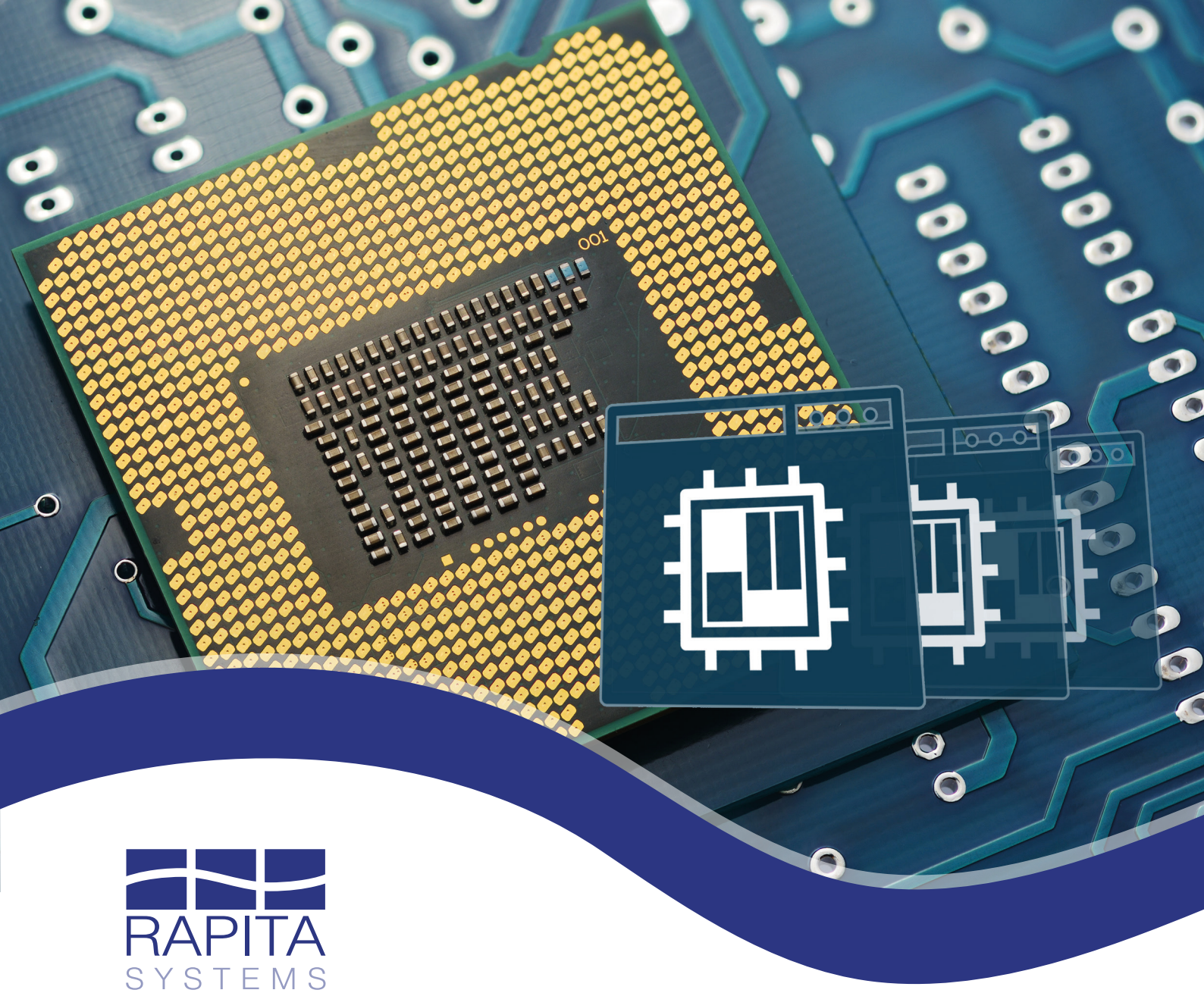


RAPITA SYSTEMS
A DANLAW COMPANY

Safety through quality

PRODUCT BRIEF

Interference channel analysis support for multicore airworthiness certification with Rapi**Daemons**

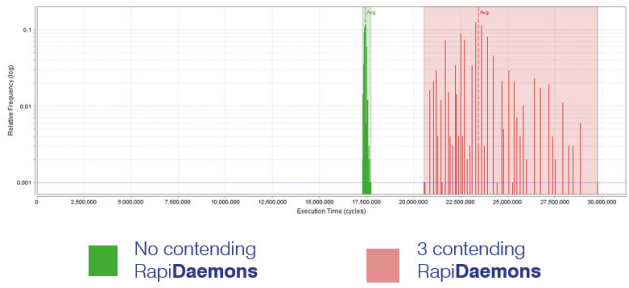
Document ID: MC-PB-108 RapiDaemons v15 INDT-v10

Product brief: Rapi**Daemons**

Rapi**Daemons**

How can Rapi**Daemons** help you?

