TU Clausthal

Abschlussvortrag Masterarbeit Andreas Vorwald

„Formale Verifikation von Reaktiven Systemen am Beispiel einer Fahrzeugfunktion“

Kontext und Motivation

In der Automobilbranche werden zunehmend herkömmliche Regler eines Fahrzeugs durch komplexe software-intensive Systeme ersetzt, um bessere Ergebnisse zu erzielen. Bevor solche Systeme in Betrieb genommen werden dürfen, fordern Gesetzgeber bzw. Zertifizierungsstellen einen Nachweis auf Korrektheit des Systems in Bezug auf die Anforderungen. Typischerweise erfolgen Korrektheitsnachweise über Test- bzw. Simulationsverfahren. Hierbei werden Szenarien von Experten definiert, auf deren Basis Test- bzw. Simulationsumgebungen das zu verifizierende System stimulieren. Allerdings lässt sich hierdurch insbesondere bei nichtlinearen Systemen schwer nachweisen, dass unerwünschtes Verhalten nie auftreten wird (Sicherheitsanforderungen). Eine andere vielversprechende Methode Korrektheit von Systemen nachzuweisen sind formale Verifikationsverfahren. Diese können mit geeigneten mathematischen Verfahren den Zustandsraum des zu verifizierenden Systems durchsuchen und bei Anforderungsverletzungen Ausführungspfade liefern, wie das unerwünschte Systemverhalten zustande kommt. Diese Verfahren sind in unterschiedlichen Verifikationswerkzeugen implementiert.

Software-intensive Regler lassen sich als reaktive Systeme beschreiben. Reaktive Systeme reagieren zyklisch auf externe Stimuli der Umgebung und berechnen damit Größen, mit denen Aktuatoren die Umgebung wiederum beeinflussen. Hierbei unterliegen die Sensoren, mit denen externe Stimuli gemessen werden, Ungenauigkeiten bzw. Abweichungen. Zudem besitzen komplexe reaktive Systeme i. d. R. nichtlineares Verhalten.

Um reaktive Systeme verifizieren zu können, muss das System unter Berücksichtigung von Toleranzen und Ungenauigkeiten modelliert werden. Jedoch verhält sich die Umgebung eines reaktiven Systems häufig anders als erwartet. Solche Ungenauigkeiten der Umgebung können durch Fehlermodelle beschrieben werden. Außerdem müssen die Systemanforderungen in einer passenden Sprache formal spezifiziert werden. Mithilfe eines abstrakten Modells des Systems, welches als Eingabe für ein Verifikations-Tool dient, kann das komplexe System gegenüber seinen Anforderungen formal verifiziert werden.

Fragestellung

Das Ziel dieser Masterarbeit ist, Methoden zur formalen Verifikation zur Absicherung von reaktiven Systemen zu recherchieren und am Beispiel einer Fahrzeugfunktion zu demonstrieren. Hierbei sollen die möglicherweise zur Verifikation geeigneten Sprachen und Tools ausgesucht und auf das gegebene System angewendet werden. Es muss folgende Frage beantwortet werden:

- Wie können komplexe, nicht lineare reaktive Systeme in Bezug auf ihre Anforderungen und unter Berücksichtigung von Fehlermodellen formal verifiziert werden?

TU Clausthal

Betreuer der Arbeit:	Prof. Dr. Andreas Rausch, Prof. Dr. Rüdiger Ehlers
Datum:	Dienstag, 26. Mai 2020, 12:30 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/b/sim-uc9-rvy