RAPITA
SYSTEMS
A DANLAW COMPANY

Safety through quality

CASE STUDY

Rapi**Time**

Verifying the Timing Correctness of
Infineon®'s SafeTCore™ Safety Drivers

Case study: Rapi**Time**

Infineon® is the world's second largest chip supplier to the automotive industry, serving automotive applications such as power, body and convenience, safety management and infotainment.

The PRO-SIL™ Concept is a range of services provided by Infineon to support customers developing applications to meet IEC 61508 or ISO 26262. These services include safety drivers called SafeTCore™. These drivers are functionally independent of microcontroller hardware and can run on all microcontrollers in Infineon's TriCore™ family.

Infineon asked Rapita to conduct a two-stage project on the timing correctness of SafeTCore drivers:

- Use Rapi**Time** to look for optimization opportunities that would lead to reduced SafeTCore driver execution times

- Perform a WCET analysis with Rapi**Time** to gain confidence that the timing requirements would still be met in worst-case situations

Challenge

Since the SafeTCore is not only dealing with functional safety but also timing safety, deadlines are being monitored and it is vital that the SafeTCore is able to provide guarantees about its own execution time requirements.

The SafeTCore software must have a low execution time so that there is sufficient time for the application to run within each frame. If the SafeTCore driver execution time is too long, then it becomes necessary to schedule some tests over multiple frames leading to a significantly longer response time for error detection.

Summary

The challenge

- To provide guaranteed WCET with minimal pessimism for SafeTCore drivers running on Infineon's TriCore family in a system with limited I/O.

The solution

- Using Rapi**Time**'s idpack feature, and a logic analyzer to collect timing data, full timing analysis of the software was performed.

The benefits

- Coverage analysis shows completeness of tests. Rapi**Time**'s optimization support identified optimizations allowing WCET of specific functions to be reduced to 56% of its original value.

Solution

Infineon selected Rapi**Time** for its ability to provide a hybrid static analysis/dynamic measurement approach to WCET analysis. This avoided the challenges of a purely static analysis technique, which relies upon a specific model for each target to be analyzed.

As well as obtaining WCET values from Rapi**Time**, Infineon recognized that it could derive other benefits from the use of a tool that measures timing for small blocks of source code. In particular, feedback is received on the software implementation quality with respect to temporal variability and optimization potential.

Using Rapi**Time**'s idpack technology meant it was possible to uniquely identify as many instrumentation points as necessary within an 8-bit value. A trace of timestamped Ipoints was collected from an 8-bit output port using a Tektronix® Logic Analyzer.

Benefits

The timing analysis part of the case study concentrated on five TriCore functions. The chart below shows the difference in WCET between the initial versions and optimized functions, showing up to 43.9% reduction in WCET.

Function » Name	W-Freq	W-SelfET	W-SubfET	W-OverET	W-SelfED	W-OverED
⊞ ➡ main	0	0.000	0.000	0.000	0.000	0.000
⊞ ➡ Sfl_CheckCSFR_StcCyclic	0	0.000	0.000	0.000	0.000	0.000
⊞ ➡ Sfl_CheckECC_Cyclic	1	-0.013	0.000	-0.013 (-5%)	-0.013 (-5%)	-0.013 (-5%)
⊞ ➡ Sfl_CheckROM_Cell	1	-0.002	0.000	-0.002 (-12.5%)	-0.002 (-12.5%)	-0.002 (-12%)
⊞ ➡ Sfl_CheckSFR_StcCyclic	1	-0.001	0.000	-0.001 (-7.7%)	-0.001 (-7.7%)	-0.001 (-7.7%)
⊞ ➡ Sfl_RAM_CheckCell	1	-9.194	0.000	-9.194 (-43.9%)	-9.194 (-43.9%)	-9.194 (-44%)

The timing measurements obtained for the WCET analysis were also used to find source code optimizations in parallel with providing evidence of meeting timing requirements.

Beyond the high potential for software optimization revealed by the WCET analysis, it was also possible to identify areas of the software for further review. For example, unexpectedly long execution times can point to an unexpected error condition being triggered.

Where Rapi**Time** showed a large difference between maximum and calculated worst-case times, the cause was quickly identified as a data-dependent algorithm. This information is valuable when providing rationale for design and implementation decisions of future software.

Next steps

To learn how Rapi**Time** can help reduce the cost and effort of execution time analysis, see our product page at www.rapitasystems.com/products/rapitime.

To enquire about what Rapita can do for you, contact us at info@rapitasystems.com.

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	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, UK
YO10 3JB

+44 (0)1904 413945

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

+1 248-957-9801

rapitasystems.com

linkedin.com/company/rapita-systems

info@rapitasystems.com