



Vera Gebhardt · Gerhard M. Rieger ·
Jürgen Mottok · Christian Gießelbach

Funktionale Sicherheit nach ISO 26262

Ein Praxisleitfaden zur Umsetzung

dpunkt.verlag

**Vera Gebhardt · Gerhard M. Rieger ·
Jürgen Mottok · Christian Gießelbach**

Funktionale Sicherheit nach ISO 26262

Ein Praxisleitfaden zur Umsetzung



dpunkt.verlag

Vera Gebhardt: vera.gebhardt@tecmeta.de · <http://www.tecmeta.de>
Gerhard M. Rieger: grieger@tuev-nord.de · <http://www.tuev-nord.de>
Jürgen Mottok: juergen.mottok@hs-regensburg.de · <http://www.las3.de>
Christian Gießelbach: c.giesselbach@tecmeta.de · <http://www.tecmeta.de>

Lektorat: Christa Preisendanz
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Birgit Bäuerlein
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN
Buch 978-3-89864-788-5
PDF 978-3-86491-338-9
ePub 978-3-86491-339-6

1. Auflage 2013
Copyright © 2013 [dpunkt.verlag](http://dpunkt.verlag.de) GmbH
Wieblinger Weg 17
69123 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Vorwort

Der Entschluss, dieses Buch zu schreiben, ist aus den praktischen Erfahrungen während unserer Projekteinsätze entstanden. Mit diesem Buch wollen wir einen Beitrag zum optimalen Funktionieren – insbesondere hinsichtlich der Verfügbarkeit, Zuverlässigkeit und vor allem der möglichst risikofreien Benutzung – von technischen Systemen in zukünftigen, modernen Straßenfahrzeugen leisten.

Die geltenden Standards zur sicherheitsbezogenen Produktentwicklung sind rein aus der Theorie schwer umsetzbar. Das zeigen uns immer wiederkehrende Fragestellungen innerhalb unserer Beratungs- und Assessoren-Tätigkeit für verschiedene Industriebranchen.

Sehr gerne geben wir den Lesern Einblick in unsere gemeinsame jahrzehntelange Erfahrung im Arbeitsgebiet der funktionalen Sicherheit und teilen mit ihnen die Kenntnisse, die wir aufgrund der Begleitung einer Vielzahl sicherheitsrelevanter Entwicklungsprojekte erlangt haben. Wir sind überzeugt, dass mit wachsendem Verständnis für die zu entwickelnden Sicherheitsmechanismen gleichzeitig das Bewusstsein zum sicherheitsbezogenen Denken und Handeln steigt.

In der Ingenieurausbildung stellt das Systemthema der funktionalen Sicherheit eine Verzahnung zwischen Elektrotechnik und der Softwareentwicklung her. Für die Studierenden ermöglicht dies wichtiges Verständnis und die fachliche Durchdringung von softwareintensiven, sicherheitsrelevanten Systemen. Das Bewusstsein für Qualität und funktionale Sicherheit kann bereits in der Ausbildung zukünftiger Ingenieure verankert werden. Dabei helfen aktuelle Forschungs- und Entwicklungsvorhaben mit Partnern aus der Wirtschaft. Die gesellschaftliche Verantwortung der Ingenieure für zukünftige Systeme, wie das autonome Fahren, stellt neue Anforderungen an die funktionale Sicherheit automobiler Systeme – auch dazu wollen wir mit diesem Buch einen Beitrag leisten.

Entwicklerteams leiden besonders unter den Planungsschwächen zu Projektbeginn, die erhebliche Mehraufwände zur Erreichung der geforderten Qualität generieren. Eine wesentliche Intention dieses Buches ist unser Bemühen, den Entwicklungsteams von sicherheitsrelevanten komplexen Systemen anhand

des beschriebenen fiktiven Projekts »Joy« Unterlagen für die Konzept- und Planungsphase für ihre Tätigkeit zur Verfügung zu stellen.

Ohne gut definierte Prozesse und Anforderungen und die dazu passenden Qualifizierungsprüfungen können Menschen, egal wie bemüht sie vorgehen, Fehler im Bereich sicherheitskritischer Aktivitäten nicht vermeiden und schon gar nicht beherrschen. Die Praxis beweist, dass mit der Einhaltung von Standards sowie den daraus abgeleiteten Regeln und Prozessen Fehlerquoten weitgehend reduziert werden können. Genauso wichtig sind die individuellen Eigenschaften eines jeden Teams, das ein gelungenes Produkt unter allen gegebenen Umständen liefern muss. Gelungen bedeutet das In-Verkehr-Bringen eines technisch sicheren und zweckmäßigen Produkts auf den Markt. Wenn wir mit diesem Buch dazu einen kleinen Beitrag leisten können, hat sich unsere Mühe dafür gelohnt.

