

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Umfeld	1
1.1.1	Komplexitätszuwachs	2
1.1.2	Qualität	3
1.1.3	Unfallstatistik und Vertrauen in E/E-basierte Systeme	4
1.1.4	Juristische Konsequenzen	5
1.1.5	Sicherheit und komplexe Fahrassistenzfunktionen	6
1.1.6	Vergleich mit Flugzeugen und Schienenfahrzeugen	7
1.1.7	Sicherheit als Entwicklungsziel	8
1.1.8	Funktionale Sicherheit	9
1.1.9	Zur Gefährdungsreduzierung reichen herkömmliche Prozesse nicht mehr aus	10
1.1.10	Systemauslegung und Entwicklung	11
1.2	Motivation	12
1.3	Ziele und eigener Beitrag	14
1.3.1	Entwicklung gemeinsames Verständnis	14
1.3.2	EEA Optimierung bezüglich funktionaler Sicherheit	15
1.3.3	Hilfestellung bei Durchführung gemäß V-Modell	15
1.3.4	Fragestellungen gegenüber EEA Modellen	15
1.4	Gliederung der Arbeit	16
<b>2</b>	<b>Grundlagen</b>	<b>19</b>
2.1	Mengenlehre	19
2.1.1	Mengen	19
2.1.2	Relation	20
2.2	Graphentheorie	21
2.3	Logik	24
2.3.1	Aussagenlogik	25
2.3.2	BOOLEsche Algebra und Schaltalgebra	27
2.3.3	Prädikatenlogik	28
2.3.4	Kategorien und Konzepte	30
2.3.5	Beschreibungslogik	33
2.4	Vorgehensmodelle	34
2.4.1	Wasserfallmodell	36
2.4.2	V-Modell	38
2.4.3	V-Modell XT	41

2.5	Sicherheit . . . . .	42
2.5.1	Risiko . . . . .	43
2.5.2	Grenzrisiko . . . . .	43
2.5.3	Gefahr . . . . .	43
2.5.4	Gefährdung . . . . .	44
2.5.5	Sicherheitsrelevanz . . . . .	44
2.6	Zuverlässigkeit und Verfügbarkeit . . . . .	44
2.6.1	Statistische Grundlagen . . . . .	45
2.6.2	Statistische Beschreibung von Zuverlässigkeit . . . . .	46
2.6.3	Fehler . . . . .	48
2.6.4	Fehlerursachen . . . . .	48
2.7	Methoden zur Kategorisierung von Gefährdungen sowie Sicherheits- assessments . . . . .	49
2.7.1	Bestimmung von Sicherheitsanforderungen . . . . .	50
2.7.2	Sicherheitsassessments . . . . .	52
2.7.2.1	Fehler-Möglichkeiten- und Einfluss-Analyse FMEA . . . . .	54
2.7.2.2	Fehlerbaumanalyse FTA . . . . .	59
2.7.2.3	Markov-Ketten . . . . .	61
2.8	Redundanz . . . . .	61
2.9	Modellierung . . . . .	63
2.9.1	Modell . . . . .	63
2.9.2	Ausprägungen von Modellen . . . . .	66
2.9.3	Standards im Umfeld des Model Driven Engineering . . . . .	69
2.9.3.1	Extensible Markup Language XML . . . . .	69
2.9.3.2	XML Schema . . . . .	71
2.9.3.3	XSL Translation (XSLT) . . . . .	72
2.9.3.4	Grundlagen der Objekt Orientierung (OO) . . . . .	72
2.9.3.5	Unified Modeling Language (UML) . . . . .	74
	Organisation des UML Metamodells . . . . .	74
	UML Superstructure . . . . .	75
2.9.3.6	Meta Object Facility . . . . .	77
2.9.3.7	XML Metadata Interchange (XMI) . . . . .	78
2.9.3.8	ECORE . . . . .	81
2.9.3.9	Modeling Spaces . . . . .	84
2.10	Modellierung von Elektrik/Elektronik Architekturen in der Automo- bilentwicklung . . . . .	86
2.10.1	PREEvision . . . . .	86
2.10.1.1	Abstraktionsebenen . . . . .	86
2.10.1.2	Modellabfragen . . . . .	89
2.10.1.3	Metrikdiagramm . . . . .	90

<b>3</b>	<b>ISO 26262 Functional Safety for Road Vehicles - Stand von Forschung und Technik</b>	<b>91</b>
3.1	Erklärung der ISO 26262 . . . . .	92
3.1.1	ISO 26262 Teil 3: Konzeptphase . . . . .	92
