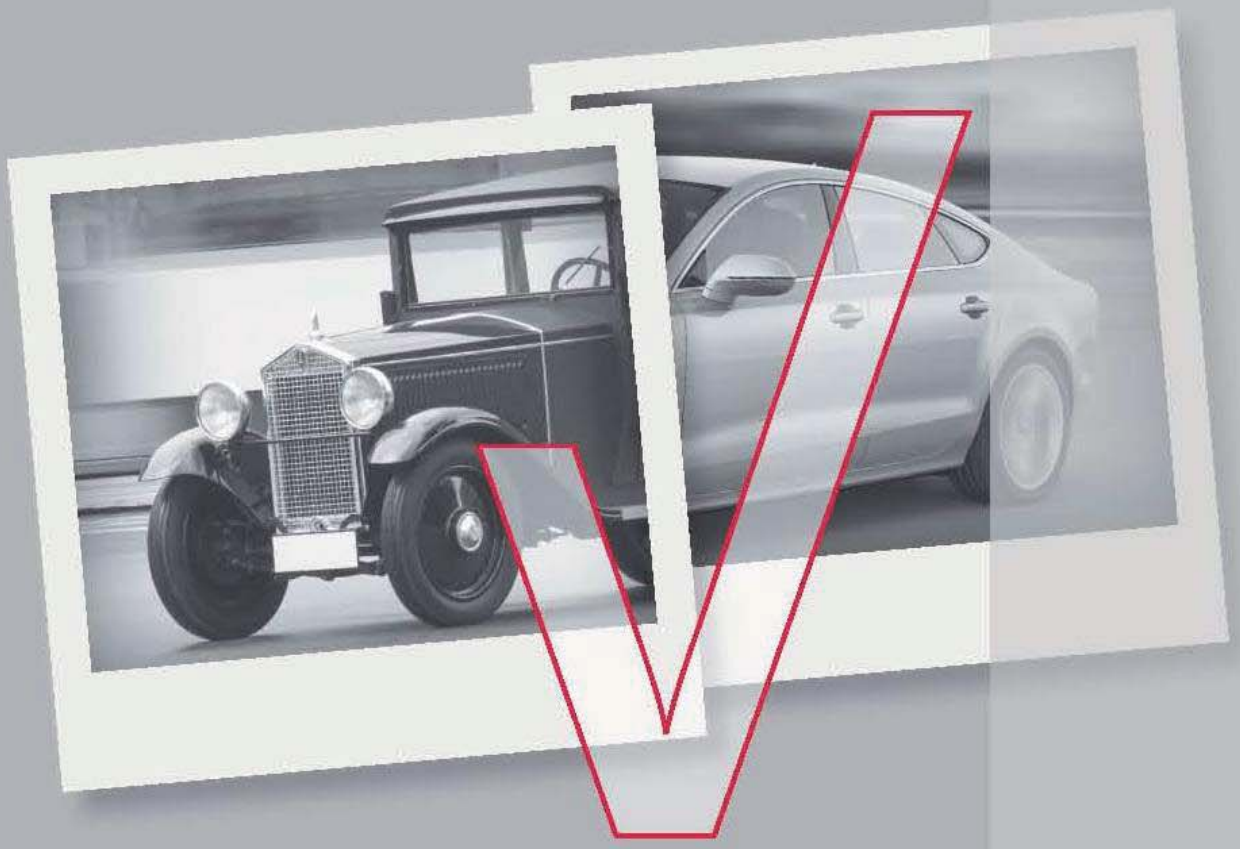
Audi
Dissertationsreihe

Spezifikation und Verifikation von eingebetteten Echtzeitsystemen in Fahrzeugen

Sebastian Siegl



Cuvillier Verlag Göttingen

INI.FAU
INGOLSTADT INSTITUTE OF THE FRIEDRICH-ALEXANDER-UNIVERSITÄT ERLANGEN-NÜRNBERG

Audi-Dissertationsreihe, Band 52

Specification and Verification of Embedded Real-Time Systems in the Automotive Domain

Spezifikation und Verifikation von eingebetteten Echtzeitsystemen in Fahrzeugen

Der Technischen Fakultät der
Universität Erlangen-Nürnberg
zur Erlangung des Grades

DOKTOR-INGENIEUR

vorgelegt von

Sebastian Siegl

Erlangen - 2011

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.

