

Funktionale Sicherheit und Cybersecurity

nach ISO 26262 und ISO/SAE 21434

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhaltsverzeichnis

Vorwort	17
1 Was Sie in diesem Buch erwartet – Einleitung und Überblick	19
1.1 Struktur des Buches	22
1.2 Wie können Sie dieses Buch lesen?	24
1.3 Projektsteckbrief ADAS NextGen	26
1.4 Projekt ADAS NextGen	27
1.5 Die beteiligten Firmen	28
2 Grundlagen und Schlüsseltechnologien für autonomes Fahren	31
2.1 Grundpfeiler der Absicherung	32
2.2 Grundlagen und Funktionsweise automatisierter Fahrzeuge	33
2.3 Evolution der vernetzten Fahrzeugarchitektur	35
2.3.1 Drei Schritte zum erfolgreichen Angriff	37
2.3.2 Projektstory ADAS NextGen: Warum intelligente Fahrzeuge intelligente Sicherheitskonzepte brauchen	38
2.4 Komplexe Anforderungen für vernetzte E/E-Systeme	40
2.4.1 ISO 26262	41
2.4.2 ISO 21448 (SOTIF – Safety of the Intended Functionality)	42
2.4.3 ISO/SAE 21434	43
2.4.4 Elektromagnetische Verträglichkeit (EMV): Schutz vor Störungen in vernetzten E/E-Systemen	44
2.4.5 Fail-Operational- und Fail-Safe-Konzepte: Sicherstellung der Zuverlässigkeit autonomer Fahrfunktionen	45
2.4.6 V2X-Kommunikation: Vernetzung als Schlüssel zur funktionalen Sicherheit und Cybersecurity	46
2.4.7 Datenintegrität und Datenschutz: Grundlage für Vertrauen und Sicherheit im vernetzten Fahrzeug	47

2.5	Die Operational Design Domain	48
2.5.1	Zweck und Bedeutung der ODD	48
2.5.2	Standards im Kontext von ODD	50
2.5.3	ODD-Formate, Simulation und Sicherheit im autonomen Fahren ...	51
2.6	Taxonomiestufen für intelligente Straßenfahrzeuge	54
2.6.1	Die SAE-J3016-Taxonomie	55
2.6.2	Details zu den Taxonomiestufen	58
2.7	Ferngelenkte Fahrzeuge und das neue StVFernLV	59
2.7.1	Rechtlicher Rahmen der StVFernLV	60
2.7.2	Voraussetzungen für die Betriebsbereichsgenehmigung nach § 7 StVFernLV	62
2.7.3	Projektstory ADAS NextGen: Die Drivesmart will fernlenkbare Fahrzeuge entwickeln	64
2.7.4	Von der Regelung zur Praxis: Erfolgsfaktoren für die Teleoperation	65
3	Zusammenspiel von funktionaler Sicherheit, Cybersecurity und KI	67
3.1	Interaktion zwischen funktionaler Sicherheit und Cybersecurity	68
3.2	Einsatzgebiete für KI in Sicherheitsdomänen	70
3.3	Anwendung von KI und maschinellem Lernen	73
3.4	Datenqualitätsmaßnahmen für Analytik und maschinelles Lernen	74
3.5	Anforderungen und Leitlinien für das Datenqualitätsmanagement – DQMS	75
3.6	Rahmen für Datenqualitätsprozesse	77
3.7	Datenqualitäts-Governance	78
3.8	Sichere KI-Zukunft im Fahrzeug: integrierte Standards und technologieneutrale Regeln	80
3.8.1	Herausforderungen durch nicht deterministisches Verhalten	81
3.8.2	ISO/PAS 8800 als Basisrahmen für KI-Sicherheit im Fahrzeug	82
3.9	Zwei Schutzeinrichtungen – ein Ziel: sichere Fahrzeugsysteme	83
3.9.1	Das Konzept der Verlässlichkeit	84
3.9.2	Risikoreduktion durch das Konzept der ASIL- und CAL-Level	87
3.9.3	Ermittlung des CAL	88
3.9.4	Beziehung zwischen CAL und Risiko	89
3.9.5	Anwendung der CAL	90