3.1.1.1	Gefährdungs- und Risikoanalyse . . . . .	94
3.1.1.2	Das funktionale Sicherheitskonzept . . . . .	96
3.1.2	ISO 26262 Teil 4: Produktentwicklung auf Systemebene . . . . .	97
3.1.3	ISO 26262 Teil 5: Produktentwicklung Hardwareebene . . . . .	99
3.1.4	ISO 26262 Part 6: Produktentwicklung Softwareebene . . . . .	100
3.2	Herausforderungen bei der Umsetzung der Norm . . . . .	101
3.3	Stand der Wissenschaft und Technik . . . . .	102
3.3.1	ATESST Projekt und Architekturbeschreibungssprache EAST-ADL . . . . .	102
3.3.1.1	Beschreibung . . . . .	102
3.3.1.2	Abgrenzung . . . . .	107
3.3.2	E/E-Architekturen zur Ableitung von Sicherheitszielen . . . . .	108
3.3.2.1	Beschreibung . . . . .	108
3.3.2.2	Abgrenzung . . . . .	109
3.3.3	Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil . . . . .	111
3.3.3.1	Beschreibung . . . . .	111
3.3.3.2	Abgrenzung . . . . .	112
3.3.4	AUTOSAR . . . . .	113
3.3.4.1	Beschreibung . . . . .	113
3.3.4.2	Abgrenzung . . . . .	119
3.3.5	HiP-HOPS . . . . .	120
3.3.5.1	Beschreibung . . . . .	120
	Functional Failure Analysis (FFA) . . . . .	121
	Interface Focused FMEA . . . . .	121
	Unterstützung von EAST-ADL . . . . .	122
3.3.5.2	Abgrenzung . . . . .	123
<b>4</b>	<b>Anforderungen an den Umgang mit Sicherheitsanforderungen in der Konzeptphase</b>	<b>125</b>
4.1	Diskussion der Herausforderungen . . . . .	125
4.2	Anforderungen an die Darstellung von Sicherheitsanforderungen . . . . .	128
4.3	Anforderungen an die Rückverfolgbarkeit von Sicherheitsbeziehungen . . . . .	129
4.4	Anforderungen an die Überarbeitung und Bewertung von E/E Architekturen . . . . .	130
4.5	Vergleich mit dem Stand der Technik . . . . .	130
4.6	Systematische Zusammenfassung der Anforderungen . . . . .	133
4.7	Sprache- und Werkzeugauswahl . . . . .	134
4.8	Vorgehensweise . . . . .	134

<b>5</b>	<b>Darstellung von Sicherheitsanforderungen</b>	<b>137</b>
5.1	Konzeptphase und E/E-Architektur im Lebenszyklus der Automobilentwicklung . . . . .	137
5.2	Relevante Konzepte der ISO 26262 für die Darstellung von Sicherheitsanforderungen . . . . .	140
5.3	Interpretation des Item in der E/E-Architektur . . . . .	140
5.3.1	Beispiel Automatischer Heckspoiler . . . . .	141
5.3.2	Zuordnung von Einheiten der EEA zu Items . . . . .	143
5.4	Formalisierte Darstellung von Sicherheitsanforderungen . . . . .	143
5.5	Bibliothek mit technischen Sicherheitsanforderungen . . . . .	147
5.6	Zusammenfassung der Darstellung von Sicherheitsanforderungen . .	149
<b>6</b>	<b>Zuteilung und Rückverfolgung von Sicherheitsanforderungen</b>	<b>151</b>
6.1	Unterscheidung zwischen Top-Down und Bottom-Up Zuteilung . . . .	151
6.2	Top-Down Zuteilung . . . . .	153
6.2.1	Zuteilung von Gefährdungen und Sicherheitszielen . . . . .	153
6.2.1.1	Initiierung der Sicherheitsmodellierung . . . . .	155
6.2.1.2	Auswirkungen auf weitere Modellierungsebenen . . .	156
6.2.2	Sicherheitsannotationen . . . . .	156
6.2.2.1	Annotationen von Kommunikationsnetzen . . . . .	158
6.2.2.2	Annotationen von Leistungsversorgungsnetzen . . . .	159
