

Inhalt

1	Nutzen der Identifikation sicherheitsbezogener Systeme ...	1
1.1	Eingebettete Systeme	1
1.2	Motivation und Ziel der Arbeit	2
1.3	Prinzipielles Vorgehen und Struktur der Arbeit	5
2	Grundlagen	9
2.1	Stand des Wissens	9
2.2	Sicherheitskritische Systeme	13
2.2.1	Standards	13
2.2.2	Begriffe	14
2.2.3	Systementwicklung nach IEC 61508	21
2.2.4	Systemanforderungen	23
2.2.5	Methoden zur Abschätzung der Sicherheit	26
2.2.6	Modellierungssprachen	30
2.2.7	OPM (Object Process Methodology)	30
2.2.8	AADL (Architecture Analysis & Design Language)	31
2.2.9	UML (Unified Modeling Language)	32
2.2.10	AltaRica / AltaRica DF	33
2.2.11	VHDL (Very High Speed Integrated Circuit Hardware Description Language)	33
2.2.12	BOM (Base Object Model)	34
2.2.13	SysML (Systems Modeling Language)	34
2.2.14	Weitere Modellierungssprachen (Auszug)	40
2.3	Grundlagen Graphentheorie	40
3	Modellbildung	43
3.1	Auswahl Modellierungssprache	44
3.1.1	Anforderungen an Modellierungssprache	44
3.1.2	Anforderungserfüllung durch Modellierungssprachen	46
3.2	Software-Werkzeuge	49
3.3	Anforderungen an das Modell	50
3.4	Erweiterung Modellierungssprache	53
3.4.1	Interne und externe Systemzustände	53
3.4.2	Extended Transition	59
3.5	SysML-Modellierung	61
3.5.1	Modellierung des Anforderungsdiagramms	62
3.5.2	Modellierung des Blockdefinitionsdiagramms	65
3.5.3	Modellierung der internen Blockdiagramme	66

3.5.4	Modellierung von Ereignissen	68
3.5.5	Modellierung der Zustandsdiagramme	69
4	Identifikation sicherheitsbezogener Systeme	73
4.1	Überführung interner Blockdiagramme der SysML in Blockdiagramme der IEC 61508	73
4.1.1	Generisches Sensor-Logik-Aktuator-System	74
4.1.2	Regelbasierte Transformation	78
4.1.3	Identifikation serieller und paralleler Strukturen	85
4.1.4	Abschätzung des Sicherheitsintegritätslevel nach IEC 61508	89
4.1.5	Systemoptimierungsmöglichkeiten, Sensitivitätsanalyse	92
4.2	Identifikation beteiligter Komponenten über Gesamtzustandsraum	93
4.2.1	Produktautomat	95
4.2.2	Zustandsidentifikation	109
4.2.3	Pfadsuche	111
4.2.4	Maße zur Auswahl beteiligter Komponenten	115
5	Bewertung anhand einer Fallstudie	123
5.1	Antriebsstrang eines Hybridfahrzeugs	123
5.2	Sicherheitsfunktionen	125
5.3	Modellbildung (Modell A)	127
5.3.1	Modellierung statischer Aspekte	127
5.3.2	Modellierung dynamischer Aspekte	132
5.3.3	Sicherheitsanforderungen	139
5.4	Evaluation	141
5.4.1	Laufzeitverhalten	142
5.4.2	Maßzahlen	146
5.4.3	Schlussfolgerungen	155
5.4.4	Vergleich der Ergebnisse mit Stand der Technik	160
6	Zusammenfassung und Ausblick	165
7	Literatur	169
8	Abkürzungen	179
9	Anhang	181
9.1	Modell B: generisches Sensor-Logik-Aktuator-System	181
9.1.1	Konfiguration B.1	186
9.1.2	Konfiguration B.2	187

9.2	Modell C: Modell wachende und schlafende Kinder	187
9.2.1	Konfiguration C.1	188
9.2.2	Konfiguration C.2	193