1. Aufl. - Göttingen: Cuvillier, 2011
Zugl.: (TU) Erlangen-Nürnberg, Univ., Diss., 2011

978-3-86955-966-7

Als Dissertation genehmigt von
der Technischen Fakultät der
Universität Erlangen-Nürnberg

Tag der Einreichung:	**18. Juli 2011**
Tag der Promotion:	**14. November 2011**
Dekan:	**Prof. Dr.-Ing. Reinhard German**
Berichterstatter:	**Prof. Dr.-Ing. Reinhard German**
	Prof. Dr. Klaus Meyer-Wegener

Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21
www.cuvillier.de

1. Auflage, 2011
Gedruckt auf säurefreiem Papier

978-3-86955-966-7

Trademarks appear throughout this thesis without any trademark symbol; they are the property of their respective trademark owner. There is no intention of infringement; the usage is to the benefit of the trademark owner.

Abstract

Increasingly intelligent and interconnected systems are embedded in automobiles to make road vehicles even more safe and economical. The realization of these systems is only possible by making use of complex and distributed software. Its development poses a challenge for the methods of specification, validation, and verification. Upcoming international standards such as ISO 26262 explicitly state requirements for the methods used for specification, design, and verification of safety-related systems.

In this thesis, a method for the formal specification and systematic verification of embedded systems is presented. The focus is on the building and gaining of confidence in the quality of the system under development with the appliance of appropriate methods during the entire development process. Key aspects are early identification of design errors and estimation of the quality of the implementation in late development phases, in which systems are integrated and verified for field usage.

For this purpose, the intended behavior of the system is analyzed and transformed into a formal model at an early development stage. The formal model serves as a test model for the following validation and verification of the system under development. Additionally, automated executable test cases can be derived from the model.

Model centric approaches that are used in industry, e.g. on the basis of Markov chain usage models, do not allow the systematic and explicit integration of time and timing dependencies in the test model. Yet time is, especially in the case of safety critical embedded systems, a vital element, that is to be considered throughout the whole development process from the specification to the final testing activities.

Time Usage Models are presented in this thesis as test models. They allow for the systematic integration of time and timing requirements already during the creation of the test model. The requirements are analyzed at this step and specified by the model unambiguously and completely on the chosen abstraction level.

Initial design decisions and first implementations can be validated in agile development processes with the generation of automated executable test cases in a Model in the Loop environment. In the late development phases, e.g. in system integration testing, test cases can be derived for verification on Hardware in the Loop test benches.

On the basis of a Time Usage Model it is possible to determine classic and newly developed indicators for the estimation of the test effort and dependability of the system under development. The timing information in the model is explicitly considered in the computations. For this reason, a realistic estimation of the test effort to achieve test goals and to meet test end criteria is made possible.

Strategies for test case generation from Time Usage Models allow for the derivation of test cases to verify non-functional requirements. Newly developed algorithms use the time information in the model to generate test cases that reflect the variability in timing in real usage in addition to the variability in the stimulation itself. Hence, a more realistic verification of functional and non-functional requirements is made possible with it.

Two case studies are presented that were conducted in cooperation with AUDI AG Ingolstadt. The first case study was performed in the early development phase of active safety functionalities, the second in the late development phase of system integration of the energy management system.

The results of both case studies substantiate the benefits of the appliance of Time Usage Models. The system requirement specification was clarified and improved in both case studies. Additionally, the quality of the implementation could be improved in both case studies because of the application of Time Usage Models. Additional flaws and errors, that had not been detected in the existing processes before, were identified and corrected.

Kurzfassung

Durch den Einsatz intelligenter eingebetteter Systeme werden zunehmend sichere und effizientere Automobile entwickelt. Die Realisierung dieser Systeme ist nur mit komplexer und verteilter Software möglich. Die hierfür eingesetzten Methoden zur Spezifikation, Validierung und Verifikation werden durch diese Entwicklung vor neue Herausforderungen gestellt. Zukünftige internationale Standards wie die ISO 26262 stellen explizite Anforderungen an die Methoden zu Spezifikation, zur Auslegung und funktionalen Absicherung von sicherheitskritischen Systemen.

In dieser Arbeit wird eine Methode vorgestellt zur Spezifikation und systematischen Absicherung von eingebetten Systemen. Ein Hauptaugenmerk ist die Vertrauensbildung und Vertrauenserhöhung in die Qualität des in der Entwicklung befindlichen Systems durch Einsatz geeigneter Methoden in der Spezifikations-, der Design- und der Testphase. Schwerpunkte sind die frühzeitige Identifikation von Entwurfsfehlern und die Abschätzung der Qualität der Implementierung in den späteren Entwicklungsphasen.