Unser herzlicher Dank gilt allen Kolleginnen und Kollegen, die zum Gelingen einzelner Kapitel besonders beigetragen haben, vor allem B.Sc. Hermann Kränzle, Dr. Immanuel Höfer (beide TÜV Nord Systems), Dr. Carsten Handel und Dipl.-Inform. (FH) Claus Bernhard (beide tecmata GmbH).

Besonders bedanken wir uns bei unseren Freunden und Familien für ihre Geduld und ihr Verständnis, da wir oft keine Zeit für sie hatten.

Die Zusammenarbeit mit dem Verlag, ganz besonders mit unserer unermüdlichen Lektorin Christa Preisendanz, war hervorragend und das Autorenteam hat gemeinsam ein hartes Stück Arbeit mit viel Humor bewerkstelligt.

Christian, ohne dich wäre die Realisierung dieses Buches nicht möglich gewesen und der Bowmore ist dir sicher.

Vera Gebhardt, Gerhard M. Rieger, Jürgen Mottok, Christian Gießelbach
Wiesbaden, Augsburg, Regensburg, im Mai 2013

Das Autorenteam



(v.l.n.r.) Gerhard M. Rieger · Christian Gießelbach · Vera Gebhardt · Prof. Dr. Jürgen Mottok

Vera Gebhardt

Vera Gebhardt war als geprüfte Versicherungsfachwirtin bis Ende 1999 im Bereich Mehrspartenversicherung und telefonischer Kundendienst für die DBV Winterthur Versicherung im Innendienst tätig. Gleichzeitig baute sie einen stabilen Kundenstamm durch qualifizierte Beratung im Segment Personenversicherung auf. Im Januar 2000 wechselte sie in die IT-Branche mit dem Schwerpunkt Finance and Insurance als leitende Qualitätsmanagerin und Testmanagerin. Mit dem Wechsel in die Ingenieurbranche/Automotive qualifizierte sie sich als SPICE-Assessorin, CMMI-Fachberaterin und Prozess-Expertin und übernahm die Verantwortung als Softwarequalitätsmanagerin für die Rücker AG. Ab 2004 wurde sie für die IAE GmbH leitende Qualitätsmanagerin und Projektmanage-

rin mit Personalverantwortung und Prokuristin. Qualifizierung und Zertifizierung im Bereich Projektmanagement und funktionale Sicherheit folgten. Heute ist Vera Gebhardt zertifizierte SPICE-Assessorin, iSQI Certified Professional for Project Management, Principal Consultant funktionale Sicherheit und Hauptniederlassungsleiterin der tecmata GmbH. Sie ist verantwortlich für die Bereiche Personal, funktionale Sicherheit, Qualitätsmanagement und Projektmanagement sowie für den Ausbau des gesamten Geschäftsnetzes. Vera Gebhardt ist Gründerin und Fachgruppenleiterin der FG Safety im ASQF und Verfasserin zahlreicher Fachvorträge.

vera.gebhardt@tecmata.de · <http://www.tecmata.de>

Gerhard M. Rieger

Gerhard M. Rieger studierte Elektrotechnik/Nachrichtentechnik in Augsburg. Nach seinem Studium war er zunächst als Sachverständiger für Baumusterprüfungen von elektronischen Geräten im IQSE in der Abteilung »Automatisierungs- und Sicherheitstechnik« beim TÜV Bayern e.V. tätig. 1992 übernahm er zusätzlich die Verantwortung für die Prüfstelle des TÜV Bayern Sachsen e.V. und war bis 1998 für das Arbeitsgebiet »Fernmeldeeinrichtungen und Fernwirkanlagen« in leitender Position tätig. Bis 2001 war Herr Rieger als Marktsegmentverantwortlicher für den Bereich sicherheitsrelevante elektronische Systeme bei der TÜV Product Service GmbH tätig und wechselte 2001 zur TÜV Informationstechnik GmbH des RWTÜV als Abteilungsleiter der Prüfstelle »Safety Approval Service«. Sein Aufgabenbereich umfasste den Aufbau des Arbeitsgebiets der funktionalen Sicherheit, personelle Führung sowie die wirtschaftliche Verantwortung der Prüfstelle. Er baute im Mutterkonzern RWTÜV den Aufgabenbereich funktionale Sicherheit weiter aus und wechselte 2004 in die Abteilung Safety Related Services des RWTÜV (seit 2006 TÜV NORD Systemtec GmbH & Co. KG). Dort leitete er bis 2010 die Geschäftsstelle in Augsburg und das Arbeitsgebiet »Functional Safety«. Seit 2011 führt er den Ausbau der Geschäftsstelle Augsburg sowie die Erweiterung des Themengebiets funktionale Sicherheit bei der TÜV NORD Systems GmbH & Co. KG fort.