6.2.3	Darstellung von Sicherheitsannotationen . . . . .	160
6.2.4	Zuteilung von funktionalen und technischen Sicherheitsanforderungen . . . . .	164
6.2.5	Übersicht der Aktivitäten . . . . .	166
6.3	Bottom-Up Zuteilung . . . . .	167
6.3.1	Propagation von Annotationen im Funktionsnetzwerk . . . . .	169
6.3.2	Propagation von Annotationen im Komponentennetzwerk . . .	171
6.3.3	Propagation von Annotationen auf Netze der Kommunikation und Leistungsversorgung . . . . .	171
6.3.4	Realisierung . . . . .	172
<b>7</b>	<b>Optimierung von E/E-Architekturen unter Berücksichtigung funktionaler Sicherheit</b>	<b>175</b>
7.1	ASIL Dekomposition nach ISO 26262 . . . . .	175
7.2	Diskussion der ASIL Dekomposition . . . . .	177
7.2.1	Dekompositionsbeispiel . . . . .	177
7.2.2	Bezug zwischen Dekomposition und Architekturänderungen .	179
7.2.3	Betrachtung im Zuverlässigkeits-Block-Diagramm . . . . .	180
7.2.4	Vorgehen bei der Dekomposition . . . . .	181
7.2.4.1	Nachschlagewerk . . . . .	182
7.2.4.2	Methodisches Vorgehen . . . . .	184
7.3	Redundanzmittel und Dekomposition in E/E-Architektur Modellierung	189
7.4	Methode zur Bewertung von Überarbeitungen . . . . .	193
7.4.1	Anforderungen an eine Methode zur qualitativen Bewertung .	193

7.4.2	Überblick über die Methode . . . . .	193
7.4.3	Methode im Detail . . . . .	194
7.4.3.1	Durchführung in Bezug auf jeweils eine systembezo- gene Fehlerart . . . . .	194
7.4.3.2	Vergleich zwischen Ergebnissen vor und nach einer Überarbeitung sowie in Bezug auf verschiedene, sys- tembezogene Fehlerarten . . . . .	197
7.4.4	Beispielhafte Anwendung der Methode . . . . .	198
7.4.4.1	Durchführung auf ursprünglichem System . . . . .	199
7.4.4.2	Durchführung auf überarbeitetem System . . . . .	201
7.4.4.3	Bestimmung der qualitativen Vergleichswerte . . . . .	201
7.4.4.4	Diskussion der Ergebnisse . . . . .	203
7.4.5	Fazit . . . . .	203
<b>8</b>	<b>Hilfestellung zur Durchführung anhand der Beispiele FMEA und HiL-Test</b>	<b>205</b>
8.1	Akkumulation kontextspezifischer Daten . . . . .	206
8.2	Freischneiden für Sicherheitsanalysen . . . . .	207
8.2.1	Durchführung am Beispiel der FMEA . . . . .	208
8.2.2	FMEA auf Basis von E/E-Architektur Modellen . . . . .	209
8.2.2.1	Strukturanalyse der FMEA . . . . .	209
8.2.2.2	Funktionsanalyse der FMEA . . . . .	211
8.2.2.3	Fehleranalyse, Analyse von Aktivitäten sowie Opti- mierung und Dokumentation der FMEA . . . . .	211
8.2.3	Akkumulation von Daten für die FMEA . . . . .	212
8.2.4	Durchführung der FMEA im EEA Modellierungswerkzeug PRE- vision . . . . .	215
8.2.4.1	Generierung von Anforderungstabellen . . . . .	215
8.2.4.2	Durchführung der FMEA . . . . .	216
8.2.4.3	Generierung von Reports . . . . .	217
8.2.5	Ergebnisse . . . . .	217
8.3	Einsatz Freischneiden für Verifikation und Test . . . . .	218
8.3.1	Grundlagen zu HiL-Testsystemen . . . . .	219
8.3.2	Aktuelle Durchführung der Spezifikation von HiL-Testsystemen	220
8.3.3	Rahmenbedingungen - Freischneiden zur Spezifikation von HiL- Testsystemen . . . . .	221