3.10	Die Rolle ergänzender Standards: ISO/SAE 21434, VDE-AR-E 2842-61, UL 4600 und ISO/IEC TR 5469	91
3.10.1	Der Bedarf nach einem integrierten Normenrahmen	93
3.10.2	Projektstory ADAS NextGen: Einsatz von KI	96
3.11	Lebenszyklusphasen im Überblick	98
3.12	Der Nutzen eines integrierten Sicherheitsansatzes	110
3.13	Verifikation und Validierung unter Berücksichtigung von KI	113
3.13.1	Historische Entwicklung von ISO/TR 4804 zu ISO/TS 5083	113
3.14	Positionierung von ISO/TS 5083 im Normenökosystem	126
3.14.1	Anwendungsbereich und Aufbau der ISO/TS 5083	127
3.14.2	Regulatorische Grundlagen und Safety Framework nach ISO/TS 5083	129
3.15	Verifikation und Validierung von KI-gestützten Fahrfunktionen: Methoden, Teststrategien und kontinuierlicher Sicherheitsnachweis	133
3.15.1	Teststrategien, Prüfplattformen und KI-spezifischen Verifikationsmaßnahmen	135
3.15.2	KI-spezifischen Aspekte, neuronale Netze, Unsicherheitsquantifizierung, Datenintegrität und Robustheit	137
3.16	Verifikation und Validierung unter Berücksichtigung von Cybersecurity	142
3.16.1	Verifikation der TARA-Aktivitäten	142
3.16.2	Systemhärtung (Hardening)	143
3.16.3	Testen der Sicherheitsmechanismen	144
3.16.4	Projektstory ADAS NextGen: Prüfung von Sicherheitsmechanismen	146
3.16.5	Penetrationstests	146
3.16.6	Projektstory ADAS NextGen: Vorbereitung von Penetrationstests	150
3.16.7	Security Monitoring	150
3.16.8	Datenbanken zu Angriffen und Schwachstellen	151
4	Item-Definition und Sicherheitsanalysen	155
4.1	Item-Definition	156
4.1.1	Rolle und Zweck der Item-Definition	156
4.1.2	Projektstory ADAS NextGen: Beschreibung des ADAS	156
4.1.3	Projektstory ADAS NextGen: Komponenten des Items ADAS NextGen	158
4.1.4	Unser betrachtetes System: automatisches Einparksystem APS	164

4.2	Gefährdungs- und Risikoanalyse (G&R)	165
4.2.1	Einführung in die G&R	165
4.2.2	Vorgehen	173
4.2.3	Projektstory ADAS NextGen: Beginn der G&R	176
4.2.4	Analysen am Beispiel ADAS NextGen	178
4.2.5	Einfluss der von Cybersecurity-Risiken	183
4.3	Grundlagen der ASIL-Dekomposition	185
4.3.1	Projektstory ADAS NextGen: Vom Sicherheitsziel zum Sicherheitskonzept	185
4.3.2	Dekomposition von Sicherheitsanforderungen	186
4.3.3	Projektstory ADAS NextGen: Kurzes Beispiel zu sicherem Zustand	189
4.3.4	Vorteile und Implikationen durch die Anwendung der ISO 26262:2018	190
4.3.5	Qualitative und quantitative Methoden	191
4.3.6	Sicherheitsanalyse	192
4.3.7	Projektstory ADAS NextGen: Qualitative und quantitative Methoden	194
4.3.8	Erkenntnistheorie	195
4.4	Threat Analysis and Risk Assessment (TARA)	195
4.4.1	Einführung in die TARA	195
4.4.2	Projektstory ADAS NextGen: TARA-Workshop	199
4.4.3	Angriffspotenzial bewerten	209
4.4.4	Projektstory ADAS NextGen: Bedrohungsanalyse	217
4.4.5	Einsatz von künstlicher Intelligenz	219
4.4.6	TARA und KI-Unterstützung	222
5	Das Lebenszyklusmodell der ISO 26262	225
5.1	Bedeutung und Ziele der ISO 26262:2018 und Zusammenspiel mit anderen Standards	226
5.1.1	Projektstory ADAS NextGen: Sicherheitskultur und Prozessintegration	228
5.1.2	Das phasenorientierte Vorgehensmodell der ISO 26262:2018 Edition 2	229
5.1.3	Die 12 Teile des Standards	232
5.1.4	Die Bedeutung des ASIL in den Tabellen der Norm	233
5.1.5	Bestätigungsmaßnahmen und Unabhängigkeitsgrade	234
5.1.6	Projektstory ADAS NextGen: Unabhängigkeiten für ASIL D – klare Trennung, klare Verantwortung	236

