

Inhalt

| | |
|---|-------------|
| Vorwort | V |
| Der Autor | XVII |
| 1 Sicherheit als Grundlage der Mobilität | 1 |
| 1.1 Anmerkungen zu diesem Buch. | 3 |
| 1.2 Sicherheit als gesellschaftliches Recht | 4 |
| 1.3 Gesetzliche Grundlagen zu Automobilität. | 6 |
| 1.3.1 Das deutsche Straßenverkehrsgesetz (StVG) | 6 |
| 1.3.2 Entstehung des StVG | 7 |
| 1.3.3 Anpassung des Straßenverkehrsrechts an den Globalisierungstrend | 8 |
| 1.3.4 Anpassung des Straßenverkehrsgesetzes an zukünftige Mobilitätslösungen | 11 |
| 1.3.5 Genfer und Wiener Übereinkommen über den Straßenverkehr | 14 |
| 1.4 EU-Richtlinien | 14 |
| 1.4.1 EU-Richtlinie zum Straßenverkehr | 15 |
| 1.4.2 EG-Fahrzeugklasse | 16 |
| 1.4.3 EU-Richtlinien für neue Kraftstoffe | 17 |
| 1.5 Zulassungsstandards | 17 |
| 1.6 Amerikanische Zulassungsvorschriften | 22 |
| 1.7 Harmonisierung der UN/ECE-Regelungen mit den amerikanischen Zulassungsgesetzen | 23 |
| 1.8 Gesetze und zukünftige Mobilisierung | 25 |
| 1.9 Produkthaftung in Deutschland | 26 |
| 1.10 Gesetzliche Regelungen in China | 30 |

| | | |
|----------|---|-----------|
| 2 | Sicherheit und funktionale Sicherheit | 35 |
| 2.1 | Warum funktionale Sicherheit in Straßenfahrzeugen? | 35 |
| 2.2 | Risiko, Sicherheit und funktionale Sicherheit | 37 |
| 2.2.1 | Ursachen für Gefahren. | 37 |
| 2.2.2 | Risiko und Integritätsdefinition aus der IEC 61508. | 41 |
| 2.2.3 | Risikodefinition aus der ISO 26262. | 51 |
| 2.3 | Qualitätsmanagementsysteme | 54 |
| 2.3.1 | Qualitätsmanagementsysteme aus Sicht der ISO 26262. | 60 |
| 2.3.2 | Qualitätsvorausplanung. | 63 |
| 2.3.3 | Prozessmodelle. | 65 |
| 2.3.4 | V-Modelle. | 66 |
| 2.3.5 | Wasserfallmodell | 70 |
| 2.3.6 | Spiralmodell | 71 |
| 2.4 | Automotive und Sicherheitslebenszyklen | 74 |
| 2.4.1 | Automotive-Sicherheitslebenszyklus | 76 |
| 2.4.2 | Sicherheitslebenszyklus nach ISO 26262. | 78 |
| 2.4.3 | Sicherheit und Sicherheitslebenszyklus | 81 |
| 3 | Sicherheit und System Engineering | 85 |
| 3.1 | Sicherheit als Grundvoraussetzung für neue Mobilitätskonzepte | 85 |
| 3.1.1 | Automatisiertes Fahren als Mobilität der Zukunft | 86 |
| 3.1.2 | Betriebssicherheit. | 90 |
| 3.1.3 | Betriebssicherheitskonzept für das automatisierte Fahren | 92 |
| 3.2 | Erweiterung des Sicherheitslebenszyklus für die automobilen Zukunft | 95 |
| 3.2.1 | Fahrzeug in einer definierten Umgebung | 96 |
| 3.2.2 | Gefahren- und Risikoanalyse. | 97 |
| 3.2.3 | Verifikation und Validation der Maßnahmen | 98 |
| 3.2.4 | Prüfung des relevanten Rechtsraums. | 99 |
| 3.2.5 | Kennzahlen und Kenngrößen | 100 |
| 3.2.6 | Betriebssicherheit für automatisierte Fahrfunktionen. | 102 |
| 3.2.7 | Ansätze zur Zulassung von automatisierten Fahrzeugen für den öffentlichen Straßenverkehr. | 103 |
| 3.2.8 | Normen aus dem Maschinenbau, die sich mit automatisierten Transportsystemen beschäftigen. | 108 |
| 3.2.9 | Erweiterter Sicherheitslebenszyklus | 112 |
| 3.3 | Systemsicherheit | 116 |
| 3.3.1 | Historischer und philosophischer Hintergrund | 117 |
| 3.3.2 | Zuverlässigkeit, Technik und Sicherheit | 120 |