Herr Rieger ist Verfasser zahlreicher Fachartikel und hält im Elitestudienang Informatik der Universität Augsburg Vorlesungen zum Thema »Funktionale Sicherheit«.

grieger@tuev-nord.de · <http://www.tuev-nord.de>

Prof. Dr. Jürgen Mottok

Prof. Dr. Jürgen Mottok lehrt Informatik an der Hochschule Regensburg. Seine Lehrgebiete sind Software Engineering, Programmiersprachen, Betriebssysteme und Functional Safety. Er leitet das Laboratory for Safe and Secure Systems, ist Beirat des Bavarian Cluster of IT-Security and Safety, Beirat des Automotive Forum Sicherheit Software Systeme, Beirat des ASQF Safety, Mitglied des Leitungsgremiums der Regionalgruppe Ostbayern der Gesellschaft für Informatik, Organisator des Fachdidaktik-Arbeitskreises Software Engineering der Bayerischen Hochschulen und Projektleiter der mit kooperativen Promotionsverfahren ausgestatteten Forschungsprojekte DynaS³ und VitaS³, S³OP und S³EMO. Partner in den Forschungsprojekten sind die AVL Software und Funktions GmbH, die Continental Automotive GmbH, die iNTENCE Automotive GmbH, die Manu AG und die exida GmbH. Prof. Dr. Jürgen Mottok ist in Programmkomitees zahlreicher wissenschaftlicher Konferenzen vertreten. Er ist Träger des Preises für herausragende Lehre, der vom Bayerischen Staatsministerium für Wissenschaft, Forschung und Kunst vergeben wird.

juergen.mottok@hs-regensburg.de · <http://www.las3.de>

Christian Gießelbach

Dipl.-Math. Christian Gießelbach studierte Mathematik und Informatik an der Universität zu Köln und war zunächst als Softwareentwickler für die IVU Traffic Technologies AG tätig. 2007 wechselte er zur tecmata GmbH und betreut dort als Experte für Softwarearchitektur sowie als Testdesigner unterschiedliche Industrieprojekte im Bereich sicherheitsrelevanter Embedded-Entwicklung. Christian Gießelbach ist Principal Consultant für funktionale Sicherheit und verantwortlich für die Konzeption sicherer Softwaresysteme. Er ist Mitglied in der ASQF-Fachgruppe Safety und Berater der Expertengruppe Funktionale Sicherheit der tecmata GmbH.

c.giesselbach@tecmata.de · <http://www.tecmata.de>

Inhaltsverzeichnis

1	Einleitung	1
1.1	Wieso die automotive spezifische Sicherheitsnorm ISO 26262:2011?	1
1.1.1	ISO 26262:2011, Edition 15.11.2011	2
1.1.2	Fachausschuss für Kraftfahrzeuge	3
1.1.3	Stand der Technik	3
1.1.4	ISO 26262:2011 – eine anwendbare Norm	3
1.1.5	Beweislastumkehr	4
1.2	Stufenweise zum ASIL-konformen Produkt	4
1.2.1	Klare Zuordnung von Verantwortung	5
1.2.2	Prozessmodell und Reifegrade von Prozessen	6
2	Was Sie in diesem Buch erwartet	7
2.1	Allgemeine Hinweise	7
	Zielgruppe für dieses Fachbuch	9
2.2	Voraussetzungen und Annahmen unseres Projekts »Joy« mit dem Produkt »Joystick-Sensor«	9
	Rechte Dritter	10
2.3	Wegweiser durch das Buch	11
2.4	Projektsteckbrief »Joy«	11
2.4.1	Die Innovation	12
2.4.2	Produktinformationen	13
2.5	Die beteiligten Firmen	16
2.6	Das Joy-Entwicklungsteam	17
2.7	Rechtliche Grundlagen und Pflichten	19

3	Das Phasenmodell	21
3.1	Organisatorische Anforderungen	21
3.2	Prozessmodelle und funktionales Sicherheitsmanagement	22
3.3	Das Phasenmodell der ISO 26262:2011	22
3.4	Schaffung einer Sicherheitskultur	25
3.4.1	Projektbeispiel	25
3.4.2	Fragenkatalog zur Sicherheitskultur	26
3.4.3	Hinweis World Cafe und Open Space	30
3.5	Management der funktionalen Sicherheit	30
	Vorgehen und Voraussetzungen	30
3.6	Funktionales Sicherheitsmanagement im Projekt Joy	31
3.7	Sicherheitspolitik und Sicherheitsplan der safehicle GmbH	32
	Maßnahmen zur Sicherstellung der funktionalen Sicherheit	32
3.8	Aktivitäten im Sicherheitslebenszyklus	33
3.8.1	Praxisbeispiel Projektstory	33
3.8.2	Managementaktivitäten	35
3.8.3	Bestätigungsmaßnahmen	36
3.9	Unterstützende Prozesse	37
	Tailoring-Anpassungsrichtlinien	37
4	Spezifische Rollen im Sicherheitslebenszyklus	39
4.1	Das effektive Team	39
4.1.1	Projektbeispiel Ressourcenplanung	40
4.1.2	Schulungsbedarf methodisch feststellen	41
4.2	Qualifikation	42
4.3	Der Sicherheitsmanager im Projekt Joy	44
4.4	Rollenbeschreibung FSM	45
4.4.1	Projektbeispiel	46
4.4.2	Der Sicherheitskoordinator im Projekt Joy	47
4.5	Rollenbeschreibung Sicherheitskoordinator	47
4.6	Weitere Rollen im Sicherheitslebenszyklus	49
4.6.1	Rolle Vertriebsverantwortlicher und Produktspezialist	49
4.6.2	Sachbearbeiter in der Angebotsabteilung	49
4.6.3	Verantwortlicher für Auftragsabwicklung	50

