

Safety through quality

PRODUCT BRIEF

MACH¹⁷⁸ – Multicore Avionics Certification for High-integrity DO-178C projects

Product brief: MACH¹⁷⁸



How can MACH¹⁷⁸ help you?

MACH¹⁷⁸ provides a solution for certifying multicore aerospace projects in accordance with AMC 20-193 and CAST-32A guidance. The solution supports different roles in the avionics supply chain, including those of Integrated Modular Avionics (IMA) System Integrators, Platform Suppliers and Application Suppliers.

Benefits

- Reduce the cost and effort of certifying your multicore aerospace project
- Streamline and automate your multicore verification using the proven **RVS** toolsuite and Rapi**Daemon** technology
- Get started quickly with our wide range of supported multicore processor architectures
- Reduce certification risk with independent verification of your project
- Produce robust certification artifacts
- Aligned packages for each role in the avionics supply chain

Use cases

System Integrator & Certification Applicant

- End-to-end process to help address all AMC 20-193 and CAST-32A objectives
- Align your platform and application suppliers to harmonize AMC 20-193 and CAST-32A certification activities and artifacts with multi-vendor licensing
- Verify that interference effects are understood and bounded, i.e. interference channels are mitigated
- Measure worst-case execution time on-target
- Robustness and sensitivity analysis
- Produce evidence to support DO-178C (AMC 20-193 and CAST-32A) certification

Platform Supplier

- Ensure that your System Integrator's requirements are met
- Characterize platform multicore interference channels
- Evaluate and select multicore hardware and RTOS
- Determine outer bounds on worst-case execution time
- Identify multicore interference mitigation strategies

Application Supplier

- Ensure that your System Integrator's requirements are met
- Software performance characterization and optimization
- Measure worst-case execution time on-target

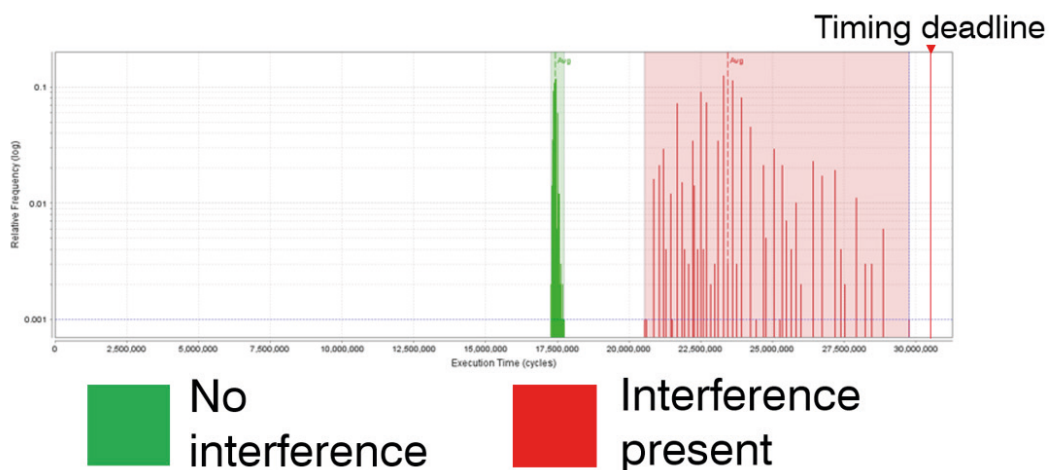


Figure 1. MACH¹⁷⁸ produces evidence on multicore timing behavior

How does it work?

