FACHHOCHSCHULE
TECHNIKUM WIEN

Einreichung zum
„FH Best Paper Award der Stadt Wien“

Kategorie: Beste Diplom- bzw. Masterarbeiten

Titel der Arbeit: Model Checking and Static Analysis of Intel MCS-51 Assembly Code

Autor: Thomas Reinbacher, MSc
Geburtsdatum: 09-11-1984
Adresse: Weidenweg 44
2020 Kleinstelzendorf

Studiengang: Master in Embedded Systems
Institut: Embedded Systems

Erstgutachter/Betreuer: FH-Prof. DI. Dr. Martin Horauer
Zweitgutachter: DI. Michael Kramer

Kurzfassung

Die Diplomarbeit „*Model Checking and Static Analysis of Intel MCS-51 Assembly Code*“ beschäftigt sich mit der formalen Verifikation von Software für eingebettete Systeme (Embedded Systems). Im Rahmen der Verifikation wird kontrolliert, ob die Software der Spezifikation entspricht und ihre Aufgaben korrekt erfüllt. Diese Kontrolle ist in der Regel aufgrund der starken Interaktion der untersuchten Systeme mit deren Umgebung ein nicht-triviales Problem. In der industriellen Praxis wird die Verifikation mittels Testen durchgeführt. Hierbei werden verschiedene Kombinationen an die Eingänge eines Systems angelegt und das entsprechende Verhalten des Systems wird beobachtet und analysiert. Mit dieser Methode kann jedoch aufgrund der großen Vielfalt an Eingangsmöglichkeiten nur ein sehr kleiner Prozentsatz des möglichen Testraums abgedeckt werden. Im Rahmen dieser Diplomarbeit wurden Konzepte und Ansätze zur Lösung dieses Problems basierend auf *Assembler-Code Model Checking* und *statischer Analyse* implementiert und erarbeitet und anhand einer industriellen Fallstudie evaluiert. Ansätze wie dieser verfolgen langfristig das Ziel, den EntwicklerInnen von Embedded Systems Software (welche in modernen Fahrzeugen, Aufzügen, Flugzeugen, etc. eingesetzt wird) eine automatisierte und vollständige Verifikationsmethode zur Verfügung zu stellen. Von der Verbesserung der Entwicklungsmethoden profitiert letzten Endes auch der Endanwender, der in den Genuss von verlässlichen und sicheren Produkten kommt.

Stichworte: Software für eingebettete Systeme, Formale Verifikation, Statische Analyse, Assembler Code Model Checking;

Abstract

The master thesis „*Model Checking and Static Analysis of Intel MCS-51 Assembly Code*“ deals with formal verification of embedded systems software. The main purpose of the verification effort is to figure out whether the software under inspection fulfils a given specification. Due to the strong interaction of embedded systems with their environment checking for correctness of the software is a delicate and challenging task. In industrial practice verification tasks are often addressed using testing. Herein, a system is stressed using various different input stimuli and the systems reaction is observed and analysed. It is, however, widely known that testing is only capable to address a very limited part of the entire testspace. This thesis presents novel concepts and approaches to tackle these issues based on assembly level model checking and static analysis. The feasibility of these approaches is demonstrated by model checking a real life industrial embedded systems software application. The implemented concepts allow the automated verification of the case study software using a kind of “push button” approach.

The achievements of the master thesis can be seen as a step towards a fully automatic embedded software verification methodology, which is still a major open issue in modern-day software development. In the long run, fully automated verification approaches will support the day-to-day practice of embedded software design and help to close the verification gap while increasing productivity of the individual developer. The end user of the applications will benefit from increased safety, reliability, and trustworthiness in new products.

Keywords: software for embedded systems, formal verification, static analyis, assembly code model checking;