4.6.4	Produktspezialist ASIL (Mitarbeiter aus dem Produktmanagement)	50
4.6.5	Projektmanager	50
4.6.6	Entwicklungspersonal und Validationspersonal	51
4.6.7	Montagepersonal	51
4.6.8	Prüfer und Personal zur Inbetriebnahme	52
4.6.9	Sachbearbeiter im Service/Sachbearbeiter in der Auftragsabwicklung	52
4.6.10	Servicetechniker in der Werkstatt	52
4.6.11	Unabhängiger Dritter (Assessment)	53
4.7	Rollenvielfalt	53
5	Konfigurations- und Änderungsmanagement	55
5.1	Konfigurationsmanagement	55
5.1.1	Aufgabe des Konfigurationsmanagements	55
5.1.2	Aktivitäten im KM am Projektbeispiel	56
5.1.3	Meilensteine – Baselines – Schnittstellen – Zugriffe	56
5.1.4	Tooleinsatz und Lieferung von KM-Items	57
5.2	Der Konfigurationsmanager	58
5.3	Änderungsmanagement nach ISO 26262:2011	59
5.4	Planung des CM im Team der Fa. safehicle	61
	Änderungen unter dem Aspekt der funktionalen Sicherheit	61
5.5	Aspekte zur Prozessanpassung	62
5.6	Zustimmungsprozess	63
	Beispiel-Fragenkatalog	64
5.7	Schnittstellenmodifikation und Zustimmung	64
	Betrachtung der technischen Schnittstellen- modifikation	65
5.8	Exkurs Retrospektive	67
5.8.1	Methoden der Retrospektive	67
5.8.2	Durchführung der Retrospektive	68
6	Initialisierung des Sicherheitslebenszyklus und Development Interface Agreement	71
6.1	Initialisierung	71
6.2	Lieferantenauswahl	71

6.3	Qualifikationsanfrage und Auswahlbericht	72
6.4	Development Interface Agreement	74
	Zusammenarbeit in der Lieferkette mit dem OEM	75
6.5	DIA-Vorgehen am Beispiel des Projekts Joy	76
6.6	Initialisierung des Sicherheitslebenszyklus	77
	Projekt Joy – Zuordnung von Phasen und Aufgaben	77
6.7	Exkurs Ausschreibung und Unterbeauftragung	78
7	Das Konzept des Automotive Safety Integrity Level	81
7.1	Historie und Hintergrund zum ASIL	81
7.1.1	Risikoreduktion	82
7.1.2	Vom Sicherheitsziel zum Sicherheitskonzept im Projekt Joy	83
7.2	Die Bedeutung von ASIL in den Tabellen der Norm	84
7.3	ASIL-abhängige Anforderungen und Empfehlungen	85
7.4	Grundlagen der ASIL-Dekomposition	87
7.4.1	Dekompositionsansatz Joystick-Sensor	87
7.4.2	Dekomposition von Sicherheitsanforderungen	87
7.4.3	Grenzen und Einschränkungen der Dekomposition	90
7.4.4	Aspekt der Verfügbarkeit	91
7.4.5	Kurzes Projektbeispiel für sicheren Zustand	91
7.5	Vorteile und Implikationen durch die Anwendung der ISO 26262	92
7.5.1	Verbesserte Prozessqualität	92
7.5.2	Verbesserte Geschäftsbeziehungen	92
7.5.3	Verbesserte Produktqualität	93
7.5.4	Finanzieller Nutzen	93
7.6	Quantitative und qualitative Methoden	94
7.6.1	Qualitative Methode	94
7.6.2	Quantitative Methode	94
7.7	Sicherheitsanalyse	95
7.7.1	Qualitative und quantitative Methoden im Projekt Joy ...	97
7.7.2	Erkenntnistheorie	97