5.2	Funktionales Sicherheitsmanagementsystem	236
5.2.1	Management bei Sicherheitsanomalien im Projekt	238
5.2.2	Projektstory ADAS NextGen: Umgang mit Sicherheitsanomalien	238
5.2.3	Kompetenzmanagement	240
5.3	Sicherheitsplan – Development Interface Agreement – Cybersecurity Interface Agreement	240
5.3.1	Projektstory ADAS NextGen: Erweitertes DIA	242
5.3.2	Sicherheitsmanagement bei Produktion, Betrieb, Inbetriebnahme und Stilllegung	244
5.3.3	Projektstory ADAS NextGen: Produktionsplan, Benutzerhandbuch und Maßnahmen zur Stilllegung	245
5.3.4	Erforderliche Arbeitsprodukte für ISO 26262-2:2018	246
5.4	Erläuterung zu einzelnen Phasen und Aktivitäten	248
5.4.1	Konzeptphase	248
5.4.2	Gefährdungs- und Risikoanalyse	248
5.4.3	Bestimmung des Automotive Safety Integrity Level	249
5.4.4	Festlegung von Sicherheitszielen	250
5.4.5	Funktionales Sicherheitskonzept	250
5.4.6	Technisches Sicherheitskonzept	252
5.4.7	Erforderliche Arbeitsprodukte für ISO 26262-3:2018	253
5.5	Produktentwicklung auf Systemebene	254
5.5.1	Spezifikation der technischen Sicherheitsanforderungen	255
5.5.2	Sicherheitsmechanismen	256
5.5.3	Sicherheitsanalysen und Vermeidung von systematischen Fehlern	257
5.5.4	Spezifikation der Hardware-Software-Schnittstelle	258
5.5.5	Produktion, Betrieb, Service und Stilllegung	258
5.5.6	Systembezogene Verifikationsaktivitäten	259
5.5.7	System-Item-Integration und Test	260
5.5.8	Hardware-Software-Integration und Prüfung	260
5.5.9	Tests auf Systemebene	262
5.5.10	Integration und Prüfung auf Fahrzeugebene	262
5.5.11	Prüfung externer Schnittstellen und Kommunikation	263
5.5.12	Projektstory ADAS NextGen: Kommunikation des ADAS-Steuergeräts	265
5.5.13	Sicherheitsvalidierung	265
5.5.14	Erforderliche Arbeitsprodukte für ISO 26262-4:2018	266

