

1	Einleitung	1
1.1	Problematik.....	1
1.2	Zielsetzung	3
1.3	Vorgehensweise	4
2	Problemanalyse	5
2.1	Grundlegende Begriffe	5
2.1.1	Verlässlichkeit als Oberbegriff für Sicherheit und Zuverlässigkeit	7
2.1.2	Beeinträchtigungen der Verlässlichkeit.....	9
2.1.3	Mittel zur Erreichung der Verlässlichkeit.....	14
2.1.4	Grundlegende Begriffe des modellbasierten Systems Engineerings.....	16
2.1.5	Zuverlässigkeit und Sicherheit technischer Systeme.....	18
2.1.5.1	Zuverlässigkeit und Sicherheit – Begriffsklärung	18
2.1.5.2	Zuverlässigkeitskenngrößen.....	19
2.1.5.3	Sicherheitskenngrößen.....	25
2.1.5.4	Ausfallraten im zeitlichen Verlauf.....	28
2.2	Fortschrittliche mechatronische Systeme	29
2.2.1	Mechatronische Systeme	31
2.2.1.1	Klassen mechatronischer Systeme	31
2.2.1.2	Grundsätzlicher Aufbau mechatronischer Systeme... ..	32
2.2.2	Adaptive Systeme.....	35
2.2.3	Selbstoptimierende Systeme	36
2.2.4	Zuverlässigkeit und Sicherheit mechatronischer Systeme	43
2.3	Mögliche Negativfolgen für Unternehmen bei Nichterreichung von Zuverlässigkeit bzw. Sicherheit	44
2.3.1	Wirtschaftliche Folgen	45
2.3.2	Rechtliche Folgen.....	47
2.4	Problemabgrenzung	48

2.5 Anforderungen an die Systematik.....	52
3 Stand der Technik.....	55
3.1 Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme	55
3.1.1 Die Grundsicherheitsnorm IEC 61508 und der zugehörige Sicherheitslebenszyklus	56
3.1.2 Die Sicherheitsnorm ISO 26262 und der zugehörige Sicherheitslebenszyklus	59
3.1.3 Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen	60
3.1.4 Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme des SFB 614	63
3.2 Methoden der Zuverlässigkeits- und Sicherheitsanalyse.....	68
3.2.1 Methoden zur Gefahrenanalyse nach MIL-STD-882	71
3.2.1.1 Vorläufige Gefahrenliste (PHL).....	72
3.2.1.2 Vorläufige Gefahrenanalyse (PHA)	72
3.2.1.3 Gefahrenanalyse auf Subsystemebene (SSHA).....	73
3.2.1.4 Gefahrenanalyse auf Systemebene (SHA).....	75
3.2.1.5 Operating and Support Hazard Analysis (O&SHA)....	76
3.2.1.6 Bewertung	77
3.2.2 Weitere ausgewählte Methoden der Sicherheits- und Zuverlässigkeitstechnik	77
3.2.2.1 Gefahrenanalyse und Risikoeinschätzung nach ISO 26262	78
3.2.2.2 Hazard and Operability Study (HAZOP).....	81
3.2.2.3 Fehlzustandsbaumanalyse (FTA).....	82
3.2.2.4 Dynamische Fehlzustandsbäume (DFT)	84
3.2.2.5 Fehlzustandsart- und -auswirkungsanalyse (FMEA) .	86
3.2.2.6 Ereignisbaumanalyse (ETA).....	88
3.2.2.7 Markoff-Analyse.....	90
3.2.2.8 Bayessche Netze (BN)	91
3.2.2.9 Dynamische Bayessche Netze (DBN)	95
3.2.2.10 Zusammenfassende Bewertung	96
3.3 Hilfsmittel zur Auswahl von Methoden	96
3.3.1 DIN EN 60300-3-1	96
3.3.2 Auswahl von Methoden zur Risikobeurteilung nach IEC 31010	98
3.3.3 IEC 61508.....	102
3.3.4 ISO 26262	102
3.3.5 Methodik zur Auswahl von Methoden des SFB 614	105
3.4 Modellierungssprachen zur Beschreibung des Produktmodells	107

