Misusing Model-Checker to Generate Correct Configurations in Embedded Systems

Christine Jakobs and Matthias Werner, Technische Universität Chemnitz

Viele eingebettete Systeme sind sicherheitskritische Systeme unterliegen Standards, die verlangen, dass die Systemkorrektheit mit formalen oder halbformalen Methoden nachgewiesen werden müssen. Ein typischer Ansatz bei den formalen Methoden ist dabei, das System zu modellieren und die Korrektheit mit einem Modellchecker nachzuweisen.

In diesem Beitrag zeigen wir am Beispiel des TLA+/PlusCal-Modell-Checkers, wie Modell-Checking nicht nur analytisch zum Korrektheitsnachweis, sondern auch konstruktiv zum Finden von a-priori korrekten Konfigurationen (im Sinne eines MDD-Ansatzes) genutzt werden kann. Dieser Ansatz wird am Beispiel der Erstellung von Timeline-Schedules demonstriert, und die erweiterte Anwendung auf das Kompositionsproblem in eingebetteter Software diskutiert.