Fraunhofer
FOKUS

FRAUNHOFER INSTITUTE FOR OPEN COMMUNICATION SYSTEMS FOKUS

DEVICE-SOFT

Contact
Dr.-Ing. Jens Gerlach
Head of Verification
System Quality Center – SQC
Phone +49 30 3463-7458
jens.gerlach@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

www.fokus.fraunhofer.de/en/sqc

Deductive Verification of Safety-Critical Software in Embedded Systems

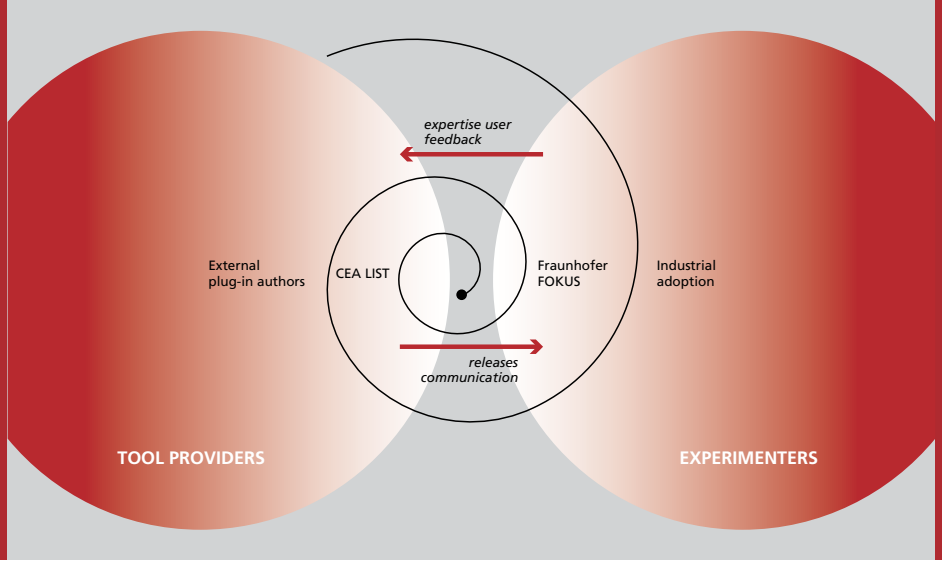
Software in embedded systems increasingly takes on key control functions, thus having to satisfy very high requirements. This is especially relevant for safety-critical applications in the aerospace, medical and railroad. In these domains, software errors can have disastrous consequences, both in financial terms and even putting people's lives at risk.

Traditional Testing and Deductive Verification

Traditional testing methods, such as unit testing, that assess the reliability of embedded software in safety-critical applications are very costly. The reason for this is that you have to make huge efforts to generate a sufficiently large number of test cases in order to attain a high level of testing coverage. Additionally, embedded software will increase in size and complexity in the future, leading in turn to greater demands on testing methodologies.

Deductive procedures represent an alternative to traditional testing methods. They prove desired software functionalities formally, using so-called unit proofs. This necessitates a formalization of the requirements. Using formulas arising from firstorder predicate logic, pre- and post-conditions for the individual program functions are defined. Afterwards, automated procedures (theorem provers) are used to prove that the program satisfies its post-condition if the pre-conditions are fulfilled.

Fraunhofer FOKUS is one of the few institutions with practical experience in the application and integration of Frama-C



The underlying methods, particularly the Hoare calculus, have extensively been researched. However, application of these methods to embedded software developed in programming languages customarily used in industry, such as C or C++, has largely been missing to date. In the DEVICE-SOFT project, Fraunhofer FOKUS has study how deductive verification methods can be applied more broadly in industrial applications with safety-critical embedded systems.

Initial findings show that unit proofs lead to lower validation costs and additionally produce higher quality when directly compared to traditional software tests. The application of deductive procedures can also ease the certification of safety-critical software because contrary to testing, they can prove that software behaves according to its specification for all possible inputs.

Application areas

- Aerospace
- Railroad technology
- Medical technology
- Automotive

Project Partner

- CEA List

Our Services

With DEVICE-SOFT, FOKUS has examined methods that enable unit tests to be replaced by unit proofs. For this, we use the Frama-C framework and its deductive verification plug-in. Frama-C enables users to generate the formal proofs needed for verification almost instantaneously. Fraunhofer FOKUS is one of the few institutions with an established practical experience in the application and integration of Frama-C in software development processes for safety-critical systems, especially for control units in railroad technology.

We support our customers in the integration of these tools in their development process. Fraunhofer FOKUS is an established expert in the usage of program analysis tools suitable for eliminating common software errors (e. g. division by zero or illegal array access). We offer our clients a wide range of services and extensive consulting options, from the selection of appropriate tools to the implementation, training and analysis of the results.

Funding

The project was funded within the scope of the Fraunhofer-Carnot initiative by the German Federal Ministry of Education and Research (BMBF) and the French National Research Agency (ANR). Approximately, 600.000 Euros in total volume were available from September 2009 to August 2011.

making cities smart

bad | 1402 (Photos: MEV Verlag; Matthias Heyde / Fraunhofer FOKUS)