MACH¹⁷⁸ is a combination of certification artifacts, software tools, engineering services and qualification support that supports compliance with AMC 20-193 and CAST-32A objectives. We provide custom packages to support AMC 20-193/CAST-32A compliance for each part of the avionics supply chain, including platform and application providers. **MACH**¹⁷⁸ comprises:

- Certification artifacts
 - Reports describing results to demonstrate that interference channels on a multicore platform have been identified and that the impact of interference has been characterized on software running on the platform
 - Processes to describe how to use the **MACH**¹⁷⁸ solution to address AMC 20-193 and CAST-32A guidelines
 - Multicore characterization tests to analyze the potential impact of interference on software timing behavior, and to analyze the worst-case execution time of multicore software when interference channels are stressed
 - Template DO-178C compliance documents including checklists
- Software tools
 - **RVS** toolsuite to automate the collection of timing evidence from multicore platforms
 - **RapiDaemons** to support the analysis of interference effects on the multicore system

- Engineering services to:
 - Analyze interference channels on the hardware and characterize interference effects
 - Integrate **RVS** into a multicore environment
 - Develop, select and port **RapiDaemons** for your platform
 - Analyze software worst-case execution times in the context of multicore interference
 - Train your team how to generate evidence on multicore timing behavior through the automated environment we set up
 - Help address all AMC 20-193 and CAST-32A objectives
- Qualification support
 - Tool Qualification Kits for **RVS** and **RapiDaemons**
 - Qualified Target Integration Service for **RVS**
 - **RapiDaemon** Qualification Service

MACH¹⁷⁸ uses a V-model framework (Figure 2) to produce a clearly structured flow of verification artifacts that satisfy DO-178C traceability requirements and meet AMC 20-193 and CAST-32A guidelines, ensuring a cost-effective and methodical verification process.

The stages may be iteratively refined – for example to redefine assumptions made about the platform under analysis after testing identifies hidden interference channels. This V-model applies to each level of the supply chain, focused on the particular requirements of each role. For more information on how this works, see our *Multicore Timing Analysis for DO-178C White paper*.

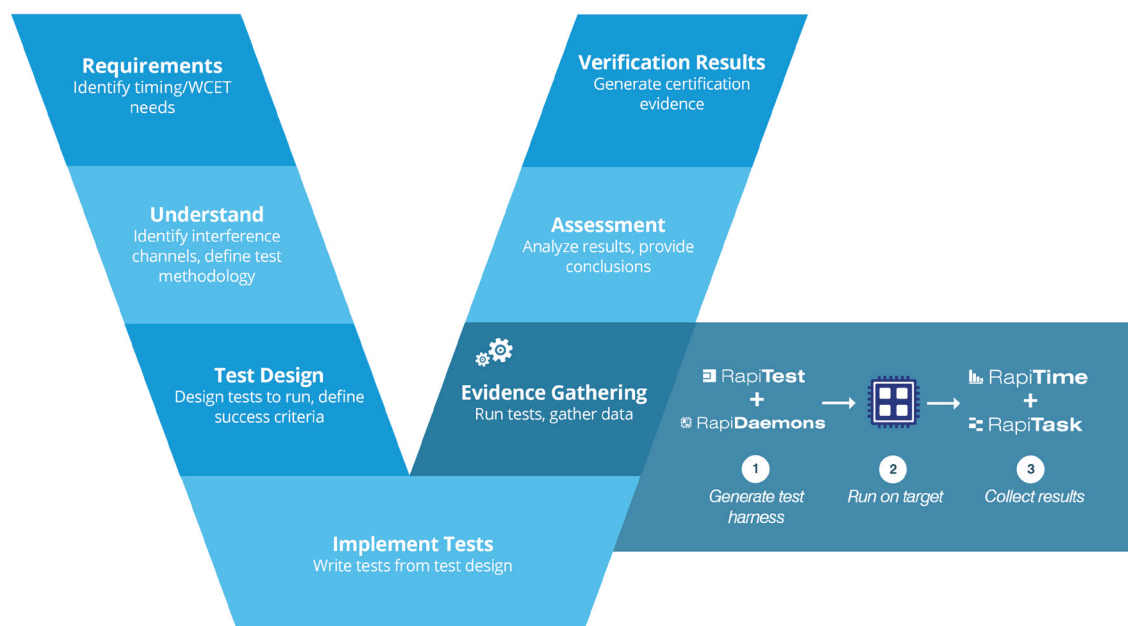


Figure 2. How we address AMC 20-193 and CAST-32A multicore timing objectives

A solution for every part of the supply chain

MACH¹⁷⁸ supports every part of the avionics supply chain.

