

Table of Contents

Acronyms xiii

1 Introduction 1

1.1 Research Question 1

1.2 Motivation for Self-Driving Vehicles 2

1.3 Terminology..... 3

1.4 From Driver Assistance to Self-Driving Vehicles 5

1.5 Residual Risk for Autonomous Systems 9

1.6 Management of Residual Risk..... 10

1.7 Dynamic Behavior Risk Assessment Overview 12

1.8 Thesis Contribution and Structure 13

2 Related Work..... 17

2.1 Conceptual Frameworks for Runtime Risk Reduction 17

2.1.1 Safety Bag 17

2.1.2 SIMPLEX 18

2.2 Classification of Safety Bag Approaches..... 19

2.3 Assessment of Related Work 21

2.3.1 Presentation of Selected Approaches 23

2.4 Summary of Related Work on Runtime Safety Monitoring 29

3 Dynamic Behavior Risk Assessment 35

3.1 A General Notion of Risk..... 35

3.1.1 Risk in the Automotive Domain 36

3.1.2 Acceptable Risk 38

3.2 The Safety Supervisor Method for Dynamic Behavior Risk Assessment 38

3.3 From Collision Avoidance Metrics to Risk Metrics 41

3.3.1 Situation Evaluation Metric Taxonomy 41

3.3.2 Analysis of Collision Avoidance Metrics 44

3.3.3 Instantiation of the Safety Supervisor Method..... 49

3.4 Dynamic Safety Engineering Approaches 51

3.4.1 Dynamic Safety Management 52

- 3.4.2 Hazard and Risk Analysis @ Runtime 54
- 4 Method for Risk Metric Calculation 59**
 - 4.1 Risk Metric Calculation Method Overview 59
 - 4.2 Offline Data Generation..... 61
 - 4.3 Online Data Generation 62
 - 4.4 Grid Map Generation 64
 - 4.5 Risk Metric Calculation 65
 - 4.6 Grid Map Visualization 65
 - 4.7 ConSerts Runtime Environment 66
- 5 Risk Metric Calculation via Deep Learning 67**
 - 5.1 Artificial Neural Network..... 67
 - 5.2 Training Data Generation 68
 - 5.3 Creating Stereo Images and Disparity 69
 - 5.4 Labeling Data with Risk Information 70
 - 5.5 Neural Network Training 72
 - 5.6 Performance of Risk Metric Calculation via Deep Learning 72
 - 5.7 Limitations of Risk Metric Calculation via Deep Learning..... 75
- 6 Risk Metric Calculation at the System Level..... 77**
 - 6.1 System-Level Safety Supervisor Method 77
 - 6.2 Prototypical Implementation of the System-Level Safety Supervisor..... 82
 - 6.3 Benefits and Limitations of the Confidence Disclosure Concept..... 86
- 7 Risk Metric Calculation at the Mission Level 91**
 - 7.1 Mission-Level Risk Metric 91
 - 7.2 Conditional Safety Certificates for Mission-Level Risk Metric Calculation..... 92
 - 7.3 Prototypical Implementation of the Mission-Level Safety Supervisor..... 96
- 8 Evaluation 103**
 - 8.1 Intelligent Automated Parking 103
 - 8.2 Static Supervision for IAP 104
 - 8.2.1 Conditional Safety Certificates for the Static Supervision of IAP 107

8.3 Dynamic Supervision for IAP 108

8.3.1 Conditional Safety Certificates for the Dynamic Supervision of IAP 114

9 Conclusion and Future Work 117

9.1 Conclusion 117

9.2 Future Work 119

References 121

A Method for Risk Metric Calculation Source Code 131

A.1 Trajectory Prediction Source Code 131

A.2 Grid Map Generation Source Code 134

A.3 Predicted Cells Calculation Source Code 135

A.4 Risk Metric Calculation Source Code 137

A.5 Grid Map Visualization Source Code 138

A.6 ConSert Tree Visualization Source Code 139