8	Gefährdungs- und Risikoanalyse	99
8.1	Ermittlung von Gefahren und Klassifikation	99
8.2	Durchführung der Analyse – Projektbeispiel	100
	Bericht zur Gefährdungs- und Risikoanalyse	101
8.3	Vorgehen in der Produktlebenszyklusphase	102
8.4	Wechselwirkungen mit anderen Systemen	102
8.5	Risikobewertung	102
	Gefährdungs- und Risikoanalyse durch den Zulieferer am Projektbeispiel	103
8.6	Methode zur Risikobewertung	104
8.7	ASIL-Bestimmung	107
8.8	Konkrete Beispiele aus dem Projekt Joy	109
	8.8.1 Beispiel »Vortrieb«	113
	8.8.2 Beispiel »Bremskraft«	116
	8.8.3 Beispiel »Lenkwinkel«	119
8.9	Abschluss der G&R	120
9	Spezifikation der funktionalen und technischen Sicherheitsanforderungen	121
9.1	Funktionale Sicherheitsanforderungsspezifikation	121
9.2	Spezifikationsvorgehen Joy und Joystick-Sensor	122
	9.2.1 Funktionale Sicherheitsanforderungsspezifikation	122
	9.2.2 Technische Sicherheitsanforderungen des Subsystems ...	122
	9.2.3 Technische Anforderungsumsetzung zur Risikoreduktion	123
	9.2.4 Projektbeispiel Joy	125
9.3	Systemvalidierung	126
9.4	Zuverlässigkeit, funktionale Sicherheit und Verfügbarkeit	127
	Konflikt zwischen Kosten und Verfügbarkeit	127
9.5	Sicherheits-Assessment	128
	9.5.1 Unabhängigkeit	129
	9.5.2 Planung des Sicherheits-Assessments	130
	9.5.3 Agenda zum Sicherheits-Assessment im Projekt Joy	130
	9.5.4 Ableitung von Maßnahmen	134

10	Verifikations- und Validationsplanung	135
10.1	Allgemeine Hinweise zu V+V	135
	Definition zu V+V im Projekt Joy	137
10.2	Handlungsfelder der Verifikation	138
10.2.1	Verifikationsspezifikation	139
10.2.2	Testbericht	140
10.3	Handlungsfelder der Validation	141
10.3.1	Umfang der Validationsplanung	142
10.3.2	Gemeinsame Validationsplanung und Planungsinhalt	143
10.4	Hardware-Software-Integration	145
10.5	Systemintegrationstests	146
10.6	Integrationstestmethoden	148
10.6.1	Fault-Injection-Test	149
10.6.2	Back-to-Back-Test	149
10.6.3	Schnittstellenprüfungen	150
10.6.4	Erfahrungsbasierte Tests	150
10.7	Integration und Tests auf Fahrzeugebene	151
10.8	Validationsplanung der Hardware	152
10.8.1	Hardwareintegration und Hardware-Integrationstest	153
10.8.2	Methoden im Projekt Joy	154
10.8.3	Bewertung der Verletzung von Sicherheitszielen im Hinblick auf zufällige Hardwarefehler	155
10.8.4	Validation der Metriken für zufällige Hardwarefehler	156
10.8.5	Bewertung der Metriken der Hardwarearchitektur	156
10.8.6	Input und Output zur Bewertung des Hardwaredesigns	157
10.8.7	Projektbeispiel Hardwaredesign-Review	157
10.9	Softwaremodultest	158
10.9.1	Methoden zur Ableitung und Durchführung von Softwaremodultestfällen	159
10.9.2	Softwareintegration und Test	160
10.9.3	Softwareintegrationstest	161
10.10	Projektbeispiel Softwaretest	162
10.11	Verifikation der Software-Sicherheitsanforderungen	163
10.12	Analyse und Validierung mechatronischer Systeme	165

11	Produktentwicklung auf Systemebene	167
11.1	2000 Anforderungen in der Konzeptphase	167
11.2	Übersicht	168
11.3	Initialisierung der Produktentwicklungsphase auf Systemebene ...	169
11.4	Spezifikation der technischen Sicherheitsanforderungen	171
11.4.1	Spezifikation von Sicherheitsmechanismen	172
11.4.2	Hardware-Fehlerklassen und Metriken	173
11.4.3	Vorgehensmodell zu den zufälligen Hardwarefehlern ...	175
11.5	Technische Sicherheitsanforderungen im Projekt Joy	176
11.5.1	Der Weg zu technischen Sicherheitsanforderungen	176
11.5.2	Projektbeispiel	178
11.5.3	Fehler in der internen Verarbeitung	179
11.5.4	Redundanz im Systemdesign	180
11.5.5	Anforderungen an die Übermittlung der Sensordaten ...	181
11.6	Systemdesign	182
11.6.1	Vermeidung systematischer Fehler	183
11.6.2	Erkennungsmaßnahmen für zufällige Fehler	183
11.6.3	Projektbeispiel	183
11.6.4	Fault Tree Analysis (FTA)	185
11.6.5	Alternative Metrik »CutSet-Methode« für Hardwarefehler	186
11.6.6	Grenzwerte der Metriken	187
11.7	Spezifikation des Hardware-Software-Interface (HSI)	188
11.8	Verifikation des Systemdesigns	189
11.9	Item-Integration und Tests	190
11.10	Zusammenfassung	190
12	Dokumentation und Arbeitsprodukte	191
12.1	Anforderungen an die Dokumentation	191
	Kennzeichnung und geforderte Informationen	193
12.2	»Wer schreibt, der bleibt« oder »allzu viel ist ungesund« – Projektbeispiel	194
	Planung und Konfliktlösung im Team	194
12.3	Phasenübergreifende Dokumentation	195

