TRUST IN SOFT

SuperTest – helping TrustInSoft guarantee its customers 100% bug-free source code

Software development tool company TrustInSoft, which serves the international aeronautics, telecommunications, industrial IoT, and automotive industries via its offices in Paris (France) and San Francisco (CA, USA), is not a typical customer for Solid Sands' SuperTest compiler test and validation suite. The company's core product – TrustInSoft Analyzer – is an advanced source code analyzer that verifies the correctness of a C or C++ program before it gets anywhere near a compiler. So for a company that's not particularly interested in compiler development or validation, what is TrustInSoft using SuperTest for? The answer lies in the need for ISO 26262 functional safety certification from one end of the toolchain to the other – from source code to binary.

TrustInSoft's source code analyzer creates a mathematically rigorous model of a C or C++ program, which together with information on the program's input parameters and target architecture, allows users to verify with 100% accuracy that their program contains no undefined behaviors and conforms to its functional requirements.

"Using formal methods, we can deliver a mathematically definitive answer about a C or C++ program's behavior – a mathematical guarantee of the absence of bugs. So, if our TrustInSoft Analyzer says a program is fine, you won't find any violations in it, whatever input vectors you use," says Benjamin Monate, co-founder and Chief Technology Officer at TrustInSoft.

As far as compilation is concerned, TrustInSoft Analyzer only requires minimal information about the compiler, such as whether it's a GCC-like target and whether it's compiling for a 32- or 64-bit architecture.

"For the analysis, we never compile anything. So while some compiler-related information is needed to parameterize the analyzer, we assume that when the compiler is eventually invoked, it will work as expected. So, it is up to the customer to select a compiler that implements the C or C++ standard correctly," says Monate. "Of course, they should validate that their compiler works correctly using a test suite such as SuperTest, because if the compiler incorrectly translates their source code, any property that we prove mathematically on the source code is not guaranteed to transfer to the executable. Note that even if a compiler is perfectly conformant to standards, compiling code that contains undefined behavior will generate an executable that makes no sense and may contain serious and unpredictable safety and security issues. That is why you need to use TrustInSoft Analyzer and SuperTest."

To guarantee that the source code and the executable have the same semantics, the most important thing is that the analyzer and the compiler interpret the C or C++ language precisely as defined in the relevant standard. For TrustInSoft, SuperTest is one of the tools it uses to check TrustInSoft Analyzer's compliance.

"Because our tool is providing a solution that offers mathematical guarantees, we must be extremely strict about how we develop the analyzer itself, which means we need to rigorously validate it. And for the automotive market, we especially needed to have ISO 26262 qualification. We already have our own extensive range of test suites, but an important part of providing the necessary evidence for ISO 26262 was to use an independent test suite that is already widely recognized in the automotive electronics industry. That's why we chose SuperTest," says Monate.

The company uses SuperTest to confirm that TrustInSoft Analyzer correctly interprets the semantics of the C and C++ language.

"Using SuperTest we identified a few subtle parts of the standard that were not yet fully supported by TrustInSoft Analyzer and are now implemented and qualified. We were also able to identify some minor discrepancies in the way Solid Sands and our own engineers interpreted the C and C++ standards, which made it a highly rewarding collaboration, and one that we hope to continue," says Monate. "What really matters to us is that SuperTest helped us to extract a coverage matrix of the standard and topresent that as evidence of the quality of our tooling – that we never say something incorrect about the code – based on a completely independent test suite that is carefully designed to check all possible corners."

For software developers of safety-critical systems who need end-to-end ISO 26262 qualification of their toolchain, using a combination of TrustInSoft Analyzer and SuperTest to validate their source code and ensure correct compilation is a powerful solution that fits seamlessly into continuous integration environments.

For more information on TrustInSoft Analyzer and SuperTest visit www.trust-in-soft.com and www.solidsands.com

SuperTest Solid Sands

TRUST IN SOFT

There is more and more software everywhere, that controls our life. TrustInSoft wants everyone to benefit from the most secure and safest software possible – and this is enabled through mathematical techniques known as formal methods.In order to do that, TrustInSoft, a software publisher based in Paris and San Francisco, provides companies with a software code analysis tool to guarantee the security and safety of their source code using formal methods.

TrustInSoft was founded in 2013 by three former researchers Fabrice Derepas, Benjamin Monate, and Pascal Cuoq of the French government's Alternative Energies and Atomic Energy Commission. Their goal was to broaden the reach of formal methods for a variety of industry verticals, to promote security and safety in source code and contribute to making the ever-increasingly digitalized world a safer place. TrustInSoft today supports customers worldwide in the aeronautics, telecommunications, industrial IoT, and automotive industries.

Solid Sands

Solid Sands is the leading provider of compiler and library testing and qualification technology in North-America, Europe and Asia. 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 by enabling their safe and secure use. With the quality level of our test suites, we stay at the forefront of software testing and qualification to help you achieve ISO compliance and functional safety standard requirements. Founded in 2014, Solid Sands is headquartered in Amsterdam, The Netherlands. With partners all over the world we serve both leading innovative companies in the semiconductor, IP and security industries as well as safety-critical companies in automotive, robotics, railway and medical.

Our SuperTest Compiler Test and Validation Suite provides a complete validation environment which enables customers to achieve the software quality level demanded by the ISO language and functional safety standards. Meanwhile, our SuperGuard C Library Safety Qualification Suite is a requirements-based test suite for the C standard library with full traceability between the requirements derived from the ISO C language definition and the individual library tests.

SOLID SANDS

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

Overschiestraat 186 | 1062 XK Amsterdam | The Netherlands | www.solidsands.nl