| | | |
|----------|--|------------|
| 3.3.3 | Technische Zuverlässigkeit | 123 |
| 3.3.4 | Zuverlässigkeit und Sicherheit | 127 |
| 4 | System Engineering und Sicherheit | 135 |
| 4.1 | Aspekte der Architekturentwicklung | 135 |
| 4.1.1 | Stakeholder von Architekturen | 138 |
| 4.1.2 | Sichten einer Architektur | 144 |
| 4.1.3 | Horizontale Abstraktionsebene | 147 |
| 4.1.4 | Hierarchie und Architektur | 157 |
| 4.2 | Anforderungs- und Architekturentwicklung | 159 |
| 4.2.1 | Anforderungs- und Designspezifikation | 162 |
| 4.2.2 | Funktionale Architektur und Verifikation | 165 |
| 4.3 | Systemengineering zur Entwicklung von Anforderungen und Architektur | 168 |
| 4.3.1 | Funktionsanalyse | 173 |
| 4.3.2 | Wirkkettenanalyse | 177 |
| 4.3.3 | Softwareentwicklung und Architektur | 180 |
| 4.4 | Fahrzeugsicherheit | 181 |
| 4.4.1 | Historischer Überblick zur Fahrzeugsicherheit | 182 |
| 4.4.2 | Grundlagen der Fahrzeugsicherheit | 186 |
| 4.4.3 | NCAP, „New Car Assessment Program“ | 188 |
| 4.4.4 | Batterie-Sicherheit | 189 |
| 4.4.5 | Fahrzeugsicherheitsarchitektur für E-Fahrzeuge | 192 |
| 5 | Methoden der Systemsicherheit | 197 |
| 5.1 | Anforderungsentwicklung aus den Gefahren- und Risikoanalysen | 197 |
| 5.1.1 | Gefahren- und Risikoanalyse zur Sicherheitsintegrität .. | 202 |
| 5.1.2 | Gefahrenanalyse und Risikobewertung gemäß ISO 26262 | 204 |
| 5.1.3 | Sicherheitsziele | 214 |
| 5.2 | Sicherheitskonzepte | 217 |
| 5.2.1 | Funktionales Sicherheitskonzept | 223 |
| 5.2.2 | Technisches Sicherheitskonzept | 236 |
| 5.2.3 | Mikrocontroller-Sicherheitskonzepte | 240 |
| 5.3 | Systemanalysen | 246 |
| 5.3.1 | Methoden zur Systemanalyse | 246 |
| 5.3.2 | Sicherheitsanalysen gemäß ISO 26262 | 255 |
| 5.3.3 | Fehlerpropagation | 263 |
| 5.3.4 | Fehlerpropagation in der Horizontalen und Vertikalen .. | 270 |
| 5.3.5 | Induktive Sicherheitsanalyse | 274 |