12.4	Schlüsseldokumente der ISO 26262:2011 – Teil 2	
	»Funktionales Sicherheitsmanagement«	196
12.4.1	Übergeordneter Sicherheitsmanagementplan	197
12.4.2	Qualifikationsnachweise	197
12.4.3	Anerkanntes dokumentiertes Qualitätsmanagement-system	198
12.4.4	Der Sicherheitsplan	198
12.5	Der Sicherheitsnachweis	200
12.5.1	Der Sicherheitsnachweis – Safety Case (FS-Arbeitsprodukte)	200
12.5.2	Referenzen und relevante Dokumente	200
12.5.3	Referenzen zu zentralen sicherheitsrelevanten Dokumenten	200
12.5.4	Definitionen, Begriffe, Abkürzungen	201
12.5.5	Sicherheitsplan	201
12.5.6	Item-Definition	201
12.5.7	Compliance-Matrix	201
12.5.8	Meeting-Protokolle	201
12.5.9	Arbeitsprodukte aus Planungsprozessen	202
12.5.10	Arbeitsprodukte aus der Initialisierung des Sicherheitslebenszyklus	202
12.5.11	Arbeitsprodukte aus den unterstützenden Prozessen	202
12.5.12	Statusberichte	202
12.5.13	Sicherheitskontrollplanung für die Produktion	202
12.5.14	Auszüge aus der G&R	203
12.5.15	Funktionales Sicherheitskonzept	203
12.5.16	Sicherheitsanforderungsspezifikation	203
12.5.17	Arbeitsprodukte aus Verifikation und Validation	203
12.5.18	Sicherheitsanalyse und Sicherheitsberichte	204
12.5.19	Sicherheitsargumente	204
12.5.20	Safety-To-do-Liste aus dem Sicherheitsnachweis	205
12.5.21	Der Assessmentplan und Prozesskonformität	205
12.5.22	Zusammenfassung	206

12.6	Schlüsseldokumente der ISO 26262:2011 – Teil 3	
	»Konzeptphase«	206
12.6.1	Item-Definition	206
12.6.2	Arbeitsprodukt Einflussanalyse	207
12.6.3	Gefährdungs- und Risikoanalyse	207
12.6.4	Funktionales Sicherheitskonzept	208
13	Abhängige Dokumentation und Arbeitsprodukte	211
13.1	Allgemein	211
13.2	Schlüsseldokumente der ISO 26262:2011 – Teil 4	
	»Produktentwicklung auf Systemebene«	212
13.2.1	Validationsplan und Validationsberichte	213
13.2.2	Sicherheits-Assessment auf Systemebene	214
13.2.3	Dokumentation zur Produktionsfreigabe	214
13.2.4	Technische Sicherheitsanforderungen	215
13.2.5	Das technische Sicherheitskonzept	215
13.3	Schlüsseldokumente der ISO 26262:2011 – Teil 5	
	»Produktentwicklung auf Hardwareebene«	216
13.3.1	Sicherheitsplan auf Hardwareebene	216
13.3.2	Spezifikationen auf Hardwareebene	217
13.3.3	Dokumentation des Hardwaredesigns	218
13.3.4	Sicherheitsanalyse	218
13.3.5	Dokumentation der Hardware-Architekturmetriken	219
13.3.6	Hardwareintegration und Hardwaretest	220
13.4	Schlüsseldokumente der ISO 26262:2011 – Teil 6	
	»Softwarerealisierung«	221
13.4.1	Planung und Initiierung	222
13.4.2	Software-Sicherheitsanforderungen sowie Verifikationsplanung	222
13.4.3	Softwareentwurf	223
13.4.4	Softwaremoduldesign und Softwareumsetzung	223
13.4.5	Softwaremodultest	224
13.4.6	Softwareintegration und Test	224
13.4.7	Konfigurationsdaten und Kalibrierungsdaten	226