8.3.4	Akkumulation von Daten . . . . .	221
8.3.4.1	Verwendungsaktivitätsspezifisches Übergabeformat . .	223
8.3.4.2	Realisierung . . . . .	225
8.3.4.3	Test . . . . .	227
8.3.5	Diskussion der Ergebnisse . . . . .	228
8.4	Zusammenfassende Diskussion des Freischneidens . . . . .	229

<b>9 Fragestellungsgraphen</b>	<b>231</b>
9.1 Stand der Wissenschaft und Technik	232
9.1.1 Mustersuche der Modell-zu-Model-Transformation	232
9.1.1.1 Beschreibung	232
9.1.1.2 Abgrenzung / Erweiterung	233
9.1.2 Modellabfrageregelwerk im E/E-Architektur Modellierungswerkzeug PREEvision	233
9.1.2.1 Beschreibung	233
9.1.2.2 Abgrenzung / Erweiterung	235
9.1.3 Abstraktionsebenenübergreifende Darstellung von E/E Architekturen in Kraftfahrzeugen	235
9.1.3.1 Beschreibung	235
9.1.3.2 Abgrenzung / Erweiterung	236
9.2 Anforderungen	237
9.2.1 Anforderungen an die Akkumulation von Daten aus E/E-Architektur Modellen	237
9.2.2 Vergleich mit dem Stand der Technik	238
9.2.3 Systematische Ableitung von Anforderungen	239
9.3 Detaillierte Betrachtung der E/E-Architektur Modellierung in Bezug auf Fragestellungen	239
9.3.1 M-Graphen und MM-Graph	239
9.3.1.1 M-Graph	240
9.3.1.2 MM-Graph	240
9.3.1.3 Teilfragestellungsgraph (TFS-Graph)	241
9.3.2 Graphenbasierte Darstellung von Fragestellungen	242
9.3.3 Graphenbasierte Darstellung einer Abfrage	244
9.4 Bedeutung von Artefaktkombinationen	245
9.5 Strukturierung graphenbasierter Darstellungen	249
9.5.1 Abfrageelement	249
9.5.2 Abfragegruppe	251
9.5.3 Abfragegraph	252
9.5.4 Fragestellungsgraph	252
9.6 Datenformat für Fragestellungsgraphen	253
9.7 Ergebnistabellen	257
9.8 Logische Relationen	262
9.8.1 Logische Relationen auf Ebene von Fragestellungsgraphen	262
9.8.1.1 Bedingte Logische Relation IF	264
9.8.2 Logische Relationen auf Ebene von Abfragegraphen	265
9.8.2.1 Logische Relation NOT	269
9.8.2.2 Logische Relation VERALLGNOT	270
9.9 Zerlegung von Fragestellungen	272
9.9.1 Übersicht über das Vorgehen	272
9.9.2 Aufteilung von Fragestellungsgraphen	274
9.9.3 Aufteilung von Abfragegraphen	276
9.9.3.1 Aufteilung in Regelabfragegraphen	277

9.9.3.2	Aufteilung in Konjunktionsgraphen . . . . .	279
9.9.3.3	Transformation in Konjunktionsketten . . . . .	281
9.9.3.4	Übersicht der Aufteilungsresultate . . . . .	282
9.9.4	Ermittlung von Ergebnissen . . . . .	283
9.10	Realisierung . . . . .	284
9.10.1	Aktivitäten der Ergebnisermittlung . . . . .	284
9.10.2	Anforderungen durch Verwendung bestehender Realisierung . . . . .	286
9.10.3	Aktivitäten der Realisierung . . . . .	287
9.10.4	Datenformat für Regelzusammenhang . . . . .	289
9.10.5	Struktur der Realisierung . . . . .	291
9.10.6	Realisierung im E/E-Architektur Werkzeug PREEvision . . . . .	292
9.11	Beispiel . . . . .	296
9.12	Zusammenfassende Diskussion von Fragestellungsgraphen . . . . .	304
9.12.1	Diskussion . . . . .	304
9.12.2	Ausblick . . . . .	306
<b>10</b>	<b>E/E-Architekturen als Ontologien</b>	<b>309</b>
10.1	Möglichkeiten zum Fassen und Ableiten von Wissen in der Entwick- lung von EEAs . . . . .	310