| | | |
|----------|---|------------|
| 5.3.6 | Deduktive Sicherheitsanalyse | 277 |
| 5.3.7 | Quantitative Sicherheitsanalyse | 283 |
| 5.3.8 | Architekturmetriken | 286 |
| 5.3.9 | Top-Fehlermetrik | 292 |
| 5.3.10 | Fehlermetriken bei Sensoren oder anderen Komponenten | 296 |
| 5.3.11 | Metriken der ISO 26262 betrachtet für einen Quarz | 298 |
| 5.3.12 | Analyse der abhängigen Fehler. | 303 |
| 5.4 | Sicherheitsanalysen im Sicherheitslebenszyklus. | 310 |
| 5.5 | Verifikation während der Entwicklung | 318 |
| 5.6 | Verifikation von Anforderungen. | 320 |
| 5.7 | Analyseprozess in Anlehnung an die ARP 4761 | 323 |
| 6 | Produktentwicklung auf Systemebene | 327 |
| 6.1 | Produktentwicklung auf Komponentenebenen. | 334 |
| 6.1.1 | Mechanikentwicklung | 337 |
| 6.1.2 | Elektronikentwicklung. | 338 |
| 6.1.3 | Softwareentwicklung | 344 |
| 6.2 | Funktionale Sicherheit und zeitliche Einschränkungen | 352 |
| 6.2.1 | Sicherheitsaspekte des Fehlerreaktionszeitintervalls | 353 |
| 6.2.2 | Sicherheitsaspekte und Echtzeitsysteme. | 354 |
| 6.2.3 | Timing und Determinismus. | 356 |
| 6.2.4 | Scheduling-Aspekte | 358 |
| 6.2.5 | Gemischte Kritikalität in harten Echtzeitsystemen | 361 |
| 6.2.6 | Programmablaufkontrolle und Mechanismen zu Steuer- und Datenfluss-Monitoring | 364 |
| 6.2.7 | Betriebssysteme im Automobil | 366 |
| 6.2.8 | Sichere Datenverarbeitungsumgebung (Safe Computing Environment). | 368 |
| 6.2.9 | Prädiktive Zustandsüberwachung | 369 |
| 6.3 | Systemengineering in der Produktrealisierung | 370 |
| 6.4 | Systemintegration | 375 |
| 6.5 | Verifikationen und Tests | 377 |
| 6.5.1 | Verifikation basierend auf Sicherheitsanalysen | 380 |
| 6.5.2 | Testmethoden | 383 |
| 6.5.3 | Integration technischer Elemente. | 384 |
| 6.6 | Validierung | 387 |
| 6.7 | Freigaben | 390 |
| 6.7.1 | Prozessfreigaben. | 391 |
| 6.7.2 | Freigabe zur Serienproduktion. | 392 |

| | | |
|----------|---|------------|
| 6.8 | Bestätigung der funktionalen Sicherheit..... | 393 |
| 6.8.1 | Reviews zur Bestätigung der Normerfüllung..... | 394 |
| 6.8.2 | Prozessanalyse zur funktionalen Sicherheit..... | 395 |
| 6.8.3 | Verifikation der Sicherheitsaktivitäten..... | 396 |
| 6.8.4 | Bewertung/Assessment der funktionalen Sicherheit.... | 398 |
| 6.9 | Sicherheitsnachweis..... | 400 |
| 6.10 | Modellbasierende Entwicklung..... | 401 |
| 6.10.1 | Modelle für die funktionale Sicherheit..... | 404 |
| 6.10.2 | Grundlagen für Modelle..... | 408 |
| 6.10.3 | Modellbasierende Sicherheitsanalyse..... | 410 |
| 6.10.4 | Modellierung zur Komplexitätsreduzierung..... | 411 |
| 7 | Anwendungsbeispiele für System-Safety-Engineering..... | 415 |
| 7.1 | Sicherheit in der Cloud..... | 417 |
| 7.1.1 | Flashing over the Air..... | 417 |
| 7.1.2 | Informationen aus der Infrastruktur zur Fahrzeugsteuerung..... | 420 |
| 7.1.3 | Hochverfügbare Sicherheitsarchitektur..... | 423 |
| 7.1.4 | Sicherheitsbegriff für die Cloud..... | 424 |
| 7.2 | Sicherheits- und Schutzfunktionen..... | 427 |
| 7.2.1 | Nominelle Performance..... | 428 |
| 7.2.2 | Redundanz zur Risikoursachenerkennung oder als Maßnahme..... | 436 |
| 7.2.3 | Verfügbarkeit und Sicherheit..... | 439 |
| 7.2.4 | Automatisiertes Fahren auf AD-Level 3..... | 450 |
| 7.3 | Schutzebenen und Barrieren..... | 453 |
| 7.3.1 | Fehler- und Risiko-Pyramide..... | 453 |
| 7.3.2 | Diversität zur Risikoreduzierung..... | 456 |
| 7.3.3 | Künstliche Intelligenz und Sicherheit..... | 459 |
| 7.3.4 | Mehrebenenabsicherung..... | 462 |
| 7.4 | AD-Sicherheitsfunktionen..... | 466 |
| 7.4.1 | Verkehrsraumabsicherung..... | 467 |
| 7.4.2 | Verkehrsraum und Situationserfassung..... | 470 |
| 7.4.3 | Verkehrsraumerfassung..... | 472 |
| 7.4.4 | AD-Wirkkette..... | 473 |
| 7.4.5 | Umfelderfassung an einem Raster..... | 475 |
| 7.5 | Ausblick auf weitere Mobilitätskonzepte..... | 477 |
| | Index..... | 481 |