Rapi**Daemons** allow you to provide the evidence to identify interference channels and quantify interference effects for multicore systems.



Understand multicore interference and predictability

Benefits of using Rapi**Daemons**

- Reduce the cost and effort of analyzing multicore hardware for timing behavior, hardware characterization and selection.
- Understand the sensitivity of your application to interference when running in a multicore environment.
- Path to multicore certification for DO-178C in line with AC 20-193 and AMC 20-193 objectives.

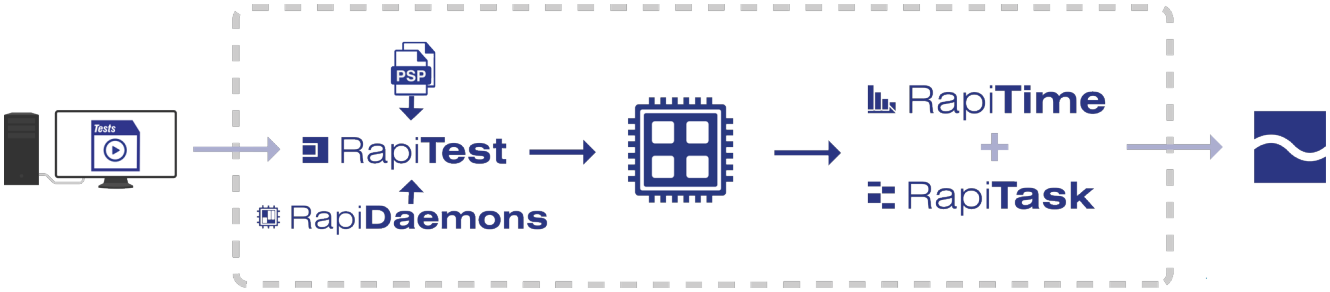
Rapi**Daemons** use cases

- Platform characterization and comparison.
- Software characterization and optimization.
- Interference channel characterization and quantification.
- Automatically discover worst-case interference profile.
- Simulate the interference of your application.
- Produce evidence for DO-178C, AC 20-193, AMC 20-193 and CAST-32A compliance.
- Robustness and sensitivity analysis.
- Verification of hardware event monitors.
- Verification of hypotheses on multicore behavior, for example effectiveness of cache partitioning and fairness of bus arbitration policies.

How do Rapi**Daemons** work?

Rapi**Daemons** are small applications that run on multicore hardware and generate accesses on specific resources within the system. Each Rapi**Daemon** targets a specific resource for example caches, interconnects, memory and other on-chip or off-chip shared resources, allowing you to identify and quantify the effects of multicore interference by running different Rapi**Daemons** in different configurations.

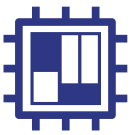
Rapi**Daemon** execution can be specified through tests created using Rapi**Test**, allowing the automatic initialization and execution of Rapi**Daemons** on your multicore platform. Meanwhile, Rapi**Time** and Rapi**Task** can be used to collect execution time results, values from hardware event monitors in your system, and scheduling information.



*Using Rapi**Daemons** within a multicore timing analysis workflow*

Types of Rapi**Daemons**

There are different types of Rapi**Daemons**, which support the analysis of multicore interference in different ways:



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

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

Tuneable Rapi**Daemons** generate configurable load on a specific hardware resource and are customized to a specific multicore setup. As they are tuneable, these Rapi**Daemons** support fine-grained analysis of interference effects.

In addition to the Rapi**Daemons** listed above, special tools generate configurations of Rapi**Daemons** for specific use cases:

The Discovery Rapi**Daemon** tool automatically generates a combination of Rapi**Daemons** that generate worst-case interference for your system.

The Surrogate Rapi**Daemon** tool automatically generates a Surrogate Application, a combination of Rapi**Daemons** that mimics a specified interference profile, often one that is similar to the profile generated by your real application as it runs on your multicore system (see Surrogate Applications).

How are Rapi**Daemons** configured for my system?

As part of our Target Integration Service, we port Rapi**Daemons** to work with your system and perform additional configuration activities.

Key features

Interference channel analysis

- Interference generators for e.g.:
  - Memory bandwidth
    - Access direction: access direction, paging, memory partitioning, memory level parallelism
  - Buses/interconnects
    - Fairness assessment, contention analysis, routing impact
  - Caches
    - Different levels: L1, L2, L3..., inter-level inclusion, coherence, partitioning
  - Shared functional resources
    - Floating point units, GPUs, DSP
  - Thermal/control features
    - Dynamic DVFS behaviors, dynamic power/ thermal caps
  - I/O devices
    - DMA, Ethernet
- Sensitive Rapi**Daemons**
- Tuneable resource accesses with Tuneable Rapi**Daemons**
- Identify the maximum interference for your system easily using Discovery Rapi**Daemons**
- Mimic the interference of your multicore applications with Surrogate Rapi**Daemons**
- Verify hardware event monitors
- Verifiable using hardware event monitors
- Integration with Rapi**Test**, Rapi**Time** and Rapi**Task**
- Documentation describing how to use Rapi**Daemons**

Supported platforms

- Rapi**Daemons** support the analysis of almost all multicore hardware architectures.
- Some of the components of multicore systems that we have analyzed are listed below.