Hierfür wird das beabsichtige Sollverhalten des Systems frühzeitig analysiert und in ein formales Modell überführt. Das formale Modell fungiert für die anschließenden Schritte als Testmodell und ermöglicht die Generierung von automatisiert ausführbaren Testfällen.

In der Industrie eingesetzte modellzentrierte Methoden, z.B. auf Basis von Markovketten-Benutzungsmodellen, sehen keine systematische explizite Integration von Zeit und zeitlichen Abhängigkeiten in das Testmodell vor. Jedoch ist Zeit, insbesondere bei sicherheitskritischen eingebetteten Systemen, ein zunehmend entscheidender Faktor, der von der Spezifikation bis hin zu den abschließenden Testaktivitäten zu berücksichtigen ist.

In dieser Arbeit werden Zeit-Benutzungsmodelle als Testmodelle vorgestellt. Diese ermöglichen die systematische Berücksichtigung von Zeit und zeitlichen Anforderungen bereits bei der Erstellung des Testmodells. Die Anforderungen werden hierbei bereits einer ersten Analyse unterzogen und durch das Modell auf dem gewählten Abstraktionsniveau eindeutig und vollständig beschrieben. Das Modell dient als Basis für alle weiteren Schritte zur Auslegung und der Absicherung des Systems.

Erste Designentscheidungen und Implementierungen können durch automatische und systematische Generierung von Testfällen für die Model-in-the-Loop-Ausführung frühzeitig in agilen Entwicklungsprozessen validiert werden. In den späteren Entwurfsphasen, z.B. im Systemintegrationstest, können Testfälle zur Verifikation an Hardware-in-the-Loop-Prüfständen generiert werden.

Auf Basis des Zeit-Benutzungsmodells können etablierte und neu entwickelte Testmanagementindikatoren zur Abschätzung des Testaufwands bestimmt werden. Die im Modell hinterlegte Zeitinformation wird explizit in den Berechnungen berücksichtigt. Damit ist eine realistische Abschätzung des Testaufwands zur Erreichung von Testzielen und Testendekriterien möglich.

Strategien zur Testfallgenerierung von Zeit-Benutzungsmodellen ermöglichen die Ableitung von Testfällen zur Absicherung von nicht funktionalen Anforderungen. Neu entwickelte Algorithmen verwenden die im Modell hinterlegte Zeitinformation, um Testfälle zu generieren, die neben der Varianz in der Stimulation auch die Varianz in der Zeit in Testfällen abbilden. Damit wird eine realistische Verifikation von funktionalen und nicht funktionalen Anforderungen ermöglicht.

Zwei in Zusammenarbeit mit der AUDI AG durchgeführte Fallstudien werden vorgestellt. Die erste wurde in der frühen Entwicklungspase von Funktionen der aktiven Fahrzeugsicherheit, die zweite in der späteren Systemintegrationsphase des Energiemanagementsystems durchgeführt. In beiden Fallstudien zeigten sich die Vorteile des Einsatzes von Zeit-Benutzungsmodellen. Die Systemanforderungsspezifikationen wurden in beiden Fällen verbessert. Ebenso konnte in beiden Fallstudien die Qualität der Implementierung durch den Einsatz von Zeit-Benutzungsmodellen gesteigert werden, wobei Mängel identifiziert und behoben wurden, die in den etablierten Methoden nicht erkannt wurden.

Contents

Chapter 1

Introduction

The thesis starts with a brief introduction of automotive systems and the importance of embedded software in modern automobiles. An outline of challenges in the development of embedded automotive software is given. Next, the topics of the thesis, the key issues in the development and the contributions of this thesis are stated. The chapter closes with an outline of the thesis and a list of publications, in which aspects and intermediate development stages of the presented work are published.

1.1 Motivation

The history of automobiles started on January 29th 1886 with patent number 37435, granted by the *Kaiserliche Patentamt des deutschen Reiches* [14]. The patent was issued for the invention of a *Fahrzeug mit Gasmotorenbetrieb*, i.e. a vehicle with gas engine. This date can be considered as the birthday of cars which have changed the world in a significant way.
As automobiles have changed people's life, automobiles themselves have evolved tremendously compared to the first one as depicted in Figure 1.1. Modern cars embed complex distributed real time systems in order to realize even more safe, comfortable, and economical vehicles. The value of the installed electronics per automobile was in the year 2000, on a world wide average, 155 USD. In 2020, it is expected to be 590 USD in an average car [39].

In 2002, software and electronics already led to 40% of the manufacturing costs of an automobile. The availability of increasingly powerful and cheaper hardware makes the implementation of increasingly elaborated functionality in mass production possible. The system's complexity increases accordingly.

