RAPITA Systems Ltd
A DANLAW Company

Case study

Validation of COTS Ada Compiler for Safety-Critical Applications

To ensure that software developed for safety-critical systems is fit for purpose, every part of the development process needs to be evaluated. One critical element is the compiler, used to convert human-readable source code into object code.

Compilers for the Ada programming language are already subject to a compiler conformity assessment, which shows that a given compiler correctly implements the Ada language specification. However, this assessment does not consider the suitability of the generated code for deployment to safety-related applications.

One frequently adopted approach to demonstrating the suitability of generated code is to manually review the inputs and outputs of the compiler wherever the compiler is used, in other words, to review the entire object code of the application.

An industry-leading avionics system integrator has adopted an alternative approach, which involves examining the output of the compiler over a large set of test cases, to ensure that the generated code does not use non-deterministic, or overly-complex features, which could be hazardous.

The benefit of this approach means, once validated, the same compiler can be deployed to multiple projects, without needing to perform a manual analysis on every project.

Summary

Challenge

- Outsource the compiler validation task, to reduce costs and effort from the systems integrator, while maintaining an equivalent level of rigour in the results.

Solution

- The compiler verification was outsourced to Rapita Systems, who completed the work on time and on budget.

Results

- A new compiler is now available to be deployed on any projects that need it, without additional validation costs.
- A number of dangerous and questionable issues have been identified in the compiler, which can now be avoided through guidance on using the compiler.

Challenge

The level of compiler validation performed by the systems integrator provides the level of assurance required for safety-critical systems, but is both expensive and complex, and ties up good engineers for long periods of time.

The systems integrator decided to outsource their compiler verification activity to Rapita Systems to reduce costs and free up valuable engineering effort.

Solution

Rapita Systems, a software verification company based in York, was approached as a possible partner for outsourcing the compiler validation work.

As a spin-out of the Real-Time Systems group at the University of York, Rapita Systems had familiarity with the original study which led to the compiler validation

work, with the Ada programming language and with the processes surrounding tool qualification.

To perform the work, Rapita adopted the test cases and processes used by the systems integrator in their previous validation of a compiler. The test cases were arranged in batches of roughly descending risk.

Each test case underwent a standard process:

- Porting. The capabilities of the new compiler meant that in some situations, the extensive test suite required porting, in order to exercise the compiler properly, for example to avoid compiler optimizations. In these cases, the test code was modified.
- The test cases were compiled using a local (to Rapita Systems) version of the compiler. Initially, the outputs of the locally-generated tests were compared against tests compiled at the system integrator's premises, to ensure the correctness of the compiler's configuration.
- The compiled test cases were analysed by a team of engineers considering a number of specific classes of phenomena, initially defined by the system integrator and enhanced by Rapita Systems.

Results

The outsourcing project has been successful: the compiler validation work was completed to time, to budget, and to the satisfaction of the system integrator's tools group.

As a consequence of this work, the systems integrator is now using the new compiler on a number of safety-critical projects within a larger program, without the per-use validation overhead typically encountered.

Within the compiler validation activity, Rapita Systems' team identified a number of issues categorised as either "dangerous" or "questionable", for which the system integrator's tools group were able to develop guidance that would avoid such issues.

Rapita Systems have developed procedures that will enable them to repeat this compiler validation activity on future programs as needed.

Next steps

To find out more about Rapita Systems, visit:

- www.rapitasystems.com

RAPITA SYSTEMS LTD
A DANLAW COMPANY

Atlas House
Osbaldwick Link Road
York
YO10 3JB
United Kingdom

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

Registered in England & Wales: 5011090

Tel (UK/International): **+44 (0)1904 413945**
Tel (US): **248-957-9801**