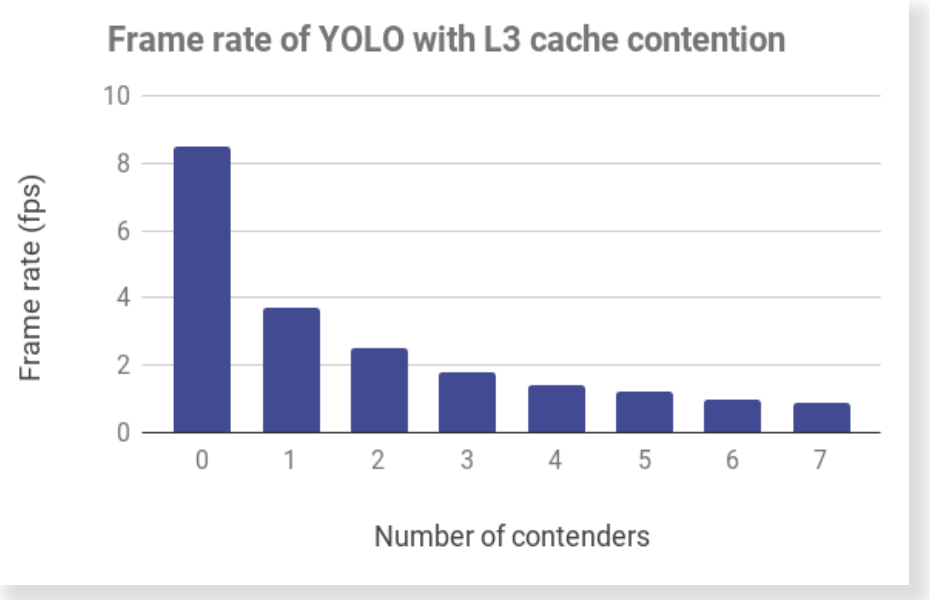
These challenges will be explored in detail in the next sections.

2.1 Resource contention & interference

The timing behavior of a task in a multicore system is affected not only by the software running on the same core and its inputs, but also by contention over resources such as buses, caches and GPUs that are shared with tasks running on other cores. This contention causes interference to the timing behavior of the task.

To demonstrate this, we will use the YOLO[1] real-time object detection software on an NVIDIA® Jetson® AGX board that has 8 NVIDIA Carmel cores. YOLO is an open source image recognition application that uses a neural network to identify and classify objects. The neural network calculations are performed on the GPU on the target board. To do this, the frame and neural network information are first loaded into memory and then pushed to the GPU for processing.

We measured the reduction in YOLO's frame rate when running YOLO on one of the cores while we applied sustained accesses on the L3 cache from tasks running on between 1 and 7 contending cores. The minimum frame rate from this series of experiments was almost a factor of 10 slower than when no contention was present, highlighting the importance of considering contention when analyzing the timing behavior of multicore systems.



YOLO frame rate data

[1] https://github.com/pjreddie/darknet

2.2 Multicore timing analysis can't be entirely automated

Timing analysis of single core systems can be entirely automated by using software tools such as Rapi**Time**, which analyze the worst-case execution time (WCET) of tasks running on the system.

This isn't the case for multicore systems, for which we must consider the effects of interference caused by resource contention on software execution times (see 2.1: We need to consider resource contention and interference). Interference effects are complex, interlinked, and involve components specific to both the multicore architecture and the scheduling and resource allocation systems in the software.

This means that, to properly perform the analysis, we need to apply the expertise of engineers who know the system in detail. While this expertise can be used to direct the use of software tools (for example specifying levels of contention to apply to specific resources), no automated timing analysis tool will be able to understand a multicore system in enough depth to perform the analysis alone.

2.3 Test on the real hardware

A measurement-based approach is necessary to obtain execution time evidence for multicore software. Static execution time analysis approaches are not suitable as they require highly detailed models of the processor that are very difficult to obtain and their use would determine the pathological worst-case behavior of the code, which is extremely unlikely to occur.

A measurement-based analysis approach, however, does not rely on models, but instead exercises tests on the multicore hardware itself. Using such an approach, it is possible to collect timing data that reflects the behavior of the system and isn't overly pessimistic.

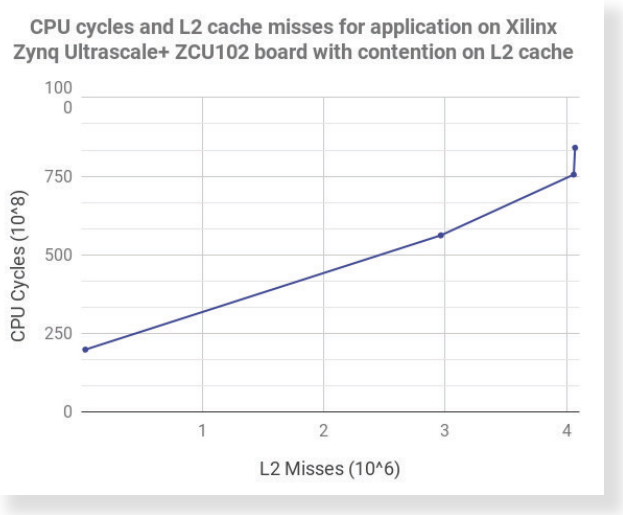
2.4 Assumptions must be tested

When beginning to analyze the timing behavior of a multicore system, a customer will need to make assumptions about the system, such as interference channels present in it and how they affect each application.

