Astrée satisfies NIST's Ockham criteria
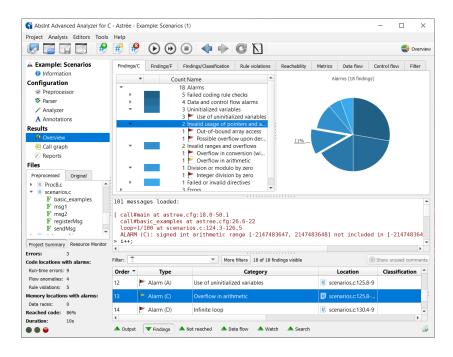
Saarbrücken, July 1, 2020: AbsInt's tool Astrée excelled at the NIST study on static analysis tools. The NIST Software Assurance Metrics And Tool Evaluation project, or SAMATE for short, is dedicated to improving software assurance by developing methods for evaluating software tools, measuring their effectiveness, and identifying gaps in methods and techniques.

The SAMATE project recognizes the value and importance of sound static code analyzers. During the 6th Static Analysis Tool Exposition (SATE VI), the NIST team evaluated static analyzers with respect to the SATE VI Ockham Sound Analysis Criteria.
In brief, these criteria are:

- The tool is claimed to be sound.
- For at least one weakness class and one test case, the tool produces findings for a minimum of 75% of appropriate sites.
- Even just one incorrect finding disqualifies a tool for SATE VI.

The definition of a finding includes reporting a buggy site as buggy, but also passing a correct code location without alarm. In other words, in order to satisfy the SATE VI Ockham Sound Analysis Criteria, all defects must be found, and the rate of false alarms must be low.

Astrée satisfies these criteria with excellent results: The tool was run on 28 sets of test cases from the Juliet 1.3 C test suite, including test cases for buffer overflows/underflows, invalid pointer dereferences, integer overflows/underflows, divisions by zero, use of uninitialized variables, dead code, infinite loops, double free, and use after free, running on a total of 18,954 buggy sites. All 18,954 were reported by Astrée. Additionally, Astrée discovered thousands of unintended defects in the Juliet 1.3 benchmark set.

The SAMATE report emphasizes Astrée's outstanding precision, both with respect to the analysis results as well as the analysis model itself: "Alarms from Astrée led us to find and fix thousands of mistakes in what was intended as the Juliet known-bug list, manifest.xml. Because Astrée analyzes code very precisely and we checked meticulously, details of modeling that otherwise would be inconsequential showed up and had to be resolved."

The full report was published in May 2020 and is available for free as PDF from nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8304.pdf

About AbsInt

AbsInt provides cutting-edge development tools for embedded systems with a focus on validation, verification, and certification of safety-critical and security-relevant software. Key products include static analysis tools to check coding guidelines, for timing and stack usage analysis, and to detect critical programming defects in C/C++ code.

Founded in 1998, AbsInt is a privately-held company located in Saarbrücken, Germany. Our customers come from various industry sectors, including aerospace, automotive, healthcare and energy, and are located in more than 40 countries all over the world.

For further information, visit www.absint.com.

Press contact

Sylvie Tritz, AbsInt Angewandte Informatik GmbH
Phone: +49 (681) 38 36 00
mail: tritz@absint.com