U3CAT

Unification of Critical C Code Analysis Techniques

ON GOING PROJECT

Embedded software is increasingly prevalent in everyday life. Moreover, very large applications are now commonly embedded in various systems and often used to perform critical tasks, for which a failure would result in serious economic loss or even casualties. There is thus a strong need to provide the architects of such systems with adequate tools that allow them to state precisely the required properties of the application and to verify that the implementation meet them. Various analysis techniques exist, which all have their pros and cons. It is thus desirable to let these analyses cooperate in order to prove properties that could not have been established by a single technique. This is the main challenge that will be addressed in U3CAT, which will be built upon the Frama-C platform, one of the results of CAT, U3CAT's predecessor.

TECHNOLOGICAL OR SCIENTIFIC INNOVATIONS

The project is mainly focused on various enhancements of the Frama-C platform. They can be grouped in three categories. A first goal is to tackle additional domains of analysis, such as floating-point computations and temporal properties. These domain require specific analysis techniques which are implemented according to requirements gathered from the industrial partners of the project. The second aspect concerns the scalability of the analyses and the cooperation of the techniques to achieve a given verification task. Frama-C already provides a strong basis for such cooperation, but some enhancements are nevertheless needed in this area. Furthermore, efficiency of static analyzers can always be increased. Last, some work will be conducted in the formalisation and methodology of use of static analysis. This will provide a trusted framework for the development of critical software. In particular, all C analyzers and compilers rely on C semantics and some more or less abstract memory model. Agreeing on a proper formalisation of such models between Frama-C and the certified CompCert compiler would thus provide a complete development and verification chain from C code to binary. Similarly, it is envisaged to lift Frama-C results up to Scade models in the case of Scade-generated code. Finally, the project will strive to create an ecosystem around Frama-C, which is available under an Open-Source License. This includes academic and industrial communication, animation of the web community (web page, wiki, discussion list, ...) and incorporation of Frama-C into larger IDE, such as Eclipse.

STATUS - MAIN PROJECT OUTCOMES

Two releases of Frama-C have occurred since the beginning of the project, which have begun to incorporate the results of U3CAT. In particular, value analysis is now much stronger regarding floating-point computations, while the deductive verification plug-in allows to state very specific properties on rounding errors for these computations. Similarly, an important work has been done to define several memory models, depending on the required level of abstraction, and to establish the relations that exist between them, allowing to safely switch from one to the other when it is appropriate. A deductive verification plug-in supporting various memory models is expected for the second half of 2010.

CONTACT

Virgile PREVOSTO
CEA LIST
+33 (0)1 69 08 82 98
virgile.prevosto@cea.fr

PARTNERS

Large companies:
AIRBUS, ATOS ORIGIN, CS COMMUNICATION & SYSTEMES, DASSAULT AVIATION, SAGEM

Research institutes, universities:
CEA LIST, CNAM, INRIA RENNES, INRIA ROCQUENCOURT, INRIA SACLAY

PROJECT DATA

Coordinator:
CEA LIST

Co-label:
AEROSPACE VALLEY

Call:
ANR

Start date:
February 2009

Duration:
36 months

Global budget (M€):
4.4

Funding (M€):
1.8