System Integrators and Certification Applicants

MACH¹⁷⁸ allows System Integrators to perform verification activities demonstrating that a multicore Platform along with its integrated Applications is compliant with AMC 20-193 and CAST-32A. When combined with the incremental assurance evidence provided by Platform Providers and Application Suppliers, this forms a complete set of AMC 20-193/CAST-32A certification evidence.

We help develop supplier frameworks and processes that can be used as acceptance criteria for AMC 20-193/CAST-32A compliance activities performed by Platform Providers and Application Suppliers on the project.

Platform Providers

MACH¹⁷⁸ allows Platform Providers to produce evidence demonstrating that their Platform is compliant with AMC 20-193/CAST-32A. This evidence can later be used by Application Suppliers, System Integrators and Certification Applicants to support AMC 20-193/CAST-32A compliance.

Application Suppliers

MACH¹⁷⁸ allows Application Suppliers to produce evidence demonstrating that their Application, running on the target Platform, is compliant with AMC 20-193/CAST-32A. This evidence can later be used by System Integrators and Certification Applicants to support AMC 20-193/CAST-32A compliance.

Incremental certification

MACH¹⁷⁸ supports an incremental approach to certification. In this approach, which is often used for the certification of Integrated Modular Avionics (IMA) as specified in DO-297, a certification argument is created incrementally in the following way:

- Evidence is produced for the multicore platform, highlighting which interference channels are present in the system. This evidence is submitted to a certification authority to achieve acceptance, and this does not need to be repeated when applications are added to the multicore platform.
- Evidence is independently produced for each application to be hosted on the multicore platform, showing that each application is robust with respect

to interference caused by the interference channels identified for the multicore platform. This evidence is submitted to a certification authority to achieve acceptance for each application.

- Hosted applications are integrated into the multicore platform.
- When the certification applicant makes a final certification application, they claim credit from the acceptance claimed previous and do not need to recertify any part of the system.

This approach also supports the addition of new applications to the system without the need to re-generate artifacts for existing applications.

In this case, acceptance must only be requested for the new applications added to the system as per DO-297.

Your path to compliance

The path to AMC 20-193/CAST-32A certification can be split into 3 distinct phases:

- **Pilot phase** – we demonstrate the **MACH**¹⁷⁸ approach on a platform to be better able to scope activities for future phases. The platform and application analyzed may be your platform or a reference platform. We work with you to plan the activities in a pilot. These may include setting up a multicore integration with **RVS**, deploying **RapiDaemons**, working through Platform Analysis and Characterization and Software Analysis and Characterization activities on a subset of the system, and reviewing your existing DO-178C planning documents for alignment with AMC 20-193/CAST-32A. We share documents to help you understand the overall AMC 20-193/CAST-32A compliance process, including certification concerns, on a limited use license.
- **Implementation phase** – we set up an environment where evidence for multicore timing behavior can be automatically generated on your complete system. We perform a platform analysis to identify potential interference channels in your system. We characterize your hardware and software for multicore interference effects, or we deliver training that lets you do this yourself.
- **Certification phase** – we expand on the work done in the Implementation phase to prepare the project for certification. This includes deploying tool qualification kits and qualified target integration services, and may include us performing a final run for score, reviewing artifacts and traceability and assisting you in producing your SAS and liaising with certification authorities.

Certification artifacts

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. Together with a Platform Characterization Report, a Platform Analysis Report provides preliminary evidence that Platform Providers can use to demonstrate that their platform is certifiable for DO-178C following AMC 20-193 and CAST-32A guidance and ensure that requirements from the System Integrator are met.