13.5	Schlüsseldokumente der ISO 26262:2011 – Teil 7	
	»Produktion und Betrieb«	227
13.5.1	Produktionsplan und Produktionskontrollplan	228
13.5.2	Betrieb, Wartung und Stilllegung	228
13.6	Schlüsseldokumente der ISO 26262:2011 – Teil 8	
	»Unterstützende Prozesse«	229
13.7	Schlüsseldokumente der ISO 26262:2011 – Teil 9	230
	»ASIL- und sicherheitsorientierte Analysen«	230
13.7.1	ASIL-Dekomposition	230
13.7.2	Kriterien für die Koexistenz von Elementen	230
13.7.3	Analyse abhängiger Fehler und Ausfälle	230
13.7.4	Sicherheitsanalyse	231
13.8	Zusammenfassung	231
14	Reviews	233
14.1	Allgemein	233
14.1.1	Vorgehensweise bei Reviews	234
14.1.2	Reviewtechniken	235
14.1.3	Abhängigkeit zwischen ASIL und Reviewtechnik	237
14.2	Lesetechniken	238
14.2.1	Einführung	238
14.2.2	Ad hoc	240
14.2.3	Checklistenbasierte Lesetechnik	241
14.2.4	Reading by stepwise abstraction	242
14.2.5	Fehlerklassenbasiertes Lesen	243
14.2.6	Perspektivenbasiertes Lesen	244
14.2.7	Zusammenfassung	245
15	Vertrauen in Softwarewerkzeuge	247
15.1	Vertrauen in und Qualifikation von Softwarewerkzeugen	247
15.2	Weshalb eine sorgfältige Werkzeugauswahl wichtig ist	248
15.3	Vertrauensgrad – Tool Confidence Level	251
15.3.1	Werkzeug-Qualifizierungsplan	254
15.3.2	Werkzeugdokumentation	254
15.3.3	Werkzeug-Bug-Report	255

15.3.4	Bewertung des Werkzeug-Entwicklungsprozesses	255
15.3.5	Überprüfung der Leistungsfähigkeit des Werkzeugs	255
15.3.6	Qualifizierungsbericht im Projekt Joy	256
15.4	Exkurs: Betriebsbewährtheit	257
16	Retrospektive	261
16.1	Die Planung sicherheitsgerichteter Items	261
16.2	Firma safehicle – Prozessveränderungen aus den Planungsaktivitäten	263
	Auswertungsbericht	265
16.3	Zusammenfassung	268
17	Ausblick	269
	Abschließende Worte der Autoren	269
A	Anhang	271
A.1	Arbeitshilfen-Checklisten zur Planung	271
A.2	Beispiel für Sicherheitskultur	280
A.3	Fundamentaler Testprozess	281
	German Testing Board (GTB)	282
A.4	Psychologische Ursachen von Fehlern	282
A.4.1	Denkfallen als Fehlerursache	283
A.4.2	Zusammenfassung	285
B	Glossar	287
C	Abkürzungsverzeichnis	293
D	Normen und Standards	297
E	Webadressen	299
F	Literaturverzeichnis	301
	Stichwortverzeichnis	305

1 Einleitung

Das Verhüten von Unfällen darf nicht als eine Vorschrift des Gesetzes aufgefasst werden, sondern als ein Gebot menschlicher Verpflichtung und wirtschaftlicher Vernunft.

(Werner von Siemens, 1880)

1.1 Wieso die automotive spezifische Sicherheitsnorm ISO 26262:2011?

Einen wesentlichen Beitrag für die Einschätzung der Zukunft sicherer eingebetteter Systeme liefert die National Roadmap Embedded Systems (NRMES).

NRMES

Die Kombination sicherer eingebetteter Systemkomponenten mit elektronischen und mechatronischen Systemen ist ein typisches Merkmal in der Technik, wie z.B. bei automobilen Sicherheitssystemen. Die NRMES stellt dar, dass eingebettete Systeme oftmals strikten sicherheitskritischen Anforderungen unterliegen, deren Verletzung verheerende Auswirkungen auf Mensch und Technik mit sich bringen kann.

So benötigen viele Systeme – z.B. in der Automobiltechnik, der Avionik oder der Medizintechnik – eine explizite Zulassung, die den Nachweis eines hinreichenden Sicherheitsniveaus erfordert. Für den Nachweis der Sicherheit eines Systems ist Korrektheit weder notwendige noch hinreichende Bedingung. Vielmehr folgt der Sicherheitsnachweis eigenen spezifischen Verfahren, die z.B. die Bestimmung und Bewertung von Risiken (Risikoakzeptanz) verlangen.

Sicherheitsnachweis

In diesem Zusammenhang spielen Verfahren zur Qualitätssicherung (QS) wie Test, Analysetechniken und formale Beweisverfahren eine wichtige Rolle. Sie liefern einen Beitrag zur Zulassung, ersetzen sie jedoch nicht.

QS-Verfahren

In technischen Anwendungsbereichen geht von Softwarefehlern einerseits potenziell eine Gefährdung aus, andererseits ermöglicht Software aber auch die Unterstützung von Sicherheit, indem sie z.B. fort-

Bezug zur Software

laufend Diagnosen des Systemzustands durchführt. Daher ist es unerlässlich, Software in die Sicherheitsanalyse und die Zertifizierung von eingebetteten Systemen einzubeziehen.

