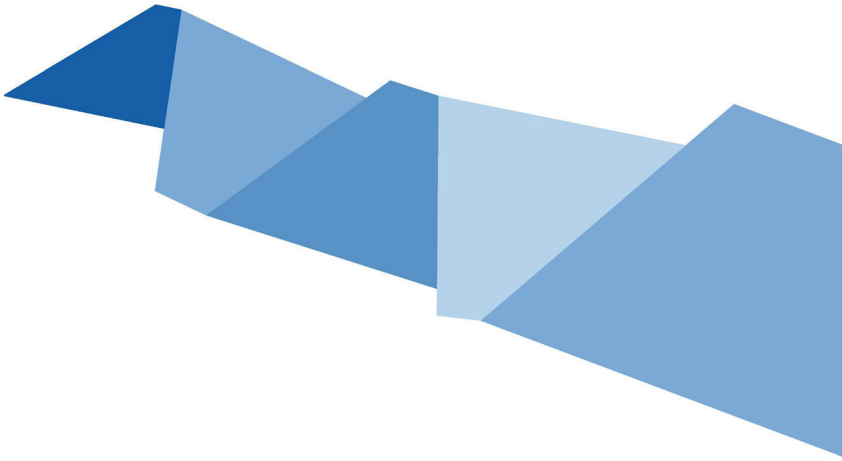

Formale Methoden für die Entwicklung von eingebetteter Software in kleinen und mittleren Unternehmen

Sebastian Patrick Grobosch

Department of Computer Science

Technical Report

Aachener Informatik-Berichte (AIB) | ISSN 0935-3232 | AIB-2019-03
RWTH Aachen University | Department of Computer Science | Oktober 2019

Formale Methoden für die Entwicklung von eingebetteter Software in kleinen und mittleren Unternehmen

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der
RWTH Aachen University zur Erlangung des akademischen Grades
eines Doktors der Ingenieurwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Ingenieur
Sebastian Patrick Grobosch
aus Bottrop

Berichter: Universitätsprofessor Dr.-Ing. Stefan Kowalewski
Universitätsprofessor Dr.-Ing. Sebastian Engell

Tag der mündlichen Prüfung: 30. November 2018

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über `http://dnb.d-nb.de` abrufbar.

Zugl.: D 82 (Diss. RWTH Aachen University, 2018)

Sebastian Patrick Grobosch
`sebastian.grobosch@rwth-aachen.de`

Aachener Informatik Bericht AIB-2019-03

Herausgeber: Fachgruppe Informatik
RWTH Aachen University
Ahornstr. 55
52074 Aachen
GERMANY

ISSN 0935-3232

ISBN 978-3-8440-6984-6

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Telefon: 02421 / 99 0 11 - 0 • Telefax: 02421 / 99 0 11 - 9
Internet: `www.shaker.de` • E-Mail: `info@shaker.de`

Zusammenfassung

Die Anzahl der Steuergeräte in Fahrzeugen der Oberklasse ist in den letzten 15 Jahren stetig gestiegen und liegt aktuell bei etwa 100 Stück. Dabei entsteht der Großteil aller Innovationen im Fahrzeug durch Elektronik und Software. Dies macht Software einerseits zu einem der wichtigsten Innovationstreiber für Unternehmen in der Automobilindustrie, andererseits birgt sie ein hohes Risikopotential: Programmfehler.

Durch internationale Normen und strengere Anforderungen an die Software-Qualität wird versucht, diesem Risiko entgegenzuwirken. Um alle Wünsche der Endkunden individuell erfüllen zu können, wächst allerdings die Komplexität der Systeme durch die steigende Variantenvielfalt. Das Testen von solchen Software-Systemen kann dabei nur das Vorhandensein von Fehlern zeigen, jedoch nicht deren Abwesenheit. Eine Garantie, dass ein System die gestellten Anforderungen erfüllt, kann durch formale Methoden gegeben werden.