We develop Platform Analysis Reports through our Platform Analysis and Characterization Service.

Platform Characterization Reports

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 **RVS** toolchain and **RapiDaemons**. Together with a Platform Analysis Report, a Platform Characterization Report provides preliminary evidence that Platform Providers can use to demonstrate that their platform is certifiable for DO-178C following AMC 20-193 and CAST-32A guidance and ensure that requirements from the System Integrator are met.

We develop Platform Characterization Reports through our Platform Analysis and Characterization Service.

Software Analysis Reports

Software Analysis Reports list requirements on software timing behavior, which are generated by reviewing and analyzing existing requirements and software architecture. Together with a Software Characterization Report, a Software Analysis Report provides evidence that Application Providers can use to demonstrate that their application is certifiable for DO-178C following AMC 20-193 and CAST-32A guidance and that requirements from the System Integrator are met.

We develop Software Analysis Reports through our Software Analysis and Characterization Service.

Software Characterization Reports

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 **RVS** toolchain and **RapiDaemons**. Together with a Software Characterization Report, a Software Analysis Report provides evidence that Application Providers can

use to demonstrate that their application is certifiable for DO-178C following AMC 20-193 and CAST-32A guidance and that requirements from the System Integrator are met.

We develop Software Characterization Reports through our Software Analysis and Characterization Service.

Process documents

We provide process documents that describe in detail how to perform multicore platform and software analysis and characterization using the Rapita 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. Where you plan to do the analysis and characterization yourselves, we further support this through our Training service.

Characterization tests

We develop and provide test artifacts needed to analyze the potential impact of interference channels on your multicore platform and the worst-case execution time of software hosted on that platform. This includes Test Cases and Test Procedures. These artifacts let you run the multicore tests on your platform and software and describe how to interpret the results.

We develop Characterization tests customized for a specific multicore platforms 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 **RapiDaemons**.

Template compliance documents

We provide template AMC 20-193/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 you are performing the analysis yourself, you can use the templates as a starting point to writing your compliance documents.

We provide the following template 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) (developed through service)

- Multicore Software Accomplishment Summary (MSAS) (developed through service)

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

Our template compliance documents cover the planning and verification activities required by 8 of the 10 AMC 20-193/CAST-32A objectives – all objectives except for MCP_Software_2 (on Data and Control Coupling) and MCP_Error_Handling_1 (on the safety net). We support planning and verification for these objectives with our Consultancy service.

Software tools

RVS toolsuite to automate gathering timing evidence

We use our software verification toolsuite – the Rapita Verification Suite – to configure and run tests on multicore platforms (RapiTest) and collect timing data (RapiTime) and scheduling data (RapiTask) from them (Figure 3). Using these tools, we automate various activities of the multicore timing analysis process. In some situations, we may also use our RTBx datalogger to collect trace data from your multicore platform during testing.

See our related *Product briefs* for more information on these tools.

RapiDaemons

RapiDaemons are small applications that run on multicore hardware and generate intentional contention on specific resources within the system (Figure 3). Each RapiDaemon targets a specific resource, for example caches, interconnects, memory and other on-chip or off-chip shared resources. This lets you identify and quantify the effects of multicore interference by running different RapiDaemons in different configurations.

We provide different types of RapiDaemons and RapiDaemon tools, which support multicore timing analysis in different ways. These include:

- Standard RapiDaemons
- Advanced RapiDaemons
- Tuneable RapiDaemons
- Discovery RapiDaemon tool
- Surrogate RapiDaemon tool

We curate and develop RapiDaemons for a specific multicore platform through our Platform Analysis and Characterization and Software Analysis and Characterization Services.

For more information on RapiDaemons, see our *RapiDaemons Product brief*.

