Contents

Series Editor's Foreword ix
Preface xi
Abbreviations xv

1 Safety Expectations for Consumers, OEMs, and Tier 1 Suppliers 1
   Trustworthiness 1
   Consumer Expectations 3
   OEM Expectations 4
   Supplier Expectations 6

2 Safety Organizations 11
   The Need for a System Safety Organization 11
     Functions of a Safety Organization 12
   Critical Criteria for Organizational Success 13
     Talent to Perform the Safety Tasks 14
     Integral to Product Engineering 14
     Career Path for Safety Personnel 15
     Safety Process Owned by Program Management 15
   Executive Review 16
   Pillars of a Safety Process 18
   Alternatives, Advantages, and Disadvantages 26

3 System Safety vs. Functional Safety in Automotive Applications 41
   Safety Terminology 41
   Functional Safety Standards vs. System Safety 42
     Background 42
     Application of Functional Safety Standards 42
   Safety of the Intended Function (e.g. SOTIF, ISO PAS 21448) 44
     Triggering Event Analyses 45
     Background 45
     Systematic Analyses 46
   Validation 49
Contents

Validation Targets 49
Requirements Verification 50
Release for Production 53
Integration of SOTIF and Functional Safety and Other Considerations 55
Background 55
Analyses and Verification 57
Validation 58

4 Safety Audits and Assessments 61
Background 61
Audits 61
Audit Format 63
Use of External Auditors 65
Assessments 67
System Safety Assessment 67
Work Product Assessment 67

5 Safety Culture 71
Background 71
Characteristics of a Safety Culture 71
Central Safety Organization 72
Safety Managers 74
Joint Development 75
Enterprise Leadership 75
Liability 75
Customers 77
Safety Culture vs. Organization 77

6 Safety Lifecycle 79
Background 79
Concept Phase Safety 80
Preliminary Hazard Analysis 80
Preliminary Architecture 81
Requirements 83
Design Phase Safety 84
Design-Level Safety Requirements 84
Verification 86
Manufacturing Phase Safety 86
Safety in Use 87
Safety in Maintenance 88
Safety in Disposal 90

7 Determining Risk in Automotive Applications 91
Analyze What the Actuator Can Do 91
Analyze Communication Sent and Received 93
Determine Potential for Harm in Different Situations and Quantify 94

- Exposure 95
- Priority 96

Consider Fire, Smoke, and Toxicity 97

8 Risk Reduction for Automotive Applications 99

- History 99
- Analysis of Architecture 99
  - System Interfaces 100
  - Internal Interfaces 101
- Requirements Elicitation and Management 102
  - Three Sources of Requirements 102
  - Cascading Requirements 104
  - Conflicts with Cybersecurity 105
- Determination of Timing Risks in an Automotive Application 106
  - Milestones 106
  - Samples 107
  - Program Management 108
- Design and Verification 109
  - Sample Evaluation 109
  - Verification 111

9 Other Discussion and Disclaimer 113

- Background 113
- Three Causes of Automotive Safety Recalls – Never “Random” Failures 114
  - Failure Rates 114
  - Recalls Due to Random Hardware Failures 115
  - Causes of Recalls 116
  - Completeness of Requirements 117
  - Timing Risk 118
- “But It’s Not in the ‘Standard’” 118
  - Competing Priorities 119
  - Audits and Assessments 120
- Disclaimer and Motivation for Continuous Improvement 121
  - Policy Statement 122
  - Governance 122
  - Metrics 123
  - Process Documentation 124
  - Tiered Metric Reporting 125
  - Use of Metrics 126

10 Summary and Conclusions 131

- Background 131
- System Safety Is More than Functional Safety 131
Contents

Safety Requirements 132
Safety Process 133

Five Criteria for a Successful Safety Organization Are Key 134

Auditing and the Use of Metrics 135
   Auditing 135
   Metrics 135

Future Considerations for SOTIF 137
   Machine Learning 138

Appendix A   IEC 51508 Compared to Typical Automotive Practices 139
Appendix B   ISO 26262 – Notes on Automotive Implementation 167
References   215
Index 217