Throughout the analysis process, many of these assumptions may turn out to be invalid, and a customer will likely need to use knowledge gained from running tests to feed into a new testing cycle until they can verify that their assumptions are valid.

This is best explained with a practical example. We studied the sensitivity of a memory-intensive application running on a Xilinx® Zynq® Ultrascale+® ZCU102 target board to different levels of interference. The Application Processing Unit on which the application was running has 4 cores.

It would be a reasonable assumption that the L2 cache is a major interference channel for this application due to prior knowledge of the system. To validate this assumption, we design and run a test where the application is running while sustained accesses are made on the L2 cache from tasks running on between 0 and 3 contender cores.



Xilinx Zync Ultrascale+ results

If the assumption is valid, then the number of both L2 cache misses and CPU cycles taken for the application to execute will increase with each additional contender core.

The figure above shows that the assumption holds until we introduce a third contender core. This increases the number of CPU cycles but the number of L2 cache misses remains around the same as when only two contender cores are active.

This highlights that the assumptions made about how the hardware behaves aren't correct and the system will need to be investigated further to identify why the CPU cycles increase without the L2 cache misses increasing. This could be due to an interference channel that we didn't account for in the analysis, such as a shared bus.

3. The solution

The multicore timing analysis solution is comprised of tools, documents and services designed to meet DO-178C (CAST-32A/A(M)C 20-193) and ISO 26262 guidelines.

3.1 Testing in continuous integration environments

Software tools are critical to making multicore timing analysis efficient and cost-effective. Although the analysis of multicore timing behavior cannot be entirely automated, the use of software tools can drastically reduce the complex manual effort of attempting to perform such analysis by hand.

3.1.1 Rapita Verification Suite (R**VS**)

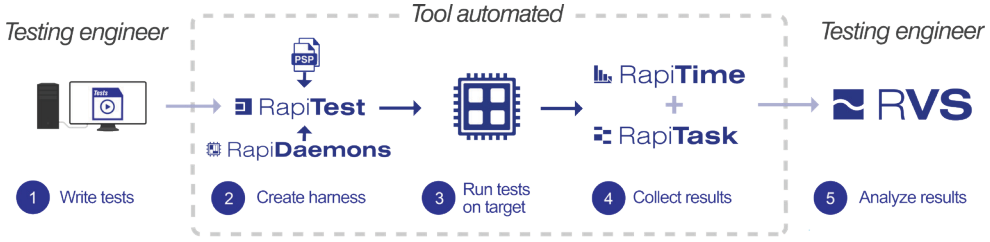
The Rapita **Verification Suite** (R**VS**) reduces the effort needed to verify critical embedded software for functional behavior (requirements-based testing), structural coverage and timing behavior, on target.

R**VS** has been used in the critical embedded industry for 15+ years and supported a number of avionics and automotive projects globally. Qualification kits for qualified R**VS** products have supported many DO-178B and C certification projects up to and including DAL A.

The following R**VS** plugins support multicore timing analysis:

- Rapi**Test** automatically measures and reports execution time metrics. It also allows customers to manage and author tests whilst maintaining requirement traceability.
- Rapi**Time** lets engineers write multicore tests easily and automatically converts these into a test harness that checks software behavior.
- Rapi**Task** automatically measures and reports scheduling metrics for each task under analysis.

Both Rapi**Time** and Rapi**Test** have been qualified for use in DO-178C projects and are supported with DO-330 tool qualification kits.



Rapita **Verification Suite**

CAST-32A and A(M)C 20-193 in DO-178C certification

CAST-32A is a position paper by the CAST team that covers DO-178C compliance concerns when using multicore processors. The FAA and EASA are currently working on an official DO-178C supplement, which will be titled AC 20-193 by the FAA and AMC 20-193 by EASA.

3.1.2 BSC's multicore micro-benchmark technology

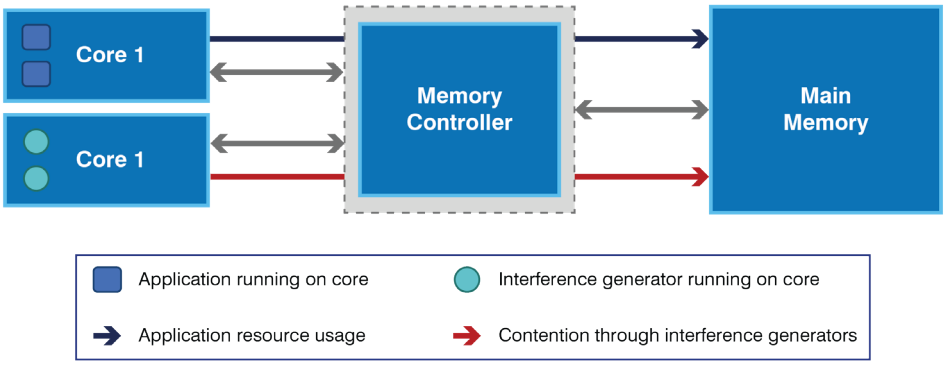
Micro-benchmarks (μB) are low-level, small code snippets that generate a high quantifiable (and adjustable) pressure on a specific shared hardwrae resource by issuing a constant flow of requests. By triggering controlled contention scenarios on a given resource, μBs allow characterizing the impact of contention. Impact characterization is not limited to the derivation of worst-case contention effects but also to assess the sensitivity of a given Unit of Analysis (UoA) to contention in the different shared hardware resources.

