

contents

Introduction

xi

FUNCTIONAL SAFETY PAPERS

CHAPTER 1

The Development of Safety Cases for an Autonomous Vehicle: A Comparative Study on Different Methods 1

Introduction 2

Vehicle Layout and ISO26262 4

Vehicle Control System and Propulsion System 4

ISO26262 Road Vehicle Functional Safety Standard 5

Failure Model and Effects Analysis Method 6

Goal Structuring Notation Method 6

Safety Case Development 7

Case Study 8

Conclusions 10

Contact Information 11

Acknowledgments 11

Definitions/Abbreviations 11

References 12

CHAPTER 2

A Means of Assessing the Entire Functional Safety Hazard Space 15

Introduction 16

Background 17

Related Work 19

Overview of Hazard Space Analysis (HSA) 20

HSA Notation Format 20

Generation of Hazard Space 22

Partitioning of a Single-Caused Hazard Space 24

Safety Rules from Hazard Scenarios 25

Aviation Safety Example	27
Managing a Large Hazard Space	27
Risk Assessment	29
Safety Requirements	31
Discussion and Limitations	31
Conclusion	32
Contact Information	33
References	33

CHAPTER 3

A Model-Driven Approach for Dependent Failure Analysis in Consideration of Multicore Processors Using Modified EAST-ADL **35**

Introduction	36
Description of the Approach	37
Approach of System and Safety Modeling	37
Approach of DFA-Analysis	39
A. Necessary Developments of EAST-ADL for the DFA Analysis	40
B. Description of DFA-Analysis and Safety Analysis	42
C. Use-Case and Reports	44
Conclusions	45
Contact Information	45
Acknowledgments	45
References	46

CHAPTER 4

An Analysis of ISO 26262: Machine Learning and Safety in Automotive Software **47**

Introduction	47
Background	48
ISO 26262	48
Machine Learning	49
Non-Transparency	50
Error Rate	50
Training-Based	50
Instability	50

Analysis of ISO 26262	50
Identifying Hazards	51
Recommendations for ISO 26262	51
Faults and Failure Modes	51
Recommendations for ISO 26262	52
Specification and Verification	52
Recommendations for ISO 26262	53
Level of ML Usage	53
Recommendations for ISO 26262	54
Required Software Techniques	54
Recommendations for ISO 26262	55
Summary and Conclusion	56
Identifying Hazards	56
Fault and Failure Modes	56
Specification and Verification	56
The Level of ML Usage	56
Required Software Techniques	57
Acknowledgment	57
References	57

SOTIF PAPERS

CHAPTER 5

Hazard Analysis and Risk Assessment beyond ISO 26262: Management of Complexity via Restructuring of Risk-Generating Process	61
Introduction	62
SOTIF HARA and State Space Explosion	63
HARA Composition	63
Hazards	63
Use Cases	63
HARA and the Hidden Semi-Markov Chain	64
Restructuring of Risk-Generating Process	65
Automatic Emergency Braking (AEB) Example	66
Markov Chain Solution	66
Regions of the Transition Matrix	67
Is There Another Way to Do It?	68
Summary	69
Outlook	69

Contact Information	69
Definitions/Abbreviations	69
References	70

CHAPTER 6

The Science of Testing: An Automotive Perspective 71

Introduction	72
Understanding Scenarios	73
Types of Testing	74
Methodology	75
Participants	75
Interview Questions Design	76
Data Analysis	76
First Cycle Coding	77
Second Cycle Coding and Category Identification	77
Results	78
Discussion	79
Conclusion	80
Contact Information	81
Acknowledgments	81
References	81

MULTI-AGENT SAFETY PAPERS

CHAPTER 7

Theory of Collision Avoidance Capability in Automated Driving Technologies 85

Introduction	86
Definition of Normal Driving	88
Requisite Sensing Range	88
Operational Design Domain	89
Formulation of Collision Avoidance in the Semantic Level	90
Candidate Path Matrix	90
Collision Avoidance by Lane Selection	91
Timing Tensor	91

Collision Avoidance Equation	92
Collision Avoidance in Normal Driving	92
Collision Avoidance in Normal Driving	93
Preparation and Response to Hazard	93
Preparation and Response to Cognitive Hazard	93
Preparation and Response to Behavioral Hazard	94
Behavior Analysis in Extreme Traffic Situations/Hazards	97
Stability of Extreme Condition	98
Trace-Back of Traffic Environment and Stability	98
Summary of Forward and Backward Analysis	100
Discussion	100
Summary/Conclusion	101
Contact Information	102
Acknowledgments	102
References	102

CHAPTER 8

A Lane-Changing Decision-Making Method for Intelligent Vehicle Based on Acceleration Field 105

Introduction	106
Acceleration Field	107
Braking Safety Distance Model	107
Acceleration Field for Intention Generating	110
Acceleration Field for Feasibility Judgement	111
Complete Acceleration Field	111
Basic Lane-Changing Decision-Making Method	112
Braking Decision-Making Method	113
Basic Lane-Changing Decision-Making Method	114
Lane-Changing Assumptions and Simplifications	114
Analysis of Lane-Changing Process	114
Decision-Making Method	116
Extended Lane-Changing Decision-Making Method	117
Inspection on Rear Side Traffic Vehicle	117
Extended Method with Velocity Regulation	117
Simulation with Polynomial Trajectory Planning	119
Summary	122
Contact Information	122
Acknowledgments	123
References	123

CHAPTER 9**Entropy in Reaction Space - Upgrade
of Time-to-Collision Quantity 125**

Introduction	126
Definition of Reaction Space	127
Interactions and Entropy	130
Application Examples	133
Conclusion	134
Contact Information	135
References	135

CHAPTER 10**A Maneuver-Based Threat Assessment
Strategy for Collision Avoidance 137**

Introduction	138
Strategy Structure	139
Maneuver-Based Trajectory Prediction Model	140
Maneuver Recognition with GMHMM	140
Trajectory Prediction	144
Collision Prediction Model	146
Threat Quantifying	148
Simulation Results	149
Summary	153
Contact Information	153
Acknowledgments	154
References	154

Epilogue	157
----------	-----