

Contents

Preface	V
Figures	IX
Tables	XIII
Abbreviations	XV
Abstract	XVII
Kurzfassung	XIX
1 Introduction	1
1.1 Motivation and Objectives	1
1.2 Thesis Outline	4
2 State of the Art	7
2.1 Functional Safety	7
2.2 ISO 26262 - Road Vehicles - Functional Safety	8
2.2.1 Safety Lifecycle	10
2.2.2 ASIL Decomposition	14
2.2.3 Analysis of Dependent Failures (DFA)	15
2.2.4 Freedom From Interference (FFI)	17
2.3 ISO/PAS 21448 – Safety of the Intended Functionality	18
2.4 SAE J3016 - Automated Driving Levels	20
2.5 Multicore Processors / Domain ECUs	21
2.6 Architecture Description Language / EAST-ADL	23
2.6.1 System Model of EAST-ADL	24
2.6.2 Dependability Model and Requirements Model of EAST-ADL	29
3 Fail-operational Safety Architecture for ADAS/AD Systems	31
3.1 Introduction	32
3.2 Safety Architecture Mechanisms	34
3.2.1 Fail-safe Safety Architecture	34
3.2.2 Fail-operational Safety Architecture	34

3.3	Fail-operational Safety Architecture for Conventional Systems ...	38
3.4	Fail-Operational Safety Architectures for ADAS/AD Systems	40
3.4.1	Fail-operational Safety Approach for ADAS/AD Systems.....	42
3.4.2	ASIL Decomposition for ADAS/AD Systems	56
3.4.3	Dependent Failure Analysis for ADAS/AD Systems.....	64
3.5	Use Cases.....	66
3.5.1	Fail-operational Safety Architecture for Powertrain Domain	66
3.5.2	ASIL Decomposition in General	67
3.5.3	ASIL Decomposition for AD Systems.....	69
3.6	Conclusion	74
4	Model-driven Approaches for ISO 26262 Work Products and DFA	77
4.1	Development of Safety Functions Using Modified EAST-ADL ...	77
4.1.1	Introduction	77
4.1.2	Description of the Approach	79
4.1.3	Extensions of EAST-ADL	82
4.1.4	Use Case	89
4.1.5	Conclusion.....	96
4.2	A Model-driven Approach for DFA Using Modified EAST-ADL	98
4.2.1	Introduction	99
4.2.2	DFA According to ISO 26262	100
4.2.3	Necessary Developments of EAST-ADL for the DFA	104
4.2.4	Description of Developed Model-based Approach for DFA and Safety Analysis	110
4.2.5	Scripts and Reports	118
4.2.6	Use case	121
4.2.7	Conclusion.....	137
5	Conclusion and Outlook.....	139
	Bibliography	143