These micro-benchmarks allow a customer to provide the evidence to identify interference channels and quantify interference effects for multicore systems.

After writing multicore timing tests with Rapi**Test**, micro-benchmarks are automatically applied to configure the desired level of resource contention in each test.

We verify the behavior of micro-benchmarks via requirements-based testing, ensuring that they execute as intended and stress the desired resources at the desired level. To verify them, we build on hardware event monitors provided by the performance monitoring unit (PMU) available in all modern processors.

Rapita distribute micro-benchmarks as part of the CAST-32A Compliance solution, under the trademark Rapi**Daemons**.



Interference generators running on multicore hardware

Types of micro-benchmarks

» Standard interference generators either generate large load or are sensitive to load on a specific hardware resource. Standard interference generators target common interference channels, for example multi-level caches, interconnects and memory.

» Advanced interference generators either generate large load or are sensitive to load on a specific hardware resource with greater accuracy and precision than Standard interference generators. Advanced Rapi**Daemons** target complex resources and interference channels such as complex I/O devices, chip-specific devices and GPUs. Some Advanced interference generators support the analysis of complex sources of interference such as cache coherency protocols, thermal behavior and the effectiveness of cache partitioning mechanisms.

» Tunable interference generators generate configurable load on a specific hardware resource and are customized to a specific multicore setup. As they are tunable, these interference generators support fine-grained analysis of interference effects.

In addition to the interference generators listed above, special tools generate configurations of interference generators for specific use cases:

» BSC's Surrogate Applications (SurApps) are synthetic programs that are specifically designed to mimic the non-functional behavior of a given application. SurApps are automatically generated based on the profile of the target application and are tunable for those aspects of execution that are considered relevant by the end user. SurApps can be exploited to enable incremental and early verification of software modules by supporting exchange of otherwise IP-protected information among distinct providers. Also, SurApps allow you to develop a robustness-testing experimental campaign that addresses the impact of multicore timing interference.

» The BSC's Task Contention Model (TCM) provides an analytical (as opposed to empirical) upper bound to the worst-case impact on the execution time of a given task when the latter executes in a multicore system as opposed to a single core one. The bound computed by the TCM can be used in the early design stage in the software development life-cycle, to steer and optimize the design and configuration of the final system in view of the reduction (or even avoidance) of multicore timing interference.

Benefits of micro-benchmarks

» Reduce the cost and effort of analyzing multicore hardware for timing behavior, hardware characterization and selection.

» Understand the sensitivity of applications to interference when running in a multicore environment.

» Enable multicore certification for DO-178 and CAST-32A.

» The BSC's Task Contention Model provides an analytical upper bound to the worst-case impact of execution time for tasks on multicore systems.

Example use cases

» Platform & software characterization.

» Interference channel characterization and quantification.

» Produce evidence for DO-178 (CAST-32A) and ISO 26262.

» Verification of Performance Monitoring Counters.

Configuring micro-benchmarks

As part of our Target Integration Service, we select appropriate micro-benchmarks for a customer's system, port these to work with their system and perform additional configuration activities.

Through this service, we deliver a Platform Support Package that provides a tracing mechanism to extract results from Performance Monitoring Counters from a customer's system and integration into the R**VS** analysis toolchain.

3.2 Documentation & tool qualification to support certification

DO-178C and ISO 26262 certification both require the submission of documentation describing the verification strategy that was planned and implemented, and results from verification. Tool qualification evidence must also be provided. We have developed documentation to support this.

Find out more about DO-178C

rapitasystems.com/do178c-testing

3.2.1 Analysis & characterization reports

Platform Analysis Reports identify the critical configuration settings that can affect hosted software on a specific multicore platform and identify and describe the interference channels present on that platform.

Platform Characterization Reports describe and document tests and results of tests used to stress interference channels on a specific multicore platform to quantify the potential impact of interference from each interference channel on that platform. Test development and execution is supported by the R**VS** toolchain and interference generators.

Used in conjunction, these platform reports provide evidence that Platform Providers can use to demonstrate that their platform is certifiable for ISO 26262 or DO-178C (following CAST-32A guidance) and ensure that requirements from the System Integrator are met.

Find out more about CAST-32A

https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/cast/media/cast-32A.pdf

Software Analysis Reports list requirements on software timing behavior, which are generated by reviewing and analyzing existing requirements and software architecture.

Software Characterization Reports describe and document tests and results of tests that quantify the worst-case execution time of software hosted on a specific multicore platform. Test development and execution is supported by the R**VS** toolchain and interference generators.

Used in conjunction, these software reports provide evidence that Application Providers can use to demonstrate that their platform is certifiable for ISO 26262 or DO-178C (following CAST-32A guidance) and ensure that requirements from the System Integrator are met.

