Zusammenfassung

Hohe Anforderungen an die Funktionssicherheit eines Automobils fordern von der Entwicklung ein Vorgehen, bei dem die Einhaltung der Funktionssicherheit überprüft werden kann. In der Praxis werden zur Verifikation der Funktionssicherheit die Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) und die Fehlerbaumanalyse (FTA) eingesetzt. Der steigende Anteil präziser formaler Modelle in der Entwicklung ermöglicht den steigenden Ansprüchen aus Normen und der Automobilindustrie hinsichtlich der Funktionssicherheit gerecht zu werden. Bei geeigneten formalen Modellen kann weiter die Verifikation teilweise automatisiert und so die Qualität der Entwicklung auf einen konstant hohen Stand gebracht werden.

Der Schwerpunkt der Arbeit ist der Entwurf formaler Modelle und Modellierungstechniken mit denen die FMEA und die FTA formal durchgeführt werden können. Die Modelle und Modellierungstechniken beschreiben das Verhalten der Systeme oder Beziehungen zwischen Systemverhalten. Sie sind für eine Integration mit bestehenden Artefakten der Entwicklung geeignet. Die Verhaltensmodellierung ist an die in der Entwicklung verwendeten Modellierungswerkzeuge, wie Simulink™, und an die verwendeten Dokumente der Entwicklung angepasst. Konsistent zur Verhaltensmodellierung werden Modellierungstechniken für Fehlverhalten definiert. Fehlverhalten werden als Modifikationen des Sollverhaltens ausgedrückt. Um die möglichen Fehlverhalten eines Systems zu erfassen, werden potentielle Fehler, die Fehlverhalten verursachen können, vorgegeben. Zu den jeweiligen Modellierungstechniken für Fehler wird allgemein der Begriff des Fehlerzusammenhangs formal definiert. Weiter werden spezifische in den Methoden FMEA und FTA verwendete Zusammenhänge formalisiert, um eine Automatisierung zu ermöglichen. Abschließend zeigt die Arbeit Möglichkeiten auf, die Durchführung der Analysen zu automatisieren.

Inhaltsverzeichnis