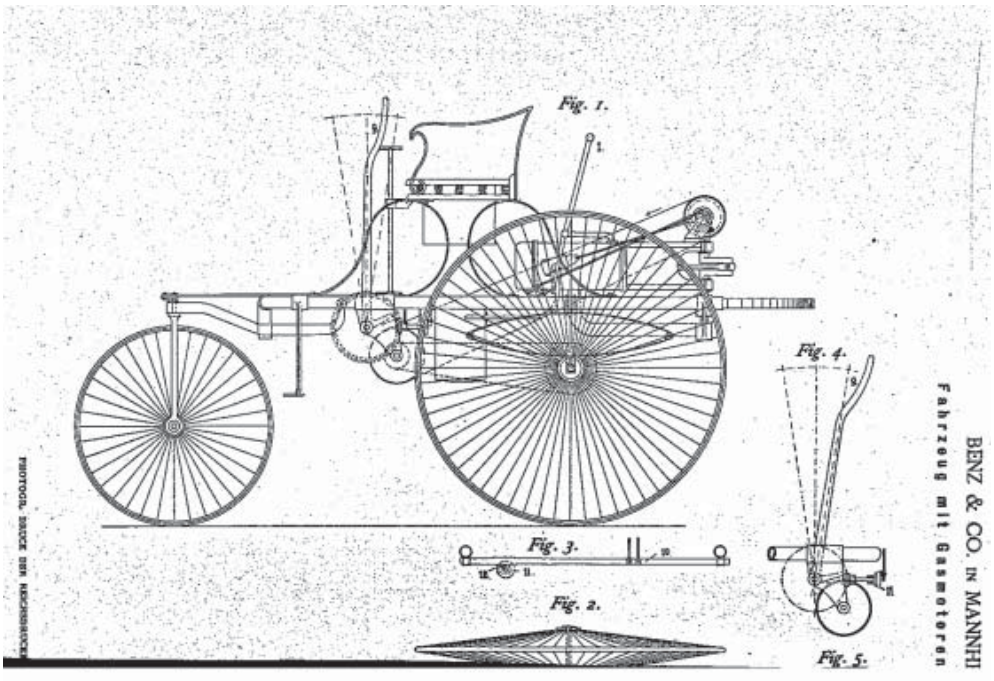


Figure 1.1: Detail of Patent No. 37435: Fahrzeug mit Gasmotorenbetrieb

Some figures about the current Audi A8: The current premium upper class automobile has 270 MB of embedded functional software. The software is distributed on 100 electronic control units (ECUs), connected with 7 bus systems. 2370 wires are installed to connect the ECUs and the associated devices.

The ratio of innovations realized with software in the automotive industry has raised from 20% to 85% over the last years [53] and is still growing [78, 115]. Ferdinand Dudenhöffer, Director of the Center of Automotive Research (CAR) of the FH Gelsenkirchen in 2002 [68], stated that electricity and electronics provide the base for 90% of all innovations in automobiles in the near future.

As a result, the importance of the software embedded in automobiles to customers and hence market shares will be vital. In [24] the conclusion is that this development establishes software as a key technology in the automotive domain. And only software enables the car manufacturers to integrate functionality for the customer to use virtually any electronic device like smart phones and laptops in combination with services provided by the car. Each device that can interact with the car adds another possible configuration to the possible ones of the car and increases the configuration space of the embedded software.

This thesis focuses on software aspects of embedded systems. Software is expected to have the greatest impact on customers, industry and market shares

in the automotive industry [95, 26]. The example in Figure 1.2 illustrates the development of modern automobiles to complex systems with integrated hardware and software to present the advances achieved compared with the first automobile in Figure 1.1.

Figure 1.2: Inner View of Components of Modern Automobile

The realization of innovations in modern vehicles is only possible by a shift from electronics to software [95].

Software development offers flexibility to build more variants and, moreover, potential to reduce development time and costs. The standards released by standardization committees like the Association for Standardization of Automation and Measuring Systems (ASAM) allow for the reuse of artifacts in different variants. However, as safety critical functionality is realized by software, it plays a critical role and a software failure can result in expensive damage to the hardware or traffic participants. As a consequence of this, the quality assurance of the entire development process, and of the resulting software is of vital interest.

However, 44% of the embedded system designs meet only 20% of the functionality and performance expectations [53]. In 2005, Dr. John J. Wargin from Hewlett-Packard stated that 60% to 70% of the warranty efforts trace back to software failures [141]. A lack of appropriate test approaches for functional validation and verification contributes to this figures. Thus, a method to improve