The above reports are also available in “template” form, for use as a convenient blueprint that can be used to generate a complete report. The template can be completed for a customer as part of a multicore engineering service, or if they are performing the analysis themselves, they can use the templates as a starting point to develop their complete reports from.

Process documents

Process documents describe in detail how to perform multicore platform and software analysis and characterization using a DO-178 workflow. This evidence can be supplied as supplementary evidence to support DO-178C certification and can be used to perform this analysis and characterization by a customer. Where a customer plans to do the analysis and characterization themselves, further support is available through comprehensive training.

Characterization tests

We provide test artifacts needed to analyze the potential impact of interference channels on a customer's multicore platform and the worst-case execution time of software hosted on that platform. This includes Test Cases and Test Procedures. These artifacts let a customer run the multicore tests on their platform and software and describe how to interpret the results. Characterization tests are customized for a specific platform or software through our Platform Analysis and Characterization Service and Software Analysis and Characterization Service. Our Characterization Tests are developed for execution using RVS and interference generators.

Template DO-178C compliance documents

We provide template CAST-32A compliance documents, which offer a convenient blueprint that can be used to generate final compliance documents. These documents can be completed as part of our Platform Analysis and Characterization and Software Analysis and Characterization Services, or if a customer is performing the analysis themselves, they can use the templates as a starting point to writing their compliance documents.

Rapita provide the following template CAST-32A compliance documents:

- Plan for Multicore Aspects of Certification (PMAC)
- Multicore Software Verification Plan (MSVP)
- Multicore Platform Characterization Results (MCPCR)
- Multicore Timing Resources Verification Results (MCTVR)
- Multicore Software Accomplishment Summary (MSAS)

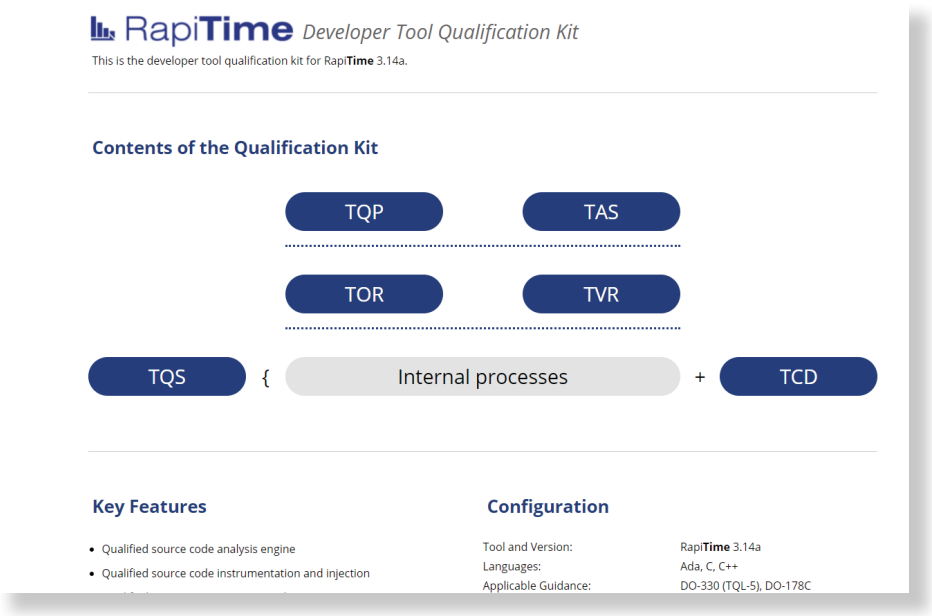
A customer can either use these templates to create standalone DO-178C compliance documents for multicore planning and verification or they can be incorporated into their standard compliance documents (PSAC, SVP etc.). These template compliance documents also include checklists that let a customer easily review their progress.

Rapita's template compliance documents cover the planning and verification activities required by 8 of the 10 CAST-32A objectives – all objectives except for MCP_Software_2 (on Data and Control Coupling) and MCP_Error_Handling_1 (on the safety net). Rapita support planning and verification for these objectives with our Consultancy service.

3.2.2 Qualification kits

R**VS** tools and micro-benchmarks are classified as Tool Qualification Level 5 Qualification tools according to RTCA's DO-330: Software Tool qualification Considerations document. As such, qualification evidence must be provided to demonstrate that the tools are robust when they are used in DO-178C projects.

DO-330 tool qualification evidence for R**VS** is already available through Rapita's Tool Qualification Kits and Qualified Target Integration Service.



RapiTime tool qualification kit cover page

DO-330 tool qualification evidence for micro-benchmarks is being developed.

DO-330

RTCA DO-330 is a document which provides tool-specific guidance for building airborne and ground based software. It may also be used in other domains such as automotive, space and electronic hardware.

3.3 Expertise for consultancy services

Expert multicore engineering services supplement the tooling and documentation described in the previous sections.

