



**Hochschule Heilbronn**

**Studiengang Electronic Business**

# **Diplomarbeit**

Modellierung eines Rekonfigurationsmodells  
zur Konfiguration der Anwendungs-Software in eingebetteten Systemen

**Betreuer:** Prof. Dr. Michael Gröschel, Hochschule Heilbronn  
Dipl.-Inf. Alexander Schäfer, Robert Bosch GmbH

**Firma:** Robert Bosch GmbH, Abstatt  
Bereich Chassis Systems Control  
Abteilung Engineering Vehicle Dynamics

Verfasser: Dario Toderico

Matrikelnummer: 161329

14.01.08

## Summary

Diese Diplomarbeit stellt einen Proof of Concept für die Integrierbarkeit des am Fraunhofer IESE entwickelten „Methodologies and Architectures for Runtime adaptive embedded Systems“(MARS)-Frameworks in die Entwicklungsprozesse und -werkzeuge der Fahrdynamikregelungen der Robert Bosch GmbH dar.

Eingebettete Systeme verrichten heutzutage in fast allen Geräten des täglichen Lebens ihren Dienst. Während die Fehlfunktion einer Waschmaschine als nicht lebensbedrohlich angesehen wird, ändert sich dieser Umstand bei Systemen in Kraftfahrzeugen. An solche sicherheitsrelevanten Systeme werden erhöhte Anforderungen an die Verlässlichkeit gestellt.

Anhand der Betrachtung eingebetteter Systeme und am Beispiel der ESP-Funktion „elektronischer Bremsassistent“ wird gezeigt, dass die Verlässlichkeit eine wichtige nicht-funktionale Anforderung an sicherheitsrelevante Systeme darstellt. Einen Ansatz bei der Entwicklung sicherer und zugleich zuverlässiger eingebetteter Systeme, verfolgt die Erweiterung des Systems um adaptive Aspekte im Bereich der Software. In dieser Arbeit wird eine konkrete Vorgehensweise zur Rekonfiguration der Systeme, die „graceful degradation“, betrachtet.

Die „graceful degradation“, auf Basis pre-determinierter Regelsätze, wird bereits in den Fahrassistenzsystemen der Robert Bosch GmbH eingesetzt. Aufgrund der hohen und weiter steigenden Gesamtkomplexität der Systeme, stellt die Verbesserung der Verlässlichkeit durch die „graceful degradation“ eine komplexe, zeit- und kostenintensive Aufgabe dar.

Es wird gezeigt, dass sich mithilfe der Service-basierten Methodik eine Komplexitätsreduktion erreichen lässt. Anhand von Beispielen wird erläutert wie sich ein System, bzw. dessen Verhalten, abstrakt darstellen lässt. Die Service-basierte Methodik bildet die Grundlage für das am Fraunhofer IESE entwickelte MARS-Framework. Dieses definiert zum Zweck der Komplexitätsreduktion und der Anwendung von Software Engineering Methoden, explizite Modellierungs- und Analysemethoden. In dieser Arbeit werden die erweiterten Ansätze zur Architekturmodellierung erläutert, welche eine formale Spezifikation des Adaptionssverhaltens ermöglichen.

Die Entwicklung der Fahrassistenzsysteme der Robert Bosch GmbH erfolgt mit der Entwicklungsumgebung ASCET, auf Basis funktionaler Modelle bereits modellgetriebenen. Diese Modelle enthalten lediglich eine implizite Adaptionsspezifikation. Es wird daher eine Vorgehensweise und Notation entwickelt, mit welcher die funktionalen Modelle um eine formale Adaptionsspezifikation (auf Basis von MARS) erweitert werden. Durch diese explizite Spezifikation des Adaptionssverhaltens werden Simulationen des Laufzeit- und

Fehlerverhaltens ermöglicht. Aufgrund der Tatsache, dass ASCET über keine Möglichkeit zur expliziten Simulation des Adaptionverhaltens verfügt, wird die Simulation in der, am Fraunhofer IESE entwickelten, MARS Entwicklungs- und Simulationsumgebung „Composer“ durchgeführt. Um aus erweiterten funktionalen ASCET-Modellen, automatisch simulierbare MARS-Modelle in Composer generieren zu können, wurde der Composer in dieser Arbeit durch ein Eclipse Plug-In erweitert. Das Plug-In ermöglicht die Extraktion der benötigten Informationen aus einem ASCET-Export und instanziiert anschließend automatisch MARS-Modelle. Auf den generierten MARS-Modellen können die angestrebten Simulationen des Adaptionverhaltens durchgeführt werden.