Die in dieser Arbeit vorgestellten Ansätze tragen dazu bei, die Software-Entwicklung in kleinen und mittleren Unternehmen durch Methoden der formalen Verifikation zu verbessern und zu unterstützen. Dabei werden die Vorteile von kleinen gegenüber großen Unternehmen genutzt und ausgebaut. Dazu zählen die ausgeprägte Nähe zum Kunden sowie ein hohes Maß an Flexibilität und Wirtschaftlichkeit. Die Systemkomplexität der meisten Projekte sowie die Prozessstrukturen können positiv zur Akzeptanz für die Einführung von formalen Methoden in den jeweiligen Entwicklungsprozess beitragen.

Der erste Ansatz befasst sich mit der Analyse von Zeitanforderungen für eingebettete Systeme basierend auf der formalen Methode des Model-Checkings. Dabei wird für ein bestehendes Variantensystem für Steuergeräte ein Task-System mittels Uppaal modelliert und eine Einplanbarkeitsanalyse auf Basis von Zeitautomaten vorgestellt. Zur Verwaltung der Varianten wurde ein Framework basierend auf pure::variants entworfen und eine bestehende Software-Plattform evolutionär in eine Produktlinie umgewandelt. Damit können sich Unternehmen stärker auf die individuellen Kundenwünsche fokussieren und vorhandene Komponenten effizient und mit hoher Qualität wiederverwenden.

Der zweite Ansatz zur Verbesserung der Software-Qualität befasst sich mit der Verifikation von Programmcode eingebetteter Systeme durch den Model-Checker Arcade. Hierbei wurde speziell das Formulieren von formalen Anforderungen und die Anwendbarkeit im industriellen Umfeld untersucht. Mittels dieses Ansatzes konnten sowohl Fehler im Programmcode lokalisiert als auch das Einhalten von Anforderungen gezeigt werden. Der Einsatz von Binär-Code-Verifikation kann den Testaufwand reduzieren, aber nicht ersetzen. Der Vorteil für Unternehmen ist allerdings, dass diese Methode das Ausbleiben von Fehlern beweisen kann, was durch herkömmliches Testen nicht möglich ist.

Insgesamt wurde ein Ansatz zur Integration formaler Methoden in den Entwicklungsprozess eines kleinen und mittleren Unternehmens vorgestellt, erfolgreich mit entsprechender Werkzeugunterstützung umgesetzt und evaluiert. Mit Hilfe der gezeigten Methoden ist es möglich, den Testaufwand zu reduzieren und die Qualität von automobilen Steuerungssystemen schon frühzeitig in den wichtigen Phasen der Entwicklung zu steigern.

Abstract

The number of control units within upper class vehicles has steadily increased over the last 15 years and is currently around 100 units. The majority of all innovations in the vehicle are generated by electronics and software. This makes software, on the one hand, one of the most important drivers of innovation for companies in the automotive industry. On the other hand, it involves a high risk potential: programming errors.

With international standards and stricter requirements for software quality the industry is trying to counteract this risk. However, the complexity of the systems is growing due to the increasing diversity of variants in order to be able to fulfil all the wishes of the end customer individually. The testing of such software systems can only show the presence of errors, but not their absence. A guarantee that a system fulfils the requirements can be provided by formal methods.

The approaches presented in this thesis help to improve and support software development in small and medium-sized enterprises by means of formal verification methods. In doing so, the advantages of small over large companies should be utilised and enhanced. This includes the close proximity to the customer as well as a high degree of flexibility and profitability. The system complexity of most projects as well as the process structures can positively contribute to the adoption of formal methods in the respective development process.

The first approach deals with the analysis of timing requirements for embedded systems based on the formal method of model checking. In this case, a task system is modelled using Uppaal for an existing variant system for control units, and a schedulability analysis based on timed automata is presented. To manage the variants, a framework based on pure::variants was designed and an existing software platform was transformed into a product line. This allows companies to focus more on individual customer requirements and to reuse existing components efficiently and with high quality.