3.3.1 Multicore engineering services

A range of services are available, including:

- **Platform Analysis and Characterization Service** – This service provides everything needed to customize Platform Analysis Reports and Platform Characterization Reports to a specific multicore platform. This includes investigations into the critical configuration settings and interference channels that can affect hosted software behavior of the platform, the development of interference generators and Characterization tests that can be used to characterize the potential impact of interference on the platform, execution of tests to produce results, and generation of a complete Platform Analysis Report and Platform Characterization Report.
- **Software Analysis and Characterization Service** – This service provides everything needed to customize Software Analysis Reports and Software Characterization Reports to specific software run on a specific multicore platform. This includes deriving requirements for software hosted on the platform, the development of interference generators and Characterization tests for that platform, execution of tests to produce results, and generation of a complete Software Analysis Report and Software Characterization Report.
- **Target Integration Service** – To integrate RVS tools to be used within a multicore environment, we provide a Target Integration Service. This is described in our Target Integration Service Product brief. Interference generators must be ported for the multicore platform they are used for. This is also provided through our Target Integration Service.
- **Training Service** – We provide training on using the Rapita CAST-32A Compliance workflow and using R**VS** and interference generators to support this workflow. Together with our workflow process documents, this supports a customer if they want to use the CAST-32A Compliance workflow to perform Platform Analysis and Characterization and/or Software Characterization themselves.
- **Consulting Service** – We provide consulting services on DO-178C and CAST-32A compliance including gap analysis consultancy, certification liaison support and consultancy to satisfy all CAST-32A objectives.

4. Industry application

4.1 Raytheon Technologies - aerospace case study

Beechcraft King Air Pro Line Fusion

Collins Aerospace, a unit of Raytheon Technologies Corp. (NYSE: RTX), is a leader in technologically advanced and intelligent solutions for the global aerospace and defense industry. Created in 2018 by bringing together UTC Aerospace Systems and Rockwell Collins, Collins Aerospace has the capabilities, comprehensive portfolio, and expertise to solve customers' toughest challenges and to meet the demands of a rapidly evolving global market.

From the Research Centre of Raytheon Technologies in Ireland (former United Technologies), we are demonstrating the use of the MASTECS technology for the Civil Certified Vehicle Management Computer (CCVMC). This is an adaptable baseline DAL-A (flight-critical) vehicle management computer able to host 3rd party applications, see Figure 1 below, combining existing legacy parts of Collins Aerospace Flight Control systems.

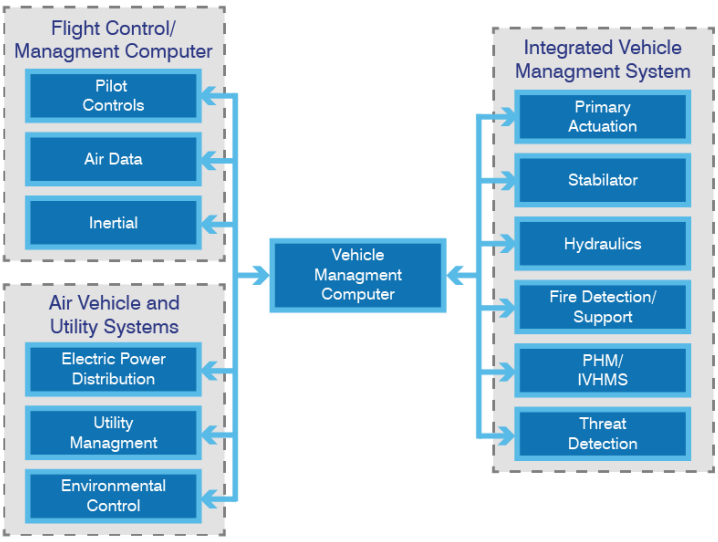


Figure 1: Functionality of Raytheon Technologies Civil Certified Vehicle Management Computer (CCMVC)

The system is compatible with the RTCA DO-297 standard for integrated modular avionics; it includes customer configurable I/O, scalable redundancy, cybersecurity protections, etc. The system contains triplex dissimilar high-performance processors as seen in Figure 2. The MASTECS project will be focused on the analysis of the software architecture running in one of these processors, the NXP T2080 quad core processor.

The system includes all necessary functions for flight-critical fly-by-wire system:

- All I/O has an Enable/Disable capability at the circuit level
- Watchdog Timers (WDT), Clock Monitors, Activity Monitors
- Cross Channel Data Links
- Cross Channel Status
- Internal Lane-to-Lane Synchronization
- External Channel-to-Channel Synchronization
- Multiple Sources of 28 VDC power
- Power hold-up circuitry
- Extensive Built-In Test (BIT)

The draft architecture of the system can be seen in Figure 2. Each Channel contains different subsystems or lanes. The idea is to offer two levels of redundancy, having different channels per aircraft and triplicated processing units per lane.

