

Praxis der Forschung

Ermittlung von Zuverlässigkeitsmaßen durch unvollständige Verifikation

Hintergrund

Es gibt viele Verifikationsverfahren, die die Korrektheit eines Programms nur teilweise überprüfen, dafür aber schneller und einfacher sind als vollständige Verfahren. Bounded Model Checking ist z.B. eine Technik, bei der die Korrektheit eines Programms für nur Programmausführungen beschränkter Länge gezeigt wird, indem z.B. Schleifen ausgerollt werden.

Es gibt auch Verfahren, mit denen man aus solchen unvollständigen Beweisen bestimmen oder abschätzen kann, für wie viele mögliche Eingaben das Programm sich korrekt verhält. Bei ereignis- und sensorgesteuerten Prozessen wie Ampelschaltungen oder Steuerungssoftware ergibt es allerdings nicht wirklich Sinn, von einer konkreten Eingabe zu sprechen, da das Programm immer wieder auf neue Eingaben reagiert, die es teilweise selbst beeinflusst. Stattdessen wüsste man gerne, wie viele Fehler im Durchschnitt in einer bestimmten Zeitspanne passieren oder wie oft der Prozess im Durchschnitt abstürzt.

Aufgabe

Das Ziel dieses Projektes ist, mit Hilfe von Machine Learning ein Softwarezuverlässigkeitsmodell zu entwickeln, das als Eingabe eine unvollständige Verifikation (z.B. von BMC) erhält und als Ausgabe verschiedene Zuverlässigkeitsmaße (z.B. die Anzahl der verbleibenden Fehler im Programm oder die *Mean time to failure*) abschätzt.

Ansprechpartner

- Florian Lanzinger, lanzinger@kit.edu, Büro 50.34R203