5.6	Produktentwicklung auf Hardwareebene	267
5.6.1	Spezifikation der Hardwareanforderungen	268
5.6.2	Hardwareentwurf	269
5.6.3	Hardware-Sicherheitsanalysen	270
5.6.4	Bewertung der Hardwarearchitekturmetriken	271
5.6.5	Maßnahmen zur Beherrschung von zufälligen Hardwareausfällen während des Betriebs	272
5.6.6	Fehlerannahmen und Fehlerausschlüsse von Hardwarebauteilen ...	279
5.6.7	Hardwareintegration und -verifizierung	291
5.6.8	Erforderliche Arbeitsprodukte für ISO 26262-5:2018	292
5.7	Produktentwicklung auf Softwareebene	294
5.7.1	Agile Softwareentwicklung in sicherheitskritischen Systemen	294
5.7.2	Projektstory ADAS NextGen: Agilität	295
5.7.3	Erfolgsfaktoren für Agilität in der sicherheitskritischen Softwareentwicklung	297
5.8	Automotive SPICE® für agile Entwicklung	300
5.8.1	Software-Sicherheitsanforderungen und Verifikationsplanung	301
5.8.2	Softwarearchitekturentwurf	302
5.8.3	Entwurf und Implementierung von Software-Units	303
5.8.4	Software-Unit-Test	303
5.8.5	Qualifizierung von Softwarekomponenten	304
5.8.6	Softwareintegration und -test	304
5.8.7	Konfigurationsdaten und Kalibrierungsdaten	305
5.8.8	Erforderliche Arbeitsprodukte für ISO 26262-6:2018	306
5.9	Herstellung, Betrieb, Wartung und Außerbetriebnahme	307
5.9.1	Produktionsplan und Produktionskontrollplan	308
5.9.2	Betrieb, Wartung und Außerbetriebnahme	309
5.9.3	Erforderliche Arbeitsprodukte für ISO 26262-7:2018	309
5.10	Bezug zwischen Automotive SPICE® und ISO/SAE 21434	311
5.10.1	Projektstory ADAS NextGen: HARA im ADAS-Projekt – Teamarbeit für Sicherheit	313
6	Der Standard ISO/SAE 21434 für Cybersecurity	315
6.1	Geltungsbereich der ISO/SAE 21434	316
6.2	Überblick über die Anforderungsgruppen	316
6.3	Cybersecurity-Management auf Organisationsebene	318
6.3.1	Cybersecurity Governance	319
6.3.2	Cybersecurity-Kultur	321

6.3.3	Informationsaustausch	322
6.3.4	Managementsysteme	322
6.3.5	Tool-Management-System	323
6.3.6	Cybersecurity-Audit	324
6.3.7	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-05-01 bis RQ-05-17	326
6.4	Projektabhängiges Cybersecurity-Management	328
6.4.1	Cybersecurity-Verantwortlichkeiten	328
6.4.2	Cybersecurity-Planung	329
6.4.3	Cybersecurity-Kontrollen	332
6.4.4	Projektstory ADAS NextGen: Cybersecurity-Kontrollen und Safety Case	333
6.4.5	Tailoring	334
6.4.6	Wiederverwendung von vorhandenen Komponenten	335
6.4.7	Komponenten außerhalb des Kontexts	336
6.4.8	Vorgefertigte Komponenten	337
6.4.9	Cybersecurity Case	339
6.5	Cybersecurity-Assessment	339
6.5.1	Freigabe nach der Entwicklung	341
6.5.2	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-06-01 bis RQ-06-34	341
6.6	Verteilte Cybersecurity-Aktivitäten	346
6.6.1	Lieferantenqualifikation	346
6.6.2	Angebotsanfrage	347
6.6.3	Cybersecurity Interface Agreement	348
6.6.4	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-07-01 bis RQ-07-08	350
6.6.5	Cybersecurity-Aktivitäten während des gesamten Lebenszyklus	351
6.6.6	Cybersecurity-Monitoring	352
6.6.7	Evaluierung von Cybersecurity-Vorfällen	353
6.6.8	Schwachstellenanalyse	355
6.6.9	Schwachstellenmanagement	357
6.6.10	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-08-01 bis RQ-08-08	358
6.6.11	Projektstory ADAS NextGen: Umgang mit einem Angriff	360
6.6.12	Regeln und Verfahren für die Erstellung von Vorlagen	362
6.6.13	Cybersecurity-Konzept	363