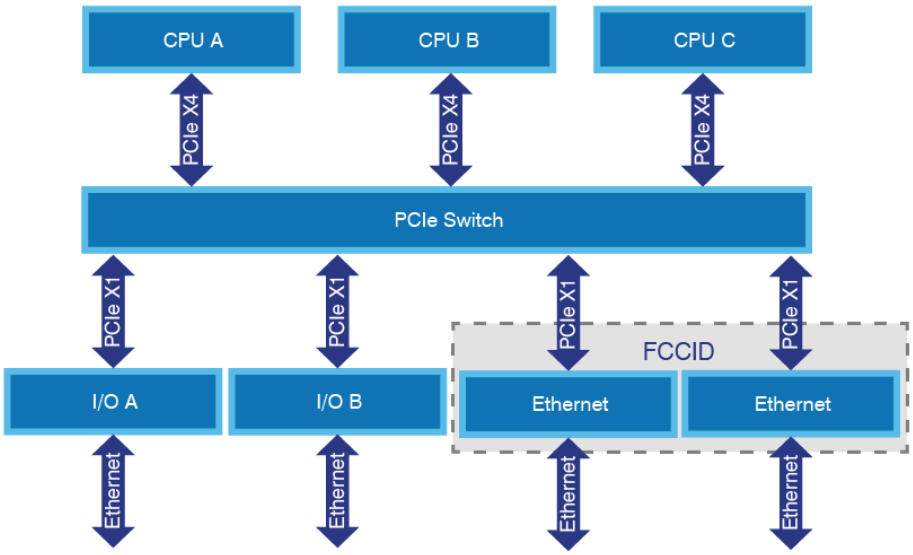


Figure 2: Vehicle management computer system architecture

LYNX

Lynx Software Technologies has expertise in multi-core, open architecture, and modular system software. LYNX MOSA.ic is a software framework for building and integrating complex multi-core safety- or security-critical systems using independent application modules. Lynx are participating in the MASTECS project by providing a multicore-optimized OS for the Raytheon, avionics multicore timing analysis case study.

As seen in Figure 2, the VMC architecture includes 6 functional components within the same integration unit that are connected via a PCIe switch:

» Three dissimilar quad core SBC processing units; a NXP T2080 processor, an Intel x86 processor, and an ARM A72 based processor. Table 1 shows detailed information of the processing units included.

» One FCC I/O Card: used for Ethernet data link and synchronization purposes.

» Two I/O Processor Cards: used for analog & discrete I/O communication with external devices.

Table 1: Detail of the selected quad-core microprocessors

CRITERIA	T2080 (NXP)	ARM A72	Intel x86
ARCHITECTURE	PPC e6500 1800 MHz	ARM A72 1800 MHz	x86 1600 MHz
SIMD	Yes	Yes	Yes
TYPICAL PART POWER	15.8 W	11.2 W	11.5 W
SERDES	16	8	8
PCIe Gen2 x4 LANE	Yes	Yes	Yes
MEMORY PROTECTION	DDR & L2/L3 ECCL1 Parity	DDR & L1 & L2 ECC	DDR & L2 ECC, L1 Parity
L2 L3 SIZE	2MB & 512 KB	2MB	8MB

The integration and timing analysis of such a system, with the added difficulty of hosting 3rd party applications, is extremely challenging. Guaranteeing Worst-Case Execution Time (WCET) values is very difficult and requires extensive hardware and software knowledge together with extremely thorough testing processes. The purpose of the MASTECS project is to achieve not only that but to do this analysis in a much shorter time when compared to the state of the art.

4.2 Marelli - automotive case study

MARELLI

Marelli Europe s.p.a. – Powertrain division is in charge of the product area dealing with the whole vehicle's propulsion system for ICE (Internal Combustion Engines) systems, inside Marelli group, one of the world's leading global independent suppliers to the automotive sector, born from the fusion of Calsonic Kansei and Magneti Marelli.

Marelli will deploy MASTECS technologies and tools for the analysis of a Vehicle Domain Control Module (VDCM). The VCDM is an integrated platform for Powertrain and Vehicle dynamic control. A high-level view of the diverse set of functionalities that can be managed by the VDCM is shown in Figure 3. The VDCM system is compliant with the ISO 26262 standard for Road Vehicle Functional Safety requirements, with the highest Automotive Safety Integrity Level (ASIL D).

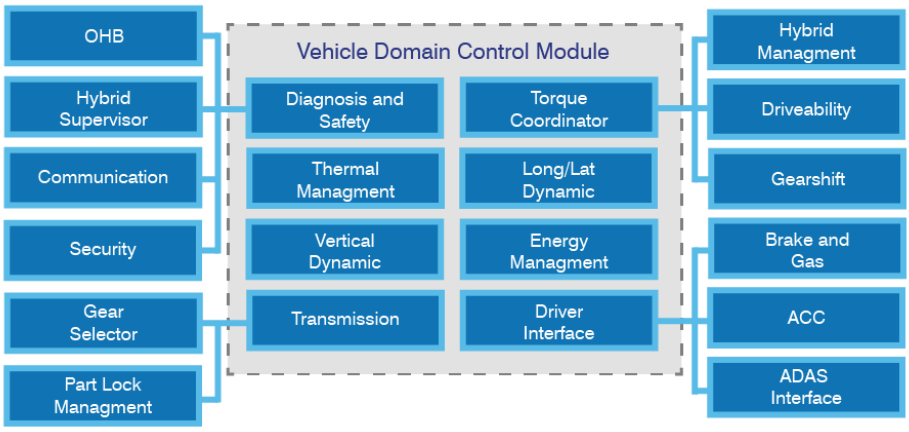


Figure 3: Marelli Vehicle Domain Control Module (VDCM) schematic view

The system is configured by "functions," where each function manages diverse aspects of the vehicle, ranging from canonical traction control functions to more cutting-edge ADAS Adaptive cruise control. Table 2 provides a hierarchical breakdown of the main functionalities provided by the VDCM.