Table 1 – Architectures we have worked with

SoC	Cores
Infineon® AURIX™	TriCore™
NVIDIA® Xavier™	Carmel Armv8
NXP® i.MX 8	Arm® Cortex®-A53
NXP® LS1048A	Arm® Cortex®-A53
NXP® LS1088M	Arm® Cortex®-A53
NXP® LX2160A	Arm® Cortex®-A72
NXP® P2041	PowerPC® e500mc
NXP® T1040/2	PowerPC® e5500
NXP® T2080/1	PowerPC® e6500
TI Keystone™ K2L	Arm® Cortex®-A15
Xilinx® Ultrascale+® Zynq MPSoC	Arm® Cortex®-A53, Arm® Cortex-R5
Xilinx® Ultrascale+® Zynq RFSoC	Arm® Cortex®-A53, Arm® Cortex-R5

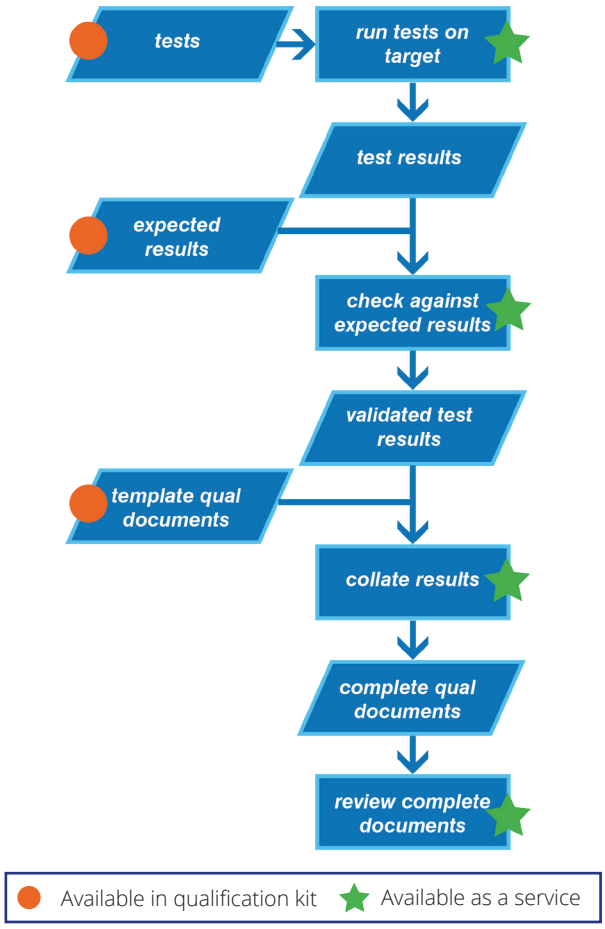
Table 2 – RTOSs we have worked with

RTOS
Bare metal
Blackberry® QNX™
DDC-I Deos™
Green Hills® INTEGRITY®
KRONO-SAFE® ASTERIOS®
Lynx Software Technologies LynxSecure®
SYSGO PikeOS®
Vector MICROSAR
Wind River® Helix/VxWorks®
Custom RTOSs

Support for other platforms is available on request.

Qualification support

- DO-178C qualification support materials for Rapi**Daemons** is available separately as a DO-330 Qualification Kit and Rapi**Daemon** Qualification Service.



*Rapi**Daemon** qualification workflow*

Licensing

- Annual or perpetual licenses

Surrogate Applications

Surrogate Applications are executable applications that mimic a specified interference profile, which is often a similar profile to that of a real application. Generated by the Surrogate Rapi**Daemon** tool, Surrogate Applications comprise a combination of Rapi**Daemons**. They support the analysis of multicore interference by allowing realistic interference scenarios to be analyzed without needing all applications in the system to be run during testing.

To generate Surrogate Applications, a profile ("fingerprint") of a target application is first created by running that application and collecting metrics from Performance Monitoring and Debug Support Units on the hardware. This fingerprint represents the non-functional behavior of the application, including metrics such as cache hits, cache misses and memory accesses.

Next, the Surrogate Rapi**Daemon** tool is configured to match a specific interference profile when generating a Surrogate Application. This includes two things: specifying the non-functional metrics that must be matched, which can include any of those in the fingerprint for an application, and specifying a value for each of these metrics. The value for each metric is tuneable and can represent the value captured from the real application or can be increased to create a more "aggressive" Surrogate Application.

Finally, the Surrogate Rapi**Daemon** tool is run to generate a Surrogate Application that mimics the desired interference profile. The tool also produces a metric that represents the similarity between the desired fingerprint and that of the generated Surrogate Application.

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:

Tools	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