Engineering services

MACH¹⁷⁸ includes a range of services, including:

- Platform Analysis and Characterization Service
- Software Analysis and Characterization Service
- Target Integration Service
- Training Service
- Consulting Service

Platform Analysis and Characterization Service

This service provides everything needed to develop Platform Analysis Reports and Platform Characterization Reports for 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 RapiDaemons 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 complete reports.

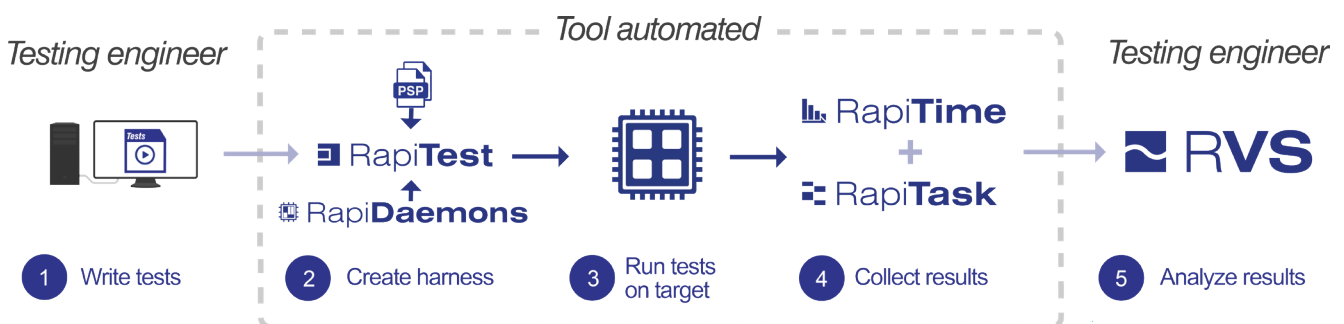


Figure 3. How RVS tools and RapiDaemons are used to gather multicore timing evidence

Software Analysis and Characterization Service

This service provides everything needed to develop Software Analysis Reports and Software Characterization Reports for specific software run on a specific multicore platform. This includes deriving requirements for software hosted on the platform, the development of Rapi**Daemons** and Characterization tests for that platform, execution of tests to produce results, and generation of complete reports.

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*.

Rapi**Daemons** must be ported for the multicore platform they are used for. This is also done through our Target Integration Service.

Training Service

We provide training on using the **MACH**¹⁷⁸ workflow and using **RVS** and Rapi**Daemons** to support this workflow.

Together with our workflow process documents, this supports you if you want to use the **MACH**¹⁷⁸ workflow to perform Platform Analysis and Characterization and/or Software Analysis and Characterization yourselves.

Consulting Service

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 and CAST-32A objectives.

Qualification support

Tool qualification kits

Our **RVS** 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. For more information, see our *Tool qualification for DO-178C Product briefs*.

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. For more information, see our *RapiDaemon Tool Qualification for DO-178C Product brief*.

Qualified Target Integration Service

To use evidence produced by **RVS** tools and Rapi**Daemons** for certification, the integration of these tools into your development environment must be qualified to produce evidence demonstrating that they have been correctly installed and are working appropriately with your system. We support this through our Qualified Target Integration Service, which is described in our *Tool Qualification for DO-178C Product briefs*.

RapiDaemon Qualification Service

Qualification evidence for Rapi**Daemons** is generated by collating results from running Rapi**Daemon** qualification tests on the target platform and using these results to instantiate template qualification documents. We provide services to run Rapi**Daemon** tests on-target, review test results, and generate and review qualification documents. For more information, see our *RapiDaemon Tool Qualification for DO-178C Product brief*.



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:

Tools

Rapita **Verification Suite**:

Rapi**Test**

Rapi**Cover**

Rapi**Time**

Rapi**Task**

Engineering Services

V&V Services

Integration Services

Qualification

SW/HW Engineering

Compiler Verification

Multicore verification

MACH¹⁷⁸

Multicore Timing Solution

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](https://www.linkedin.com/company/rapita-systems)



info@rapitasystems.com