Table 2: Hierarchical breakdown of provided functionalities for Vehicle Domain Control Module

Function	Breakdown
Longitudinal Dynamic Control	Drivability Control, Electric Motor Torque Limiter, Traction Control, Drag Control, Electric Motor Braking Control
Vertical Dynamic Control	Levelling Control, Hydraulic Lifter, Stiffness Control, Damping Control, Pro-Active System (Clear motion)
Lateral Dynamic Control	Torque Vectoring, All Wheel Driving, Rear Wheel Steering
Transmission Control	Gear Selector, Park Lock Management
Thermal Management	Cabin Heating and Cooling, HV Battery Heating and Cooling, Inverters Cooling, Motors Cooling
Energy Management	Torque Split, Battery Charging Control
ADAS Management	Battery Depleting Control, Adaptive Cruise Control, e-Horizon interface, Dual VDCM configuration

A schematic view of the system is depicted in Figure 4, which shows how the VDCM ECU is connected to other vehicle's components as sensors, actuators, smart actuators, or other ECU.

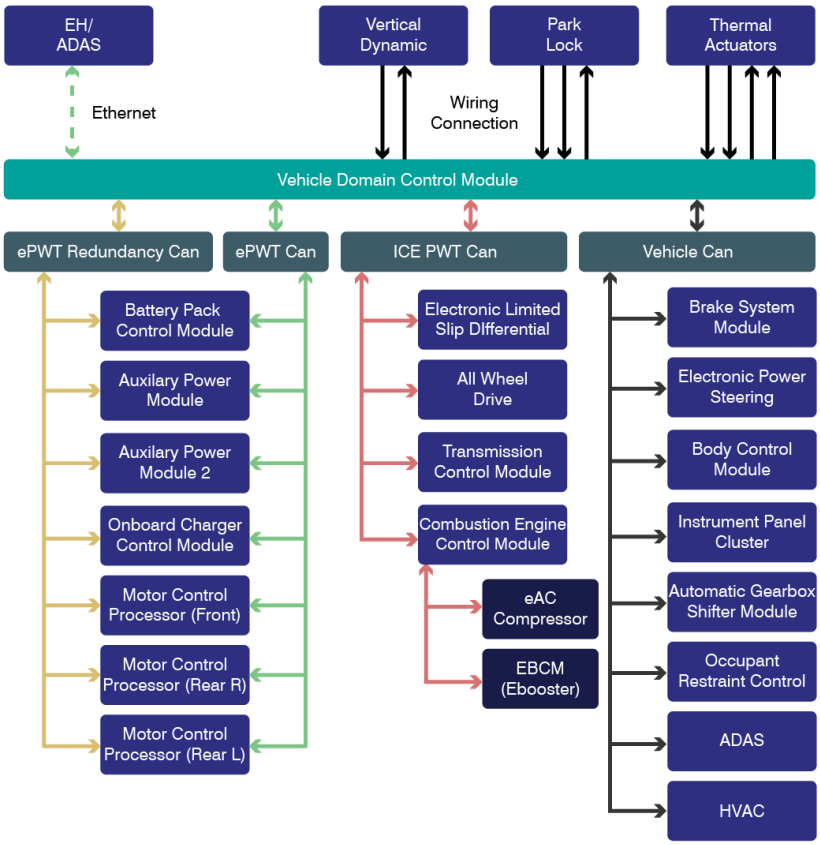


Figure 4: Overview of system connection for Vehicle Domain Control Module

On the hardware side, the VDCM platform is based on 32-bit TriCore™ AURIX™- TC397 Microcontroller by Infineon with the following characteristics:

- 6 TriCore™ running at 300 MHz (with 4 additional checker cores delivering 4000 DMIPS).
- Supports floating point and fix point with all cores.
- 16 MB flash/ ECC protection.
- Up to 6.9 MB SRAM/ ECC protection.
- 1 Gbit Ethernet.
- 12x CAN FD, 2x FlexRay, 12x ASCLIN, 6x QSPI, 2x I^2C, 25x SENT, 4x PSI5, 1x PSI5S, 2x HSSL, 4x MSC, 1x eMMC/SDIOT, 1x I^2S emulation.
- Redundant and diverse timer modules (GTM, CCU6, GPT12).
- EVITA Full HSM (ECC256 and SHA2).
- LFBGA-292 package.
- LFBGA-516 package.
- Developed and documented following ISO 26262/IEC61508 to support safety requirements up to ASIL-D/SIL3.
- AUTOSAR 4.2 support.
- Single voltage supply 5 V or 3.3 V.
- 165°C junction temperature.

From the software perspective, the VDCM architecture is based on AUTOSAR 4.3 Conformance Class ICC3. VDCM is implemented as an Embedded Real Time Multitasking full preemptive Software and the management of scheduling and context is done by an OSEK AUTOSAR compliant Operating System.