The second approach to improve the quality of software is to verify the program code of embedded systems through the model checker Arcade. Specifically, the formalization of formal requirements and the applicability in the industrial environment were analysed. Errors in the program code could be localized as well as compliance with requirements were shown. The use of binary code verification can reduce the test effort, but will not replace it. The advantage for companies is, however, that this method can prove the absence of errors, which is not possible by conventional testing.

Overall, an approach to the integration of formal methods into the development process of a small and medium-sized enterprise was presented, successfully implemented and evaluated with appropriate tool support. With the methods shown, it is possible to reduce the test effort and to increase the quality of automotive control systems at an early stage in the important phases of development.

Danksagung

Grundlage für die erzielten Ergebnisse ist die kooperative und freundschaftliche Zusammenarbeit des RWTH Lehrstuhls Informatik 11 - Embedded Software mit der VEMAC GmbH & Co. KG, durch die sie erst möglich wurde.

An erster Stelle gilt mein Dank meinem Doktorvater Prof. Dr.-Ing. Stefan Kowalewski für seine wissenschaftliche und methodische Anleitung und konstruktive Rückmeldung über die vielen Jahre hinweg. Prof. Dr.-Ing. Sebastian Engell danke ich für die Übernahme des Zweitgutachtens sowie für die fruchtbaren Hinweise während der Zusammenarbeit im MULTIFORM Projekt. Desweiteren danke ich Prof. Dr. rer. nat. Leif Kobbelt als Vorsitzenden der Prüfungskommision und ebenfalls Prof. Dr. rer. nat. Matthias Müller als Beisitzer.

Prof. Dr.-Ing. Michael Reke hat großen Anteil am Gelingen meiner Dissertation, denn er war unermüdlich an meiner Seite und hatte gewöhnlich zum richtigen Zeitpunkt die notwendigen aufbauenden Worte sowie Ratschläge, mit denen er mich bis zuletzt begleitet und unterstützt hat. Ihm möchte ich daher ganz besonders danken. Bei Dr. Martin Düsterhöft bedanke ich mich ferner sehr für das Initiieren und Ermöglichen meines Promotionsvorhabens.

Frau Margit Offergeld und Herrn Dr. Johannes Offergeld danke ich für ihr entgegengebrachtes Vertrauen, mit diesem und durch die kontinuierliche Begleitung der gesamten VEMAC - im Speziellen seitens Michael Kiausch und Axel Koblenz - diese Arbeit erst realisierbar war. Vor allem die tiefschürfenden Diskussionen und die konstruktive sowie immer amüsante Zusammenarbeit waren bedeutsam für deren Gelingen.

Meinen Studenten Surapa Ratanaprutthakul, Thorsten Will, Kriengkrai Krirkkawin danke ich, denn sie haben tatkräftigen Anteil an den Ergebnissen dieser Arbeit und trugen zu einem anregenden sowie ebenso angenehmen Arbeitsumfeld bei.

Dr.-Ing. Martin Hüfner und Volker Kamin sowie Dr. rer. nat. Sebastian Biallas bin ich dankbar für viele fachliche Gespräche und die multi-formale Zusammenarbeit. Überaus geholfen hat mir Dr.-Ing. André Stollenwerk, indem er mir den direkten Draht zum Lehrstuhl ermöglichte und darüber hinaus mich durch viele Diskussionen inspirierte.

Meinen Eltern Doris und Reinhard sowie meiner Schwester Anja bin ich sehr dankbar für die anhaltende Hilfestellung und Wegbereitung über all die Jahre hinweg, wodurch sie mich erst dahin gebracht haben, wo ich heute stehe.

Ferner danke ich meiner Frau Henrike für die liebevolle und ausdauernde Unterstüzung auch in schwierigen Zeiten sowie für das Rückenfreihalten und zahlreiche Zeitgeschenke. Meine beiden Töchter Antonia und Mathilda haben mir immer wieder neu Mut gemacht und mich motiviert. Ihnen möchte ich vor allem danken und hieran verdeutlichen, dass Durchhaltevermögen und Ausdauer, wovon mir viel abverlangt wurde, lohnenswert und zielführend sind.

Hildesheim, im Oktober 2019

Inhaltsverzeichnis