

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-Möglichkeiten- 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 SimulinkTM, 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

1	Einleitung	1
1.1	Motivation und Problemstellung	1
1.2	Beitrag der Arbeit	2
1.3	Begleitende Fallstudien	3
1.4	Related Work	4
1.5	Kapitelübersicht	5
2	Funktionssicherheitsanalyse	9
2.1	Definitionen (Terminologie)	11
2.1.1	Fehler	11
2.1.2	Zusammenspiel von Fehlern	14
2.1.3	Bewertung der Fehler	16
2.2	Sicherheitsanalyse in der Systementwicklung	19
2.3	Fehler-Möglichkeit- und Einfluss-Analyse	22
2.4	Fehlerbaumanalyse	32
2.5	Zusammenführung von Analysen	36
2.6	Zusammenfassung	37
3	Grundlegende Modelle und Modellierungstechniken	39
3.1	Referenzmodelle	40
3.2	Modellierung der Systeme	45
3.2.1	Modellierung der Verhaltensebene	46
3.2.2	Modellierung der Implementierungsstruktur	51
3.3	Modellierungstechniken	53
3.3.1	Blackbox Spezifikationen	54
3.3.2	Spezifikation mit zu Ausgabekanälen aufgelösten Gleichungen	57

3.3.3	Spezifikation mit Zustandsautomaten	59
3.3.4	Spezifikation mit Betriebsmodi-Automaten	63
3.3.5	Spezifikation der kontinuierlichen Anteile	67
3.4	Abhängigkeiten zwischen Modellen	69
3.4.1	Komposition	69
3.4.2	Verfeinerung	71
3.5	Ansatzpunkte für Fehlerbeschreibungen	76
3.6	Zusammenfassung	78
4	Fehlermodelle, -modellierung und -ermittlung	79
4.1	Fehlermodellierung auf Verhaltensebene	80
4.2	Modellierungstechniken für Fehler	85
4.2.1	Modifikation von Black-Box-Spezifikationen	87
4.2.2	Modifikation von aufgelösten totalen Gleichungen	97
4.2.3	Modifikation von Zustandsautomaten	107
4.2.4	Modifikation von Betriebsmodi-Automaten	110
4.3	Fehler in der Implementierungsstruktur	114
4.4	Fehlerinduktion in Verhaltensmodelle	116
4.5	Spezifische Fehlerbilder aus Fallstudien und Literatur	117
4.5.1	Fehlverhalten an der Nutzungsschnittstelle der Software	117
4.5.2	Fehler in der Implementierungsstruktur	122
4.6	Zusammenfassung	123
5	Zusammenhangsmodelle, -modellierung und -ermittlung	125
5.1	Zusammenhänge auf Verhaltensebene	126
5.1.1	Folgefehler auf Verhaltensebene	127
5.1.2	Fehlerauswirkung auf Verhaltensebene	131
5.2	Spezifische Modelle und Ermittlungstechniken	139
5.2.1	Zusammenhänge bei Black-Box-Spezifikationen	140
5.2.2	Zusammenhänge bei aufgelösten totalen Gleichungen	153
5.2.3	Zusammenhänge bei Zustandsautomaten	158
5.3	Integration der Implementierungsstruktur	163
5.4	Fallstudie	166
5.5	Zusammenfassung	169

6	Werkzeuge und Analysetechniken	171
6.1	Analysetechniken für Verhaltensmodelle	171
6.1.1	Syntaktische Analyse	171
6.1.2	Simulation und Test	172
6.1.3	Boolesche Verifikation modulo Theorien	173
6.1.4	Abstraktionsmechanismen	177
6.2	Spezifische Umsetzungen mit Analysewerkzeugen	182
6.2.1	Systemstrukturbaum, Anforderungs- und Fehlerzuordnung	182
6.2.2	Anforderungsabhängigkeit	183
6.2.3	Fehlerabhängigkeit	184
6.3	Fallstudie	191
6.3.1	Struktur	191
6.3.2	Anforderungsabhängigkeit	193
6.3.3	Fehlerzusammenhänge	194
6.4	Zusammenfassung	196
7	Zusammenfassung und Ausblick	199
7.1	Zusammenfassung	199
7.2	Ausblick	201
A	Generierung der FMEA-Struktur	203
A.1	Systemstrukturbaum	203
A.2	Anforderungszuweisung	205
A.3	Fehlerzuweisung	208
B	Ermittlung der Funktionsabhängigkeiten in Komponenten	215
B.1	Ausgabeabhängigkeiten	215
B.2	Verhaltensbedingungen	218
C	Ermittlung der Fehlerabhängigkeiten	222
C.1	Verhaltensbedingungen	222
C.2	Ausgaben	224