AUTomotive Open System ARchitecture (AUTOSAR) is a standardized automotive software architecture developed by car manufacturers, suppliers and tool developers. The goal of AUTOSAR is to introduce a standardized layer between application software and hardware in automotive applications to allow transferability of software components, easy collaboration between partners, and robust maintainability in projects.

In the scope of MASTECS the VCDM will be initially released as a Single Core Application and developed into a multicore application. MASTECS technology will help Marelli in finding an efficient way to partition the Software on the different cores, as well as in supporting a multicore timing analysis framework addressing the verification and certification requirements of the VDCM when it is deployed as a multicore application. Deploying VDCM as multicore application will also require the adaptation of the implemented AUTOSAR Basic Software Architecture, as depicted in the Figure 5.

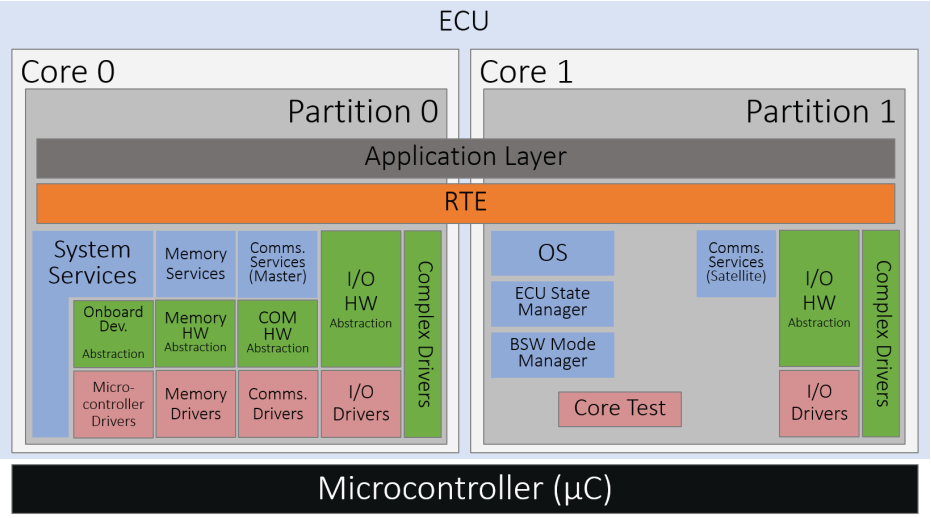


Figure 5: AUTOSAR Basic Software Architecture

5. Impact

MASTECS will offer automotive and avionics providers the first certification-ready timing analysis tool and service for critical systems, capable of handling the complexity of multicore processors.

5.1 Commercial

MASTECS, as a Fast Track to Innovation project, is focused on bringing technology to commercial reality, through building business and commercial exploitation.

Rapita Systems Ltd is delivering mulicore timing analysis technologies commercially through a market-leading product "CAST-32A Compliance" which includes R**VS**, the micro-benchmarks (branded as Rapi**Daemons**), qualification materials and services. The CAST-32A Compliance solution offers an end-to-end approach to multicore certification for CAST-32A projects.

The ecosystem and supply-chain includes the spin-off company, Maspatechnologies, which is set up to develop Barcelona Supercomputing Center's MicroBenchmark technology), Rapita's sister company in the USA - Rapita Systems, Inc. to generate and deliver commercial business in the USA, a network of distributors around the world and industry partners.

The CAST-32A Compliance solution is already being used by 10+ aerospace OEMs.

MASTECS will provide a significant contribution to the European economy, demonstrating that Europe and the UK are areas leaders in this area. The MASTECS project and its partners aim to lay the foundations for 50 new, skilled career opportunities by 2023 thanks to the new service offering, including three at Maspatechnologies. The products and services stemming from the MASTECS project will create an additional EUR 5 million in sustainable revenue per year by 2023.

5.2 Scientific

MASTECS aims to transform the possibilities of multicore verification by providing the first commercial multicore timing analysis solution on the market. Specifically, the multicore timing analysis solution technology (including tools and interference generators) readiness level will be developed from level 6 to level 8.

Additionally, two Industrial case studies will be used to demonstrate that the new solution is ready to be used to overcome real industry multicore challenges and ensure that the solution will meet certification criteria and the commercial needs of leading OEMs.

5.3 Societal and Environmental

Single-core processors are gradually being phased out of production and support by chip manufacturers. Multicore processors represent the present and future of safety-critical embedded computing and ensuring that there is a commercial solution to verify their behavior is vital to ensure that the transport systems of tomorrow are safe. The multicore timing analysis solution MASTECS is advancing will lead to reduced fatalities on the road and safer and cheaper air travel.

Environmentally, one of the key benefits of multicore processors over their single-core counterparts are their size, weight and power (SWaP) characteristics. By using multicore processors, system designers can reduce the number of embedded computers that would have been required in traditional, federated single-core systems.

The use of multicore processing reduces power/fuel consumption as such systems create less heat, weigh less and take up less room, hence increasing the efficiency of systems such as cars and airplanes. These efficiency gains, when applied at scale, will have a significant impact on global CO_2 emissions.

The use of fewer federeated processors in an embedded system is also beneficial in regards to the ongoing supply issues in the semiconductor industry (as at time of writing - 2021).

The MASTECS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 878752.

www.mastecs-project.eu