RAPITA
SYSTEMS
A DANLAW COMPANY

Safety through quality

BROCHURE

MACH[178] – Multicore Avionics Certification for High-integrity DO-178C projects

MACH¹⁷⁸

MACH¹⁷⁸ is a unique solution to support the certification of multicore DO-178C projects. By meeting the specific objectives of AMC 20-193 and CAST-32A, **MACH**¹⁷⁸ lets users reduce migration risks and open up the performance benefits that multicore processors offer while building a robust certification case.

> *Multicore systems are becoming more popular in critical embedded system development due to the increased performance they offer.*
>
> *Our MACH¹⁷⁸ Solution solves an important challenge in using these complex systems; ensuring that the software execution time meets timing deadlines and satisfies certification objectives.*
>
> *Dr. Guillem Bernat, CEO of Rapita Systems*

A unique solution

With the increasing adoption of multicore systems in the critical software industry, new methods are needed to analyze the timing behavior of these systems in line with DO-178C, AMC 20-193, CAST-32A and upcoming AC 20-193 objectives.

Combining expert knowledge from dedicated engineers with products from ground breaking academic research and our industry-leading software tool support, our solution to DO-178C compliance for multicore systems is truly unique.
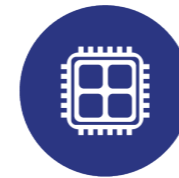
Use cases

Our solution supports a variety of use cases when migrating to, using and verifying multicore systems:

Produce certification evidence

Produce timing evidence for multicore systems to meet DO-178C, AMC 20-193, CAST-32A and upcoming AC 20-193 objectives.

Evaluate multicore hardware

Evaluate candidate multicore hardware architectures against performance criteria, taking into account the effects of contention from shared resources.

Optimize code for timing

Optimize multicore code for execution time behavior, ensuring that it meets timing deadlines and can be verified against safety objectives.

Benefits of our approach

Our approach not only identifies interference channels in multicore systems, but also quantifies them and takes them into account during timing analysis. We deploy our industry-leading tool automation support to provide a cost-effective solution to analyze multicore timing behavior and produce timing evidence for DO-178C, AMC 20-193 and CAST-32A certification of multicore systems. As the FAA's AC 20-193 guidance is expected to be very similar to AMC 20-193, the solution will also support AC 20-193 compliance.

Working with us

- We recognize that every project is different, and work with you to meet your needs.
- We run services at our engineering facilities in the UK or US. We can support projects with **UK / US eyes only** requirements.
- We can provide services to produce evidence needed for AMC 20-193 and CAST-32A compliance for you, or implement the **MACH**¹⁷⁸ workflow and provide you with training so you can do so yourself.

How it works

Restrict scope of the analysis

Q: Is the partitioning mechanism effective in removing inter-core interference on the LLC?

Requirements
Identify timing/WCET needs

Verification Results
Generate certification evidence

Generate multicore analysis report

Automatically generated document with traceability info summarizing test plans, implementation and results.

Understand the platform

The target features a shared L2 cache with the capability of a partitioning in between cores. Need to check that no additional L2 miss is incurred because of multicore execution.

Understand
Identify interference channels, define test methodology

Assessment
Analyze results, provide conclusions

Analyze raw results

Check that no additional L2 miss occurred. Access whether isolation is guaranteed.

Define test plan for each requirement

Tests designed to access the Level of isolation in the LLC.
Test shall execute X against YY in Core N... etc.
*LLC-01-01 Rapi**Daemon** selected.*

Test Design
Design tests to run, plan Rapi**Daemon** configuration

Evidence Gathering
Run tests, gather data

Tool Support

Configure resource contention	⚙ Rapi**Daemons**
Write tests, run on target	⊟ Rapi**Test**
Execution time analysis	⊪ Rapi**Time**
Scheduling analysis	⠿ Rapi**Task**

Tests implemented according to test plans

(Automatically) Generate binaries and deployment configurations e.g:
- *Synthetic contenders triggering L2 misses in N cores*
- *Enabling LL2_Miss_Count PMC*

Test
Integrate tool support and Rapi**Daemons**

Implementation
automation, configure for platform

Resource contention and interference

To analyze the timing behavior of multicore systems, the effects of contention on shared hardware resources such as caches and buses must be taken into account.

