RAPITA Systems
A DANLAW Company

Case study

Capturing worst case timing and stack usage data for DO-178B Level A Embraer flight control systems

*"[Rapi**Time**] was able to support our hardware platform and once the system was set up, the analysis method could be repeated with relative ease"*

Since 1969 Embraer has built more than 5,000 aircraft that operate in 92 countries on five continents.

Working on the R&D stage of a DO-178B Level A Flight Control System (FCS) software application, Embraer wanted to obtain worst-case execution times (WCET) and worst-case stack usage data.

EMBRAER

Their solution was to choose Rapita Verification Suite (RVS) from Rapita Systems Ltd.

An important part of the development of this system's software was meeting the verification objectives required by DO-178B while at the same time decreasing development costs.

Summary

Challenge

- To capture WCET times and data while meeting DO-178B standards and reducing costs

Solution

- Use RVS tools to instrument the FCS source code and analyze the results from on-target testing

Benefits

- Obtaining a WCET and stack usage value without the need to generate and demonstrate a test scenario saves resources and time by automatically determining test scenarios for WCET and largest stack usage

Challenge

The Embraer FCS employs Fly-By-Wire (FBW) technology. Data processing and the logic of the FCS system are implemented by software, which due to the criticality of the FCS function, is classified as Level A software. Initial requirements for the FCS application required a WCET of less than 5 milliseconds, and a maximum stack usage of 20,000 bytes.

Embraer faced three major challenges during FCS development:

- to effectively capture worst case execution times and worst case stack usage data;
- to meet DO-178B requirements;
- to reduce development costs.

Solution

Instrumenting source code

Using RVS, instrumentation is added to the source code, which is then built using a compiler configured in the same way as during development activities.

The process for stack analysis is similar to that for timing analysis, except that points of instrumentation are only used for function entry and exits, and timestamps are replaced with the value of the stack pointer.

Analyzing the source code

RVS analyzes the source code and determines an overall structure of the code and the paths through it.

It was not necessary to design a test case for the paths leading to WCET or biggest stack usage because Rapi**Time** calculates them and reports whether that path corresponds to the longest path observed during testing.

This leads to a significant reduction of resource effort since generating a worst-case time scenario is a time consuming activity.

On-target testing

Since the purpose of this testing activity was only to exercise the paths of the application, the outputs were not evaluated and could be ignored. This method achieved coverage of approximately 77% of the instrumentation points for timing analysis, and 100% of the instrumentation points for stack analysis.

Benefits

Because it was not necessary to manually design a test case for the worst-case path, a significant resource effort was avoided, saving time and money.

After running and processing data, the WCET value for the whole integrated application was computed as 2.279ms and the worst-case stack usage was 3416 bytes.

Even with the partial timing coverage, the results confirmed that the FCS was compliant with the required limit on the execution time of 5ms, and that the stack usage was below the limit of 20,000 bytes.

> *"We have successfully shown the viability of using RapiTime to measure WCET.*
>
> *It was able to support our hardware platform and once the system was set up, the analysis method could be repeated with relative ease.*
>
> *With the WCET results, time partitioning was easily configured in the platform for the FCS application.*
>
> *Processing resources could be optimized by tightening the time window, even leaving some room for future expansion.*
>
> *Additionally the application hard deadline could be configured based on the results, with a Health Monitor to trigger if exceeded."*

Felipe Kamei, Embraer

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 enquiries@rapitasystems.com.

RAPITA SYSTEMS A DANLAW COMPANY

Rapita Systems Inc.
41131 Vincenti Ct.
Novi, MI 48375

Tel (USA):
+1 248-957-9801

Rapita Systems Ltd.
Atlas House, Osbaldwick Link Road
York , YO10 3JB
Registered in England & Wales: 5011090

Tel (UK/International):
+44 (0)1904 413945

Email: **enquiries@rapitasystems.com** | Website: **www.rapitasystems.com**