*Branchen und funktionale
Sicherheit*

Eingebettete Systeme als bedeutende Innovationstreiber mit hoher querschnittlicher Wirkung bilden das Nervensystem moderner Steuer- und Informationssysteme. In ihnen ist inhärent die funktionale Sicherheit der jeweilig realisierten Produkte sicherzustellen. Dies gilt insbesondere in so wichtigen Gebieten wie Energietechnik, Medizin- und Gesundheitstechnik, Verkehrs- und Transportwesen (mit Automobil-, Schienen-, Luft- und Raumfahrttechnik), Industrieautomatisierung/ Robotik sowie der Informations- und Kommunikationstechnik mit ihren diversen Ausprägungen.

1.1.1 ISO 26262:2011, Edition 15.11.2011

Für die Automobiltechnik enthält der neue Standard ISO 26262:2011 (wir beziehen uns in diesem Fachbuch ausschließlich auf den Stand 15.11.2011 für die Teile 1 bis einschließlich 9 und den Stand 08.01.2012 für den Teil 10 des Standards) Richtlinien zur Entwicklung funktional sicherer Systeme.

Es gibt kaum noch Projekte in der Automobilindustrie, bei denen nicht Sicherheitsanforderungen nach einer ASIL-Klassifikation gefordert werden.

ASIL-Klassifikation

Der ASIL (Automotive Safety Integrity Level) wird nach bestimmten Parametern ermittelt und die Einstufung kann aus einer in der ISO 26262:2011 vorgegebenen Tabelle für jede Gefährdung in den Stufen QM oder ASIL-A bis ASIL-D abgelesen werden. Neuere Technologien wie Assistenzfunktionen und erweiterte Fahrzeugfunktionalitäten sowie die Entwicklung von Mehrwertfunktionen durch Integration bisher getrennter Funktionen führen dazu, dass eine zunehmende Anzahl softwareintensiver elektronischer Systeme als sicherheitsrelevant eingestuft wird und deshalb entsprechend dem Automotive-Sicherheitsstandard ISO 26262:2011 entwickelt werden muss.

Steigende Komplexität

Damit steigt einerseits die Zahl der sicherheitsrelevanten elektronischen Komponenten und Systeme, andererseits werden aber auch die Vernetzung, Interaktion und Komplexität sowie die Sicherheitsanforderungen untereinander immer komplexer. Zusätzlich zu den hohen Sicherheitsanforderungen der einzelnen Systeme wächst auch deren Komplexität bei der heute üblichen verteilten Durchführung der Entwicklungsprojekte. Die Einsatztauglichkeit derartig entwickelter Produkte erfordert einwandfrei funktionierende Hardware und Software in Bezug auf die zu erfüllenden Sicherheitsfunktionen. Neue Zukunfts-

technologien, wie z.B. Hybridantriebe und E-Fahrzeuge, beinhalten beträchtliches Entwicklungspotenzial.

1.1.2 Fachausschuss für Kraftfahrzeuge

Der Fachausschuss für Kraftfahrzeuge (FAKRA) bildete Ende 2003 eine Arbeitsgruppe mit dem Ziel, den generischen Standard IEC 61508 für die Automotive-Industrie zu interpretieren, um die Spezialisierung auf die Serienproduktion in der Automobilbranche abbilden zu können.

Durch die daraus resultierenden Management- und technischen Aktivitäten im Bereich der funktionalen Sicherheit (FuSi) sollen elektronisch basierte Elemente so sicher entwickelt werden, wie es nach dem Stand der Technik möglich ist.

1.1.3 Stand der Technik

Dazu wurde der Stand der Technik bezüglich aller Aspekte, die für die Sicherheit von Bedeutung sind, in der ISO 26262:2011 beschrieben.

Die branchenweite Definition, Einführung und Etablierung dieses überarbeiteten Standards sind abgeschlossen und der Standard wurde in 2011 ratifiziert.

Wird ein Fahrzeug auf allen Ebenen – auch bei allen Zulieferern – gemäß ISO 26262:2011 entwickelt und hergestellt, kann der Automobilhersteller den notwendigen Nachweis liefern, den Erfordernissen bei der Herstellung sicherheitskritischer, elektronischer Einrichtungen entsprochen zu haben. Einige sicherheitsrelevante Funktionen wie z.B. die vollständig elektronisch betätigte Parkbremse, die elektronische Lenksäulenverriegelung, veränderbare Dämpfercharakteristiken bei Fahrzeugen mit Luftfederung, das neue Aktiv-Lenksystem von BMW oder das Dynamic Steering von AUDI, das durch gezieltes Gegenlenken zur Fahrstabilität beiträgt, wurden bereits in Anlehnung an die IEC 61508 bzw. den Normenentwurf der ISO/DIS 26262:2009 entwickelt sowie einem