These effects generate interference that affects software execution time, and can in some cases have a huge impact. We determine the level of interference that can realistically occur in the system, as assuming the maximum level of interference possible leads to timing estimates that are wildly pessimistic and of no practical use.

Working with us

To examine the effects of resource contention and interference on multicore timing behavior, our multicore timing services use Rapi**Daemons**.

These are specially designed applications that can be integrated with the system under analysis to create a configurable degree of contention for shared resources such as caches and buses when running tests.

Rapi**Daemons** are built on the Barcelona Supercomputing Center's (BSC) micro-benchmark technology (MuBT).

Documents and tests
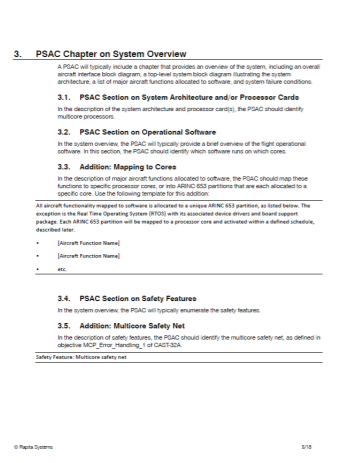
Template compliance documents

Our template AMC 20-193/CAST-32A compliance documents 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 you are performing the analysis yourself, you can use the templates as a starting point to writing your compliance documents.
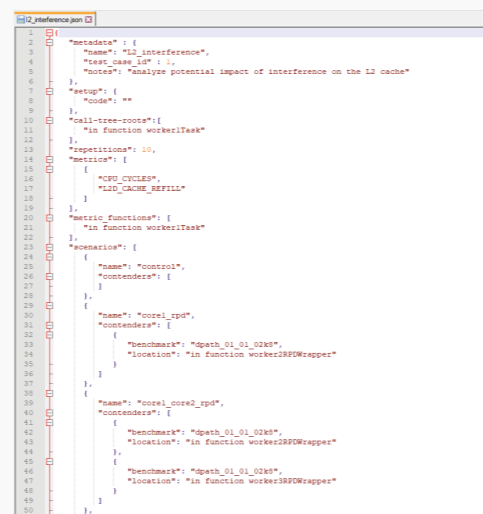
Reports

We provide four key reports to identify the interference channels in a range of multicore platform and to characterize the impact of interference on software execution time. These reports can be completed as part of our Platform Analysis and Characterization Service (for Platform reports) and Software Analysis and Characterization Service (for Software reports).
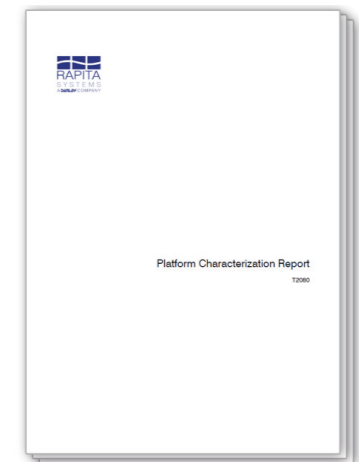
Characterization tests

Characterization tests include test artifacts needed to analyze the potential impact of interference channels on multicore platforms and the worst-case execution time of software hosted on those platforms. This includes Test Cases and Test Procedures. These artifacts provide tests to run on the target platform and describe how to interpret the results.

Characterization Tests are developed for execution using R**VS** and Rapi**Daemons**.
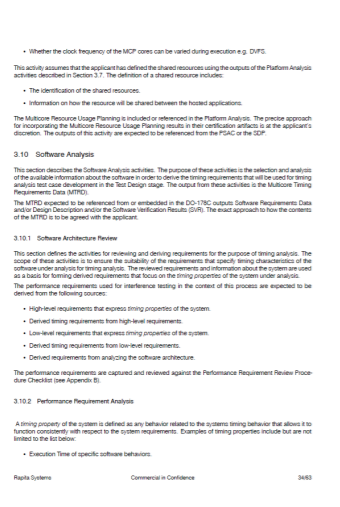

Platform Analysis Reports

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 Report

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.

Process documents

We provide process documents that describe in detail how to perform multicore platform and software analysis and characterization using the **MACH**[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 yourselves.

