

contents

Introduction	xi
--------------	----

CHAPTER 1

Sensor ICs, Semiconductors and Safety	1
Standard-IC Challenges	2
Cost vs. Performance Tradeoffs	4
Implementing Safety Features	4

CHAPTER 2

Calculation of Failure Detection Probability on Safety Mechanisms of Correlated Sensor Signals According to ISO 26262	7
Introduction	8
Diagnostic Function	11
Safety Requirement	11
Safety Mechanism	11
Definition of Sensor Deviations	12
Definition of Sensor Safety Mechanism Deviations	12
Diagnostic Coverage Figures	16
Basic Principle to Calculate Detection Probability	17
Detection Probability Calculation with Sensor Deviations	20
Availability Gap	22
Non Availability Caused by Safe-Faults in Channel 1	22
Non Availability Caused by Faults in Channel 2	25
Improvement Potentials	25
Improve Sensor Accuracy	27
Optimize Safety Mechanism Limit	27
Summary/Conclusions	28
Contact Information	28
Acknowledgments	28
Definitions/Abbreviations	29
References	29

CHAPTER 3

Towards Fail-Operational Systems on Controller Level Using Heterogeneous Multicore SoC Architectures and Hardware Support 31

Introduction	32
Related Work and Environment	33
Concept	34
Implementation	39
Hardware Platform	39
Mapping of the Architecture	39
Dynamic Behavior	41
Realization of the State Transfer Entity	45
Fault Injection	46
Experimental Results	47
Summary	52
Acknowledgments	52
Contact Information	52
References	53

CHAPTER 4

Fail-Operational Safety Architecture for ADAS Systems Considering Domain ECUs 55

Introduction	56
Safety Architecture Mechanisms	56
Fail-Safe Safety Architecture	57
Fail-Operational Safety Architectures	57
1-Out-Of-2 Safety Architecture (1oo2)	57
2-Out-Of-3 Safety Architecture (2oo3)	57
Fail-Operational Safety Architectures for Conventional Systems Considering Domain ECUs with Multicore Processors	58
Fail-Operational Safety Architectures for ADAS Systems Considering Domain ECUs with Multicore Processors	59
Fail-Operational Approach for ADAS	60
Sensor Redundancy/Mapping of Functions to Sensors	61
Electronic Control Unit Redundancy/HW Redundancy	62
Conclusions	66
Contact Information	66
Definitions/Abbreviations	66
References	67

CHAPTER 5

Calculating System Failure Rates Using Field Return Data. Application of SAE-J3083 for Functional Safety and Beyond **69**

1. Introduction	70
2. Modeling System Reliability	70
2.1 Failure Rate and Distribution Assumptions	70
2.2 Failure Rate and Distribution Assumptions	72
3. Calculating Failure Rates	72
3.1 Simplified Calculations	72
3.2 Statistical Confidence Intervals on Failure Rates	73
3.3 Sources for Failure Data and the Required Info	73
4. Operating Time in the Field and Usage Data	74
5. Components Classification and Grouping	74
6. Data Analysis and Failure Rate Calculations	76
6.1 Data Analysis Checklist	76
6.2 Process Flow	76
6.3 Analysis of a Complete Data Set	76
6.4 Data Approximation	77
7. Case Study	78
8. Comparison of SAE-J3083 with the Handbooks Based Methods	81
Summary/Conclusions	81
Contact Information	82
Acknowledgments	82
Definitions/Abbreviations	82
References	82

CHAPTER 6

Calculating Probability Metric for Random Hardware Failures (PMHF) in the New Version of ISO 26262 Functional Safety - Methodology and Case Studies **85**

Introduction	86
ISO 26262 and the Concept of PMHF	86
PMHF and Basic Reliability Calculations	87
Case Study	89

Summary/Conclusions	91
Contact Information	91
Acknowledgments	91
Definitions/Abbreviations	92
References	92
A. Appendix	93

CHAPTER 7

Unsettled Topics Concerning Sensors for Automated Road Vehicles	95
Contributors	96
Introduction	96
State of the Industry	96
Unsettled Domains in Automated Vehicle Sensors	102
Sensor Terminology and Taxonomy	102
Importance and Scope of Vocabulary	102
Frames of Reference	103
Types of Vehicle Sensors	104
Sensor Boundaries Unclear	105
Fields of Coverage	107
Other Terminological Issues	108
Need for a General Glossary	109
Recommendations	109
Testing, Simulation, and Calibration of Sensors	110
Importance of Testing	110
Industry-Wide Alignment of Sensor Testing	111
Benefits from Standardized Testing	112
Benefits from Standardized Simulation	112
Fidelity in Sensor Simulation	113
Other Issues	114
Adjacent Initiatives and Further Considerations	114
Need for a Working Committee	114
Recommendations	115
Integrity, Robustness, and Security of Sensors	116
Importance of Integrity, Robustness, and Security	116
Security Aspects for Sensors	117
Robustness Regarding Scalability	118
Robustness Regarding Disturbances	119

Integrity	120
Adjacent Initiatives and Further Considerations	122
Need for a New Sensor Standard	122
Recommendations	122
Outlook of Data Ownership and Privacy	123
Recommendations	124
Summary/Conclusions	124
Need for Common Practices	124
SAE EDGE™ Research Reports	125
Next Steps for ADS Sensors	125
Recommendations	126
Contact Information	128
Acknowledgments	128
Abbreviations/Definitions	130
Professional References	134

CHAPTER 8

A Model-Driven Approach for Dependent Failure Analysis in Consideration of Multicore Processors Using Modified EAST-ADL 135

Introduction	136
Description of the Approach	137
Approach of System and Safety Modeling	137
Approach of DFA-Analysis	139
A. Necessary Developments of EAST-ADL for the DFA Analysis	140
B. Description of DFA-Analysis and Safety Analysis	141
C. Use-Case and Reports	144
Conclusions	146
Contact Information	146
Acknowledgments	147
References	147

CHAPTER 9

Evaluation of Parallel Executions on Multiple Virtual ECU Systems 149

Introduction	150
Multiple Virtual ECU System	150
Issues and Approach for Virtual Multiple ECUs	151
Multiple ECU Cooperative Simulation	152
vECUCAN-BUS	152

D-EIPF	153
Proposed Configuration	155
Results	157
Deadlock Investigation and Measurement	157
Executions Speed	159
Summary/Conclusions	160
Contact Information	161
Acknowledgments	161
References	161

CHAPTER 10

Bayesian Test Design for Reliability Assessments of Safety-Relevant Environment Sensors Considering Dependent Failures	163
Introduction	164
Background: Reliability Assessment of Automotive Environment Perception	165
Null Hypothesis Significance Testing for Sensor Reliability Assessment	166
Performance Evaluation of NHST	167
Alternatives to NHST for Reliability Assessments	168
Bayesian Methodology for Empirical Perception Reliability Assessments of Environment Sensors	169
Statistical Model	169
Mathematical Representation of Dependent Errors	170
Considering a Non-Stationary Error Rate	172
Bayesian Reliability Assessment and Test Effort Estimation	173
Assessing the Reliability of a Multi-Sensor System	174
Case study: Empirically Demonstrating the Perception Reliability of Environment Sensors	177
Estimating the Necessary Test Drive Effort	177
Evaluating Hypothetical Test Results	178
Influence of Error Dependence on Multi-Sensor Based Machine Vision	178
Discussion	181
Conclusions	182
Contact Information	182
References	183
Appendix	186