

## Verifying the Timing Correctness of Infineon's SafeTCore Safety Drivers

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 Systems to conduct a two-stage project on the timing correctness of SafeTCore drivers:

- to use RapiTime to look for optimization opportunities that would lead to reduced SafeTCore driver execution times.
- to perform a WCET analysis with RapiTime 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.

### Solution

Infineon selected RapiTime 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.

### 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 RapiTime's idpack feature, and a logic analyzer to collect timing data, full timing analysis of the software was performed.**

### The Benefits

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

As well as obtaining WCET values from RapiTime, 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 RapiTime'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 lpoints 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 RapiTime 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 discuss timing verification solutions for your company, please contact Rapita Systems at [www.rapitasystems.com/contact](http://www.rapitasystems.com/contact) or via our worldwide network of distributors.

## About Rapita Systems Ltd

Rapita Systems Ltd specialize in providing customised on-target verification solutions for large critical real-time embedded software systems in the avionics and automotive electronics markets.

Rapita Verification Suite (RVS), which includes RapiTime and RapiCover, is the essential collection of on-target timing verification, optimization and code coverage measurement tools for real-time embedded systems. It is the only product on the market that can tell users exactly where to focus optimization effort to minimize worst-case execution time.

Using RVS, customers have cut the worst-case execution time of large scale, legacy applications by up to 50% with only a few days effort, and significantly reduced unnecessary testing and instrumentation overheads.



Atlas House  
Osbalwick Link Road  
York  
YO10 3JB  
United Kingdom

Tel No: +44 (0)1904 413945  
Email: [enquiries@rapitasystems.com](mailto:enquiries@rapitasystems.com)  
Website: [www.rapitasystems.com](http://www.rapitasystems.com)

Registered in England & Wales 5011090

China [www.cinawind.com](http://www.cinawind.com)  
Germany [www.embedded-tools.de](http://www.embedded-tools.de)  
India [www.spundhan.com](http://www.spundhan.com)  
Japan [www.aicp.co.jp](http://www.aicp.co.jp)  
Korea [www.rapitasystems.co.kr](http://www.rapitasystems.co.kr)