3.4.1	Situationsbasierte Qualitative Modellbildung und Analyse (SQMA).....	107
3.4.2	Systems Modeling Language (SysML).....	110
3.4.3	Spezifikationstechnik CONSENS	114
3.5	Methoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer Beschreibung des Produktmodells	117
3.5.1	Functional Failure Identification and Propagation (FFIP).....	117
3.5.2	Ein UML-Profil zur FTA-basierten Absicherung der Sicherheit eines technischen Systems nach DOUGLASS	121
3.5.3	Analysen auf Basis einer mit der Spezifikationstechnik CONSENS beschriebenen Produktkonzeption.....	122
3.5.4	FMEA auf Basis eines SysML-Modells nach ALT	124
3.5.5	MeDISIS (Integration Method of Reliability Analysis in the System Engineering Process)	124
3.6	Software-Unterstützung.....	126
3.6.1	Etablierte Software-Pakete zur Absicherung der Zuverlässigkeit und Sicherheit.....	127
3.6.2	medini analyze – ein Software-Werkzeug zur Absicherung der funktionalen Sicherheit	128
3.6.3	Mechatronic Modeller	129
3.7	Bewertung des Stands der Technik und Handlungsbedarf.....	130
4	Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit	135
4.1	Die Systematik im Überblick	135
4.2	Vorgehensmodell.....	137
4.2.1	Aufbau des Vorgehensmodells.....	137
4.2.1.1	Phase 1 – Analyse der Entwicklungsaufgabe.....	139
4.2.1.2	Phase 2 – Auswahl und Planung von Methoden	140
4.2.1.3	Phase 3 – Erweiterung/Anpassung der Modellierungssprache	141
4.2.1.4	Phase 4 – Absicherung (Spezifikation, Analyse, Verbesserung).....	142
4.2.2	Einbettung in den Referenzprozess für die Konzipierung.....	143
4.3	Rechnerunterstützte Auswahl und Planung von Methoden der Zuverlässigkeit und Sicherheit in der Konzipierung.....	144
4.3.1	Charakterisierung der Entwicklungsaufgabe	144
4.3.2	Klassifizierungsschema für Methoden und Methoden-Steckbriefe.....	146

4.3.3	Methodik zur Auswahl und Planung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in der Konzipierung.....	151
4.4	Spezifikation des Produkts unter Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen.....	153
4.4.1	Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS ausgehend von den ausgewählten Methoden	154
4.4.2	Leitlinie zur Erweiterung der Spezifikationstechnik CONSENS	156
4.4.3	Erweiterung der Spezifikationstechnik CONSENS am Beispiel der Integration der Methoden FTA und FMEA.....	158
4.5	Angepasste Methoden zur Analyse und Verbesserung.....	162
4.5.1	Spezifikation der Ausfallfortpflanzung innerhalb der Produktkonzeption.....	163
4.5.2	Automatisierte Erzeugung eines Fehlzustandsbaums.....	163
4.5.3	Automatisierte Erzeugung einer FMEA-Tabelle.....	164
4.5.4	Durchführung BN-orientierter Analysen	164
4.6	Werkzeugunterstützung für Modellierung und Analyse	167
5	Validierung der Systematik	169
5.1	Überblick über die X-by-Wire-Technologie	169
5.1.1	Herausforderung: Verzicht auf die mechanische Rückfallebene.....	170
5.1.2	Absicherung der Sicherheit von X-by-Wire-Systemen.....	171
5.2	Anwendungsbeispiel: X-by-Wire-Versuchsfahrzeug Chamäleon.....	172
5.3	Phase 1 – Analyse der Entwicklungsaufgabe.....	173
5.4	Phase 2 – Auswahl und Planung von Methoden	174
5.5	Phase 3 – Erweiterung/Anpassung der Modellierungssprache	176
5.6	Phase 4 – Absicherung (Spezifikation, Analyse, Verbesserung).....	178
5.6.1	Sicherheitsziele und sicherer Zustand.....	184
5.6.2	Funktionales Sicherheitskonzept.....	186
5.6.3	Informationsverarbeitung des Chamäleons	190
5.6.4	Auf dem Weg zum technischen Sicherheitskonzept.....	194
5.6.4.1	Absicherung der Energieversorgung	195
5.6.4.2	Überwachung externer Signale und der Sensorik ...	195
5.6.4.3	Überwachungskonzept für die Informationsverarbeitung 197	
5.6.4.4	Überwachung Aktorik	201
5.6.4.5	Absicherung Grundsystem	201
5.7	Bewertung der Systematik hinsichtlich der Erfüllung der Anforderungen.....	202

6 Zusammenfassung und Ausblick 205