SuperTest – elevating AdaCore's C compiler to Ada/SPARK safety

Leading one-stop-shop developer of Ada and SPARK tool sets uses SuperTest™ to validate its C compiler for mixed-language programming environments.

AdaCore, a world leader in tools and services for high-integrity software development, provides comprehensive support for the Ada and SPARK programming languages. Both languages have gained significant traction in safety-critical application areas such as railway, avionics and automotive systems, where reliability, safety and security are paramount. However, as Vasiliy Fofanov, Certification Lead in AdaCore's Paris office points out, most application development teams are rarely purist in their choice of language.

"In practice, many of our customers have systems that use several different languages at the same time. Most of the code may be written in Ada or SPARK but they also have some secondary algorithms implemented in C. Because they don't want to have to deal with multiple software tool suppliers, many of them also ask us to provide solutions for C," he says. "Our expertise in high-integrity software development tools also means that we are often approached by companies that do not use Ada – so not our traditional customers – to provide a C tool chain with the same safety guarantees that we provide for Ada and SPARK."

Both types of customer demand mean that AdaCore needs to supply C compilers, and to ensure that they meet the safety requirements of its customers, it needs to verify them to international standards such as ISO 26262. That's where SuperTest comes to the rescue. AdaCore uses SuperTest to verify the front-end of a C compiler that is common to many of the target instruction set architectures it supports, including ARM 32- and 64-bit, PowerPC 32- and 64-bit, native Windows, Linux, and more recently, RISC-V.

According to Vasiliy, getting SuperTest up and running to suit AdaCore's customized GCC compiler was relatively straightforward, although not completely hassle free.

"Our GCC compiler is a customized version that's not always in sync with the standard GCC community releases, so we never expected that testing it would be a walk in the park. In practice, there were a few difficulties connecting the SuperTest tools to our compilation environment, but the Solid Sands team were very responsive and the issues quickly sorted out," he says. "Overall, it turned out to be a very positive experience."

AdaCore did not take its own compiler verification efforts for granted. In fact, the principal aim of using SuperTest was to gain external approval for its C compiler. It therefore subjected its methodology and verification results to independent external auditing, which it successfully passed.

"In terms of quality assurance, I think our C compiler is pretty much on the same level as our Ada and SPARK tool set, so we are now in a position to offer the same compiler quality to our safety-conscious C customers as we are for Ada and SPARK," says Vasiliy. "For new projects we would obviously recommend they go for Ada and SPARK, because even if the compiler faithfully translates a C program into object code this does not necessarily mean that the original C program is safe. With SPARK, program safety comes straight out of the box."

Nevertheless, with C's ubiquity and its huge ecosystem of available target processors, tools and devotees, he concedes that C will continue to be a significant part of the language mix.

"We appreciate that many customers, especially when they get closer and closer to the target architecture, prefer to write those 'close-in' segments of code in C. So having a mix of SPARK, Ada and C in the final solution will not be uncommon. The important thing is that thanks to SuperTest we can now provide the same level of tool assurance for all three languages."

AdaCore

COMPANY PROFILE

Founded in 1994, AdaCore supplies software development and verification tools for mission-critical, safety-critical, and security-critical systems. Four flagship products highlight the company's offerings:

- The GNAT Pro development environment for Ada, a complete toolset for designing, implementing, and managing applications that demand high reliability and maintainability. GNAT Pro is available for Ada and also for C and C++.
- The CWE-Compatible CodePeer advanced static analysis tool, an automatic Ada code reviewer and validator that can detect and eliminate errors both during development and retrospectively on existing software. CodePeer can detect a number of the "Top 25 Most Dangerous Software Errors" in the MITRE Corporation's Common Weakness Enumeration (CWE).
- The SPARK Pro verification environment, a toolset providing full formal verification oriented toward high-assurance systems with stringent security and/or safety requirements.
- The QGen model-based development tool suite for safety-critical control systems, providing a qualifiable and customizable code generator and static verifier for a safe subset of Simulink® and Stateflow® models, and a model-level debugger.

Over the years customers have used AdaCore products to field and maintain a wide range of critical applications in domains such as commercial and military avionics, automotive, railway, space, defense systems, air traffic management/control, medical devices, and financial services. AdaCore has an extensive and growing worldwide customer base.

AdaCore products are open source and come with expert on-line support provided by the developers themselves. The company has North American headquarters in New York and European headquarters in Paris.

Solid Sands

Solid Sands is based in Amsterdam, the Netherlands. Our mission is to put quality into C. We do that by improving the quality of C and C++ compilers, libraries and analysis tools, and their safe and secure use, with the best possible test and validation suite. With SuperTest, Solid Sands serves its customers to achieve the software quality level required by the ISO language and functional safety standards. With our history in compiler development, our knowledge of past, current and upcoming versions of the C and C++ standards, new analysis and optimization techniques and new use cases, Solid Sands stays at the fore-front of tools testing and validation.

SOLID SANDS

from Amsterdam is the one-stop shop
for C and C++ compiler and library testing,
validation and safety services.

Postbus 7897 | 1008 AB AMSTERDAM | The Netherlands | www.solidsands.nl