Software Analysis Report

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

Software Characterization Report

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.
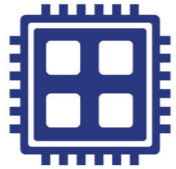
Tool support

1 Write tests

TESTING ENGINEER

2 Create test harness

PSP

3 Run tests on target

TOOL AUTOMATED

4 Collect results
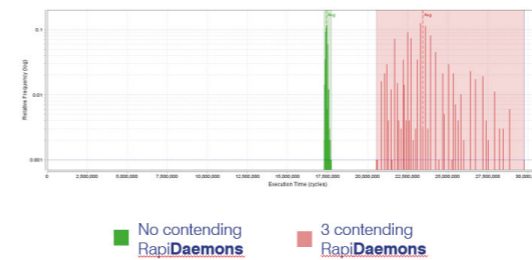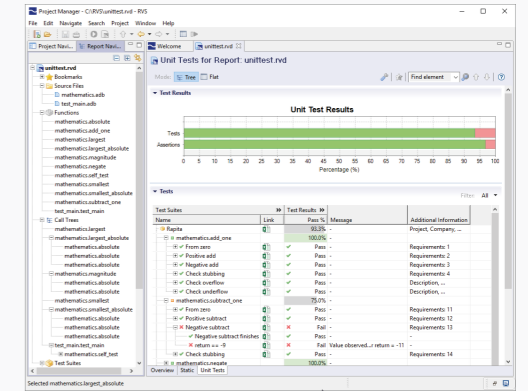
5 Analyze result

TESTING ENGINEER

RapiTest

Rapi**Test** helps to produce and run tests that exercise multicore software for execution time behavior while taking into account the effects of resource contention and interference (through applying Rapi**Daemons**).

Rapi**Test** automatically converts tests into a test harness that can be run on the multicore hardware.

RapiDaemons

Rapi**Daemons** create resource contention while analyzing a multicore task under analysis. Some micro-benchmarks are generic and are available as a standard library, while some are platform-specific and must be adapted to the platform under analysis through an integration service.

■ No contending Rapi**Daemons** ■ 3 contending Rapi**Daemons**

RapiTime

Rapi**Time** automatically calculates execution time metrics when multicore software runs on its target hardware, and reports them in a format that is easy to understand.

These metrics can be used to optimize code for timing behavior and provide evidence for DO-178C certification in line with AMC 20-193 guidelines.
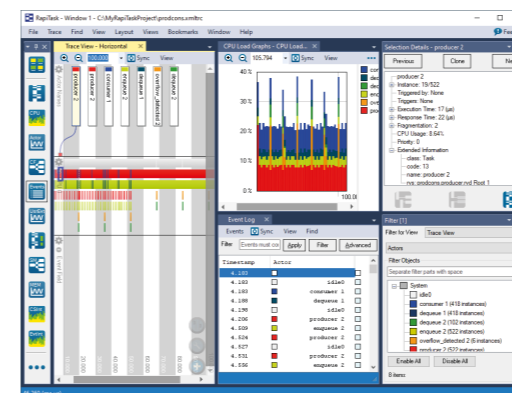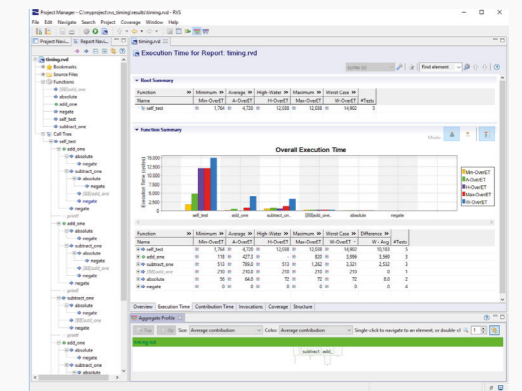
RapiTask

Rapi**Task** automatically measures and reports scheduling metrics for each task under analysis when multicore software runs on its target hardware.

These metrics can be used to identify system capacity issues and rare events such as race conditions in the software.

