TRUSTINSOFT ANALYZER

HOW IT WORKS

WHAT IS A MATHEMATICAL GUARANTEE?

A mathematical guarantee is a property on a well defined set of objects. Its main benefits are generality and absence of ambiguity as all hypothesis become explicit. Applied to source code, this guarantee means that all the software behaviours are verified, as if exhaustive testing had been performed with a perfect oracle.

GLOBAL ARCHITECTURE

TrustInSoft's technology relies on a collaborative framework that facilitates seamless collaboration of different formal methods to address any kind of verification needs. Formal methods are implemented in different plug-ins, for instance, there is a plug-in for deductive proofs, abstract interpretation, and program slicing. A mathematical language named ACSL supports the communication between the plug-ins.

Media Contact

contact@trust-in-soft.com

USA: +1 (408) 829-5882

Europe: +33 1 84 06 43 91

ABSTRACT INTERPRETATION

Abstract interpretation is an analysis technique that computes an over-approximation of all the program behaviours. Indeed, it computes ranges of possible values for each variable at each step of the program.

PROGRAM SLICING

Program slicing is a technique that allows seamless navigation on a path sensitive, and context sensistive global data, and control flow graph. It allows a very fluid exploration of any program, and a fast and easy understanding of its semantics. Thanks to this technique, one can verify legacy and undocumented software without trusting anything but the source code.

DEDUCTIVE PROOF

When very advanced properties must be verified, TrustInSoft Analyzer provides deductive proof tools. Starting from a formal specification provided by the user, this analysis generates a lemma expressing that the code fulfills the user specification.

These lemmas are then proven, either automatically thanks to state-of-the-art SMT solvers (Microsoft Research Z3, INRIA/CNRS AltErgo, Google/Oxford/NYU/SRI CVC4), or interactively with proof assistants (Inria Coq, SRI PVS).

TRUST IN SOFT

trust-in-soft.com