# Contents

## Introduction

### Chapter 1: Fault-Tolerant Ability Testing for Automotive Ethernet

- **Introduction**
- **Physical Layer Analysis**
- **Fault Tolerance Testing**
  - Wire Short or Open Testing
  - Resistance Testing
  - Capacitance Testing
  - Ground Shift Testing
- **Result Analysis**
- **Summary/Conclusions**
- **Contact Information**
- **Acknowledgments**
- **Definitions/Abbreviations**
- **References**

### Chapter 2: An Analysis of ISO 26262: Machine Learning and Safety in Automotive Software

- **Introduction**
- **Background**
  - ISO 26262
  - Machine Learning
- **Analysis of ISO 26262**
  - Identifying Hazards
  - Faults and Failure Modes
CHAPTER 3
The Development of Safety Cases for an Autonomous Vehicle: A Comparative Study on Different Methods

Introduction
Vehicle Layout and ISO26262
Vehicle Control System and Propulsion System
ISO26262 Road Vehicle Functional Safety Standard
Failure Model and Effects Analysis Method
Goal Structuring Notation Method
Safety Case Development
Case Study
Conclusions
Contact Information
Acknowledgments
Definitions/Abbreviations
References

CHAPTER 4
Autonomous Vehicle Sensor Suite Data with Ground Truth Trajectories for Algorithm Development and Evaluation

Introduction
Location
Experimental Design
Autonomous Vehicle Sensors
Cameras
CHAPTER 5

Integrating STPA into ISO 26262 Process for Requirement Development

Introduction 54

Process Map for STPA Integration 55
  ISO 26262 55
  STPA 56
  Process Map for Creating Functional Safety Requirement 56

Modeling and Tool Support 57
  Intro to SysML 57

Meta-Model for Hazard Analysis & Requirement Generation 58
  System Engineering Foundations Based on Item Definition 60
  Integration of STPA Step 1 for Evaluating Existing Safety Goals 61
  Integration of STPA Step 2 for Creating Functional Safety Requirements 63
  Consideration for Integration with Cyber Security Analysis 65

Summary/Conclusions 66

Definition/Abbreviations 67

References 67
CHAPTER 6
Hazard Analysis and Risk Assessment beyond ISO 26262: Management of Complexity via Restructuring of Risk-Generating Process

Introduction 70
SOTIF HARA and State Space Explosion 71
HARA Composition 71
Hazards 71
Use Cases 71
HARA and the Hidden Semi-Markov Chain 72
Restructuring of Risk-Generating Process 73
Automatic Emergency Braking (AEB) Example 74
Markov Chain Solution 74
Regions of the Transition Matrix 75
Is There Another Way to Do It? 76
Summary 76
Outlook 77
Contact Information 77
Definitions/Abbreviations 77
References 77

CHAPTER 7
Toward a Framework for Highly Automated Vehicle Safety Validation

Introduction 80
Approach 80
Terminology 81
The Role of Vehicle Test and Simulation 81
Beyond ISO 26262 81
System Test/Debug/Patch as a Baseline Strategy 82
Limitations of Vehicle-Level Testing and Simulation 82
Simulation Realism for Its Own Sake Is Inefficient 83
Clarifying the Goals of Testing 83
HAV Requirements Will Be Incomplete 84
Vehicle Testing for Debugging Can Be Ineffective 84
Vehicle Testing as Requirements Discovery 85
Separating Requirements Discovery and Design Testing 86
Vehicle Testing to Mitigate Residual Risks 86

A Layered Residual Risk Approach 87
Validation According to Safety Requirements 87
Basing Validation on Residual Risks 88
Managing Residual Risks 88
An Example of Residual Risks 89

Improving Observability 90
Controllability and Observability 90
Software Test Points 91
Passing Tests for the Right Reason 91

Coping with Uncertainty 93
Knowns and Unknowns 93
Dealing with Unknown Defects 93
HAV Maturity 94
HAV Probation: Monitoring Assumptions 94
Deploying with Residual Risks 95

Conclusions 95
Contact Information 96
Definitions/Abbreviations 97
References 97

CHAPTER 8
Bayesian Test Design for Reliability Assessments of Safety-Relevant Environment Sensors Considering Dependent Failures 101

Introduction 102
Background: Reliability Assessment of Automotive Environment Perception 103
Null Hypothesis Significance Testing for Sensor Reliability Assessment 104
Performance Evaluation of NHST 105
Alternatives to NHST for Reliability Assessments 106

Bayesian Methodology for Empirical Perception Reliability Assessments of Environment Sensors 106
Statistical Model 106
Mathematical Representation of Dependent Errors 107
CHAPTER 9

Challenges in Autonomous Vehicle Testing and Validation 125

Introduction 126
  Infeasibility of Complete Testing 126
  The V Model as a Starting Point 127

Driver Out of the Loop 127
  Controllability Challenges 128
  Autonomy Architecture Approaches 128

Complex Requirements 129
  Requirements Challenges 130
  Operational Concept Approaches 130
  Safety Requirements and Invariants 131

Non-Deterministic and Statistical Algorithms 132
  Challenges of Stochastic Systems 132
  Non-Determinism in Testing 133

Machine Learning Systems 134
  Challenges of Validating Inductive Learning 134
  Solutions to Inductive Learning 135

Mission Critical Operational Requirements 136
  Challenges of Fail-Operational System Design 136
  Failover Missions 137