Services and certification support

Platform Analysis & Characterization

Software Analysis & Characterization
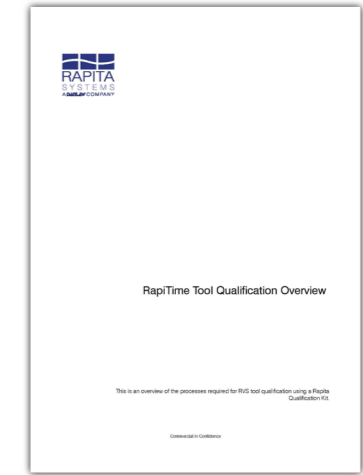
Analysis and Characterization Services

Our Platform Analysis and Characterization and Software Analysis and Characterization Services provide everything needed to implement the **MACH**[178] workflow on a specific multicore platform or application.

This includes performing analysis and characterization activities to produce reports and the development of Rapi**Daemons** and characterization tests.

DO-330 Qualification Kits

R**VS** automation tools are classified as Tool Qualification Level (TQL) 5 tools as per DO-330. Qualification support is available for Rapi**Test** and Rapi**Time** through our DO-330 Qualification kits, which have been used for certification in many DAL A aerospace projects certifying against DO-178C.

Rapi**Daemons** are classified as TQL 5 tools as per DO-330. Qualification support for Rapi**Daemons** is available through our DO-330 Qualification kits.

Target Integration Service

Our Target Integration Service integrates R**VS** tools and Rapi**Daemons** into a specific multicore platform and development environment.

Integration Services

Qualification

Qualification Services

Supplementing the generic test evidence in our DO-330 qualification kits, our Qualified Target Integration Service and Rapi**Daemon** Qualification Service provide the evidence needed to qualify the use of R**VS** tools and Rapi**Daemons** on specific multicore platforms.

Consulting

Training

Consulting and Training

We provide consulting services on DO-178C, AMC 20-193 and CAST-32A compliance including gap analysis consultancy, certification liaison support and consultancy to satisfy all AMC 20-193/CAST-32A objectives.

We provide training on using the **MACH**[178] workflow and using R**VS** and Rapi**Daemons** to support this workflow.

Incremental Assurance

With **MACH**[178], assurance evidence can be developed incrementally and independently for the multicore platform and each hosted application, supporting the development of Integrated Modular Avionics.

Assurance of Partition 2 behavior

Core 0		
Core 1	Par 2	Par 2
Core 2		
Core 3		

Cert Artifacts

Rapi**Daemon** running on partition
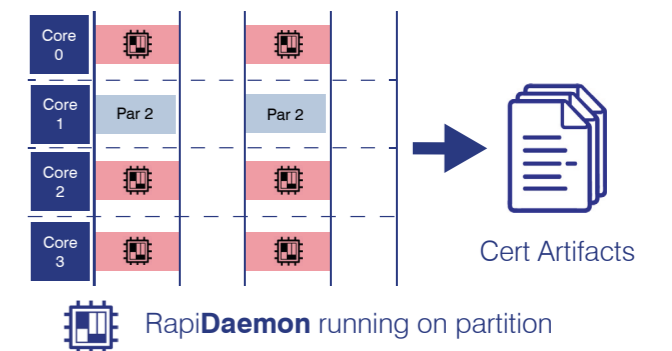
RAPITA Systems
A DANLAW Company

About Rapita

Rapita Systems provides on-target software verification tools and services globally to the embedded aerospace and automotive electronics industries.

Our solutions help to increase software quality, deliver evidence to meet safety and certification objectives and reduce costs.

Find out more

A range of free high-quality materials are available at:
rapitasystems.com/downloads

SUPPORTING CUSTOMERS WITH:

Engineering Services	Engineering Services	Multicore verification
Rapita **Verification Suite**:	V&V Services	**MACH**[178]
Rapi**Test**	Integration Services	Multicore Timing Solution
Rapi**Cover**	Qualification	
Rapi**Time**	SW/HW Engineering	
Rapi**Task**	Compiler Verification	

Contact

Rapita Systems Ltd.
Atlas House
York, YO10 3JB
UK

+44 (0)1904 413945

Rapita Systems, Inc.
41131 Vincenti Ct.
Novi, Mi, 48375
USA

+1 248-957-9801

Rapita Systems S.L.
Parc UPC, Edificio K2M
c/ Jordi Girona, 1-3
Barcelona 08034
Spain

+34 93 351 02 05

rapitasystems.com

linkedin.com/company/rapita-systems

info@rapitasystems.com