Fraunhofer
FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

DEVICE-SOFT

Kontakt
Dr.-Ing. Jens Gerlach
Forschungsgruppenleiter Verifikation
System Quality Center – SQC
Tel. +49 30 3463-7458
jens.gerlach@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de/de/sqc

Deduktive Verifikation für sicherheitskritische Software eingebetteter Systeme

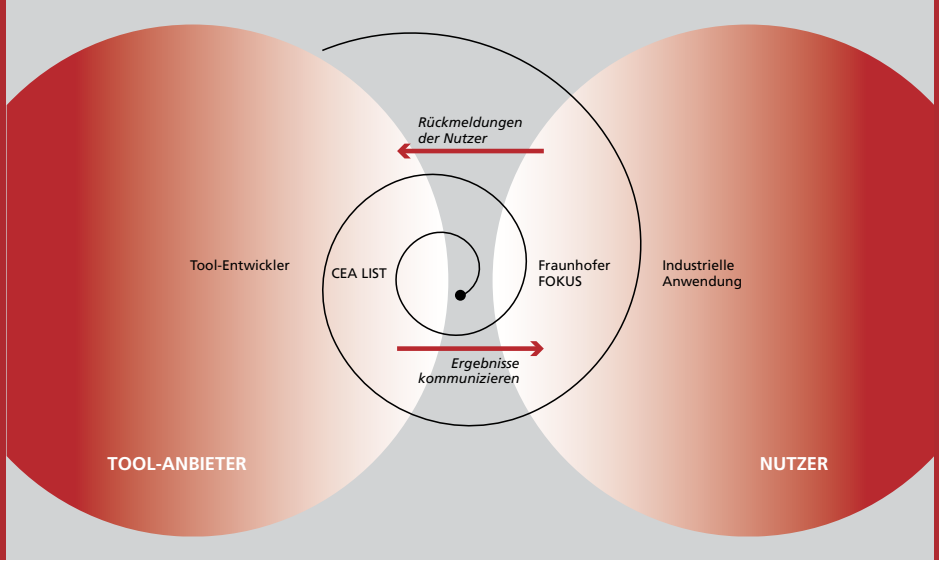
Die Software eingebetteter Systeme übernimmt zunehmend zentrale Steuerungsfunktionen und muss deshalb sehr hohen Auflagen genügen. Dies gilt insbesondere für sicherheitskritische Anwendungen in der Luft- und Raumfahrt, im Medizinbereich und im Bahnwesen. Hier können Softwarefehler katastrophale Folgen in finanzieller Hinsicht haben oder sogar Menschenleben gefährden.

Traditionelle Testmethoden und Deduktive Verifikation

Traditionelle Testmethoden, wie z. B. Unit-Tests, mit denen die Verlässlichkeit eingebetteter Software bei sicherheitskritischen Anwendungen überprüft wird, haben sich als teuer erwiesen. Denn um mit ihnen eine ausreichend hohe Testabdeckung zu erreichen, muss mit hohem Aufwand eine große Menge an Testfällen generiert werden. Hinzu kommt, dass in Zukunft die Komplexität eingebetteter Software und damit die Anforderungen an das Testverfahren noch zunehmen werden.

Eine Alternative zu traditionellen Testmethoden sind deduktive Verfahren, die die erwünschten Eigenschaften einer Software formal mit sogenannten Unit-Beweisen belegen. Dazu benötigt man eine formalisierte Dokumentation der Anforderungen. Mithilfe von prädikatenlogischen Formeln werden z. B. die Vor- und Nachbedingungen für die einzelnen Programmfunktionen definiert. Anschließend wird mit automatisierten Verfahren (Theorembeweisern) bewiesen, dass das Programm bei Einhaltung der Vorbedingungen die spezifizierten Nachbedingungen erfüllt.

Fraunhofer FOKUS gehört zu den wenigen Einrichtungen mit praktischer Erfahrung beim Einsatz von Frama-C



Die zugrunde liegenden Methoden, insbesondere der Hoare-Kalkül, sind wissenschaftlich eingehend untersucht worden. Allerdings fehlt bislang noch weitestgehend die Anwendung dieser Methoden für eingebettete Software, die in industrieüblichen Programmiersprachen, wie z. B. C oder C++, entwickelt wurde.

Fraunhofer FOKUS hat im Projekt DEVICE-SOFT untersucht, wie sich deduktive Verifikationsmethoden für industrielle Anwendungen mit sicherheitskritischen eingebetteten Systemen breiter einsetzen lassen. Erste Erfahrungen zeigen, dass Unit-Beweise zu geringeren Validierungskosten führen und darüber hinaus eine höhere Qualität erbringen als Softwaretests. Der Einsatz deduktiver Verfahren kann außerdem die Zertifizierung sicherheitskritischer Software erleichtern, denn im Gegensatz zum Testen lässt sich mit ihnen beweisen, dass eine Software für alle möglichen Eingaben spezifikationsgemäß funktioniert.

Anwendungsbereiche

- Luft- und Raumfahrt
- Bahntechnik
- Medizintechnik
- Automotive

Projektpartner

- CEA List

Unser Angebot

Fraunhofer FOKUS hat im DEVICE-SOFT Projekt Methoden untersucht, mit denen sich Unit-Tests durch Unit-Beweise ersetzen lassen. Dazu wurden das Frama-C Framework von CEA LIST und seine deduktiven Verifikations-Plug-Ins genutzt. Frama-C versetzt seine Nutzer in die Lage, die für die Verifikation benötigten formalen Beweise weitgehend automatisch zu generieren. Fraunhofer FOKUS gehört zu den wenigen Einrichtungen mit ausgewiesener praktischer Erfahrung in der Anwendung und Integration von Frama-C in Softwareentwicklungsprozesse für sicherheitskritische Steuergeräte in der Bahntechnik.

Wir unterstützen Sie bei der Integration dieser Werkzeuge in Ihren Entwicklungsprozess. Darüber hinaus verfügt Fraunhofer FOKUS auch über ausgewiesene Expertise beim Einsatz von anderen Analysewerkzeugen, mit denen häufige Softwarefehler ausgeschlossen werden können. Wir beraten Sie von der Auswahl der geeigneten Werkzeuge über die Implementierung und Schulung bis hin zur Analyse der Ergebnisse.

Förderung

Das Projekt wurde im Rahmen der Fraunhofer-Carnot-Initiative vom Bundesministerium für Bildung und Forschung (BMBF) sowie der Agence Nationale de la Recherche (ANR) gefördert. Von September 2009 bis Juni 2012 standen rund 600.000 Euro an Gesamtvolumen zur Verfügung.

Wir machen Städte schlau

bad | 1402 (Fotos: MEV Verlag, Matthias Heyde / Fraunhofer FOKUS)