10.1.1	Annotationen . . . . .	310
10.1.2	Modellabfragen . . . . .	313
10.1.3	Bewertung . . . . .	314
10.2	Ansätze zur Wissensmodellierung . . . . .	315
10.3	Grundlagen zur Wissensmodellierung mit Ontologien . . . . .	316
10.3.1	Logischer Hintergrund . . . . .	317
10.3.2	Darstellung und Methodik von Ontologien . . . . .	318
10.3.2.1	Resource Description Framework . . . . .	318
10.3.2.2	RDF Schema . . . . .	319
10.3.2.3	Web Ontology Language . . . . .	319
10.3.2.4	F-Logic . . . . .	321
10.3.2.5	Schlussfolgerungen . . . . .	321
10.3.2.6	Abfragen . . . . .	322
10.3.2.7	Graphische Darstellung . . . . .	323
10.4	Motivation für den Einsatz von Ontologien . . . . .	324
10.4.1	Anforderungen an die Transformation und die Nutzung der ontologiebasierten Darstellung . . . . .	324
10.5	Stand der Forschung und Technik . . . . .	325
10.5.1	Ontologie-basierte Ansätze zur Auswertung von Hardware-in- the-Loop Testergebnissen . . . . .	325
10.5.2	Design Process Model for Automotive Systems (DeSCAS) . . . . .	325
10.5.3	ModelCVS . . . . .	327
10.6	Anforderungen an die ontologische Betrachtung von E/E-Architekturen	328
10.6.1	Anforderungen an die Übersetzung . . . . .	328

10.6.2	Anforderungen an die Nutzung der ontologiebasierten Betrachtung . . . . .	329
10.6.3	Vergleich mit dem Stand der Technik . . . . .	329
10.6.4	Systematische Zusammenfassung der Anforderungen . . . . .	330
10.6.5	Vorgehensweise . . . . .	330
10.7	Transformation . . . . .	331
10.7.1	Einführung des Beispielsmodells . . . . .	331
10.7.2	Konzeption der Transformation . . . . .	332
10.7.3	Transformation des E/E-Architektur Metamodells . . . . .	334
10.7.4	Transformation des E/E-Architektur Modells . . . . .	340
10.7.5	Durchführung der Transformation und Diskussion der Ergebnisse . . . . .	341
10.8	Bearbeitung der ontologiebasierten Darstellung von E/E-Architekturen	344
10.8.1	Aufbereitung der Transformationsergebnisse . . . . .	345
10.8.2	Anreicherung mit Domänenwissen . . . . .	346
10.9	Verwendung der ontologiebasierten Darstellung von E/E-Architekturen	349
10.9.1	Schlussfolgerung impliziten Wissens . . . . .	349
10.9.2	Regelabfragen . . . . .	350
10.9.3	Diskussion der Ergebnisse . . . . .	352
10.10	Einordnung in den Entwicklungsprozess . . . . .	353
10.11	Zusammenfassung und Ausblick . . . . .	356
<b>11</b>	<b>Zusammenfassung und Ausblick</b>	<b>357</b>
11.1	Zusammenfassung . . . . .	357
11.1.1	ISO 26262 in der Entwicklungsphase der Modellierung von Elektrik/Elektronik Architekturen . . . . .	358
11.1.2	Fragestellungsgraphen zur domänenspezifischen Anwendung auf Elektrik/Elektronik Architekturen . . . . .	359
11.1.3	Elektrik/Elektronik Architekturen als Ontologien . . . . .	360
11.2	Ausblick . . . . .	361
<b>Verzeichnisse</b>		<b>363</b>
	Abbildungsverzeichnis . . . . .	363
	Tabellenverzeichnis . . . . .	369
	Abkürzungsverzeichnis . . . . .	371
<b>Literatur- und Quellennachweise</b>		<b>377</b>
<b>Betreute studentische Arbeiten</b>		<b>393</b>
<b>Eigene Veröffentlichungen</b>		<b>397</b>