6.6.14	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-09-01 bis RQ-09-11	364
6.6.15	Vorlagen zum Cybersecurity-Konzept	366
6.7	Produktentwicklungsphase	367
6.7.1	Ziele der Produktentwicklungsphase	368
6.7.2	Entwurfsphase	368
6.7.3	Integration und Verifikation	370
6.7.4	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-10-1 bis RQ-10-13	371
6.7.5	Der Nutzen von Vorlagen	372
6.8	Cybersecurity-Validierung	374
6.8.1	Validierungsbericht	375
6.8.2	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-11-01 bis RQ-11-02	377
6.8.3	Projektstory NextGen: Validierung eines Cybersecurity Case am Beispiel des automatisierten Parksystems	378
6.9	Produktionsphase	380
6.9.1	Ziele der Produktionsphase	380
6.9.2	Erforderliche Arbeitsprodukte für ISO/SAE 21434, RQ-12-01 bis RQ-12-02	381
6.9.3	Vorlagen für die Fertigungsphase	382
7	SOTIF – Safety of the Intended Funtionality.....	387
7.1	Die Rolle von SOTIF im modernen Fahrzeugdesign	388
7.2	SOTIF-Risiken und gefährliche Ereignisse	389
7.2.1	Fehlerhafte Umweltwahrnehmung und ihre Risiken	389
7.2.2	Sensorbegrenzungen und algorithmische Schwächen	390
7.2.3	Grenzen der Sensorik und das menschliche Verhalten	390
7.2.4	Unerwartetes Nutzerverhalten	390
7.2.5	Beispiele für SOTIF-Risiken	390
7.3	Kooperation von SOTIF mit anderen Normen	393
7.3.1	Projektstory ADAS NextGen: SOTIF	394
7.3.2	Interaktion mit weiteren Standards	394
7.4	Zentrale Begriffe von SOTIF	396
7.4.1	Sicherheit der beabsichtigten Funktionalität (SOTIF)	396
7.4.2	Vernünftigerweise vorhersehbarer Missbrauch	396
7.4.3	Gefährliches Verhalten ohne technisches Versagen	396

7.4.4	Situationsbewusstsein und seine Grenzen	396
7.4.5	Beabsichtigte Funktionalität	397
7.5	Der SOTIF-Entwicklungsprozess	397
7.5.1	Anforderungsanalyse und Systementwurf	397
7.5.2	Mitigationsmaßnahmen	397
7.6	Management von unvorhergesehenen Ereignissen	398
7.6.1	Gefährdungs- und Risikoanalyse	398
7.6.2	Bewertung der Szenarien und Annahmen	399
7.6.3	Die Rolle menschlichen Verhaltens	400
7.6.4	Sicherheitsmarge und Unsicherheit	401
7.7	Verifikation und Validierung	402
7.8	Dokumentation und Rückverfolgbarkeit	403
7.8.1	Projektstory ADAS NextGen: Sensortechnologie	404
7.9	Kontinuierliche Verbesserung	404
7.9.1	Monitoring und On-Board-Diagnose	405
7.9.2	Bedeutung von Datensätzen und Machine Learning	405
7.9.3	Rückkopplung aus realen Daten	406
8	Unterstützende Prozesse und Querschnittsthemen der ISO 26262	409
8.1	Schnittstellen innerhalb verteilter Entwicklungen	410
8.1.1	Projektstory ADAS NextGen: Development Interface Agreement ..	411
8.1.2	Spezifikation und Management von Sicherheitsanforderungen	412
8.2	Unterstützende Prozesse	413
8.2.1	Konfigurationsmanagement	414
8.2.2	Änderungsmanagement	414
8.2.3	Allgemeine Verifikationsprozesse	416
8.2.4	Betriebsbewährtheit	418
8.2.5	Erforderliche Arbeitsprodukte für ISO 26262-8	421
8.3	ASIL-orientierte und sicherheitsorientierte Analysen	422
8.3.1	Dekomposition der Anforderungen im Hinblick auf eine ASIL-Anpassung	423
8.3.2	Analyse von abhängigen Fehlern	425
8.3.3	Projektstory ADAS NextGen: Analyse von abhängigen Fehlern	426
8.3.4	Sicherheitsanalysen	427
8.3.5	Erforderliche Arbeitsprodukte für ISO 26262-9:2018	427

8.4	Safety Element out of Context	428
8.4.1	Projektstory ADAS NextGen: Einsatz von SEooC-Komponenten ..	429
8.5	Normen im Zusammenspiel	431
8.6	Sicheres Zeitverhalten	434
8.7	Wichtige Kenngrößen der Zeit	434
8.7.1	Die Zeit in der ISO 26262:2018	436
8.7.2	Timing-Analysetechniken	438
8.7.3	Projektstory ADAS NextGen: Scheduling	439
8.7.4	ISO 26262:2018 und SoC (System-on-Chip)	441
9	Leitlinien für die Anwendung der ISO 26262 bei der Entwicklung eines SoC.....	443
9.1	Unterteilung eines SoC	444
9.2	Betrachtung von zufälligen Hardwarefehlern und SoC-Ausfallarten	444
9.3	Geistiges Eigentum (Intellectual Property, IP)	446
9.3.1	IP entwickelt als Safety Element out of Context (SeooC)	447
9.3.2	IP im Kontext entwickelt	448
9.3.3	IP-Nutzung durch Evaluierung des Hardwareelements	449
9.3.4	IP-Nutzung durch einen Betriebsbewährtheitsnachweis	451
9.4	Arbeitsprodukte für die Entwicklung einer IP	452
9.5	Analyse von abhängigen Fehlern (DFA) im SoC	453
9.6	ADAS-SoC-Produktion – Anforderungen und Best Practices	456
9.6.1	Planung der Produktion	457
9.6.2	Qualitätsmanagement und Integration von IATF 16949:2016	458
9.6.3	Sicherheitsanforderungen in der Praxis	459
9.6.4	Vorproduktion und Serienproduktion	459
9.6.5	Projektstory ADAS NextGen: Wie man ein ganzes Auto auf einen Chip bekommt	460
10	Spezifische Rollen im Sicherheitslebenszyklus.....	463
10.1	Das effektive Team	463
10.1.1	Projektstory ADAS NextGen: Ressourcenplanung	464
10.2	Qualifikation	467
10.3	Der Sicherheitsmanager auf Projektebene	471
10.4	Rollenbeschreibung Safety Manager im Projekt ADAS NextGen	472
10.4.1	Projektstory ADAS NextGen: Rollenbeschreibung Sicherheitsmanager	474
10.4.2	Rollenbeschreibung Sicherheitskoordinator	475

10.5	Weitere Rollen im Sicherheitslebenszyklus	476
10.5.1	Rolle Vertriebsverantwortlicher und Produktspezialist	477
10.5.2	Sachbearbeiter in der Angebotsabteilung	477
10.5.3	Verantwortlicher für Auftragsabwicklung	477
10.5.4	Produktspezialist ASIL (Mitarbeiter aus dem Produktmanagement)	477
10.5.5	Projektmanager	478
10.5.6	Entwicklungspersonal und Validationspersonal	478
10.5.7	Montagepersonal	479
10.5.8	Prüfer und Personal zur Inbetriebnahme	479
10.5.9	Sachbearbeiter im Service	479
10.5.10	Servicetechniker in Werkstatt	480
10.5.11	Die Rolle des Konfigurationsmanagers im Bereich der funktionalen Sicherheit und Cybersecurity	480
10.5.12	Die Rolle des Änderungsmanagers (Change Manager)	481
10.5.13	Unabhängiger Dritter (Audit & Assessment)	482
10.6	Verantwortlichkeiten im Cybersecurity-Prozess	483
10.6.1	Projektstory ADAS NextGen: Entwicklungsteams	484
11	Geplante Neuerungen zur ISO 26262 Edition 3	489
11.1	Zielrichtung der Neuerungen der ISO 26262 Edition 3	489
11.2	Integration von ISO/TR 9968	490
11.3	Integration von ISO/TR 9839 in ISO 26262-5	491
11.4	Integration von ISO/PAS 8926	492
11.5	Integration von ISO 8800	493
11.6	Erweiterung agiler Softwareentwicklungsmethoden	495
11.7	SOTIF – ISO 21448	496
11.8	Ausblick und Chancen	496
Literaturverzeichnis		499
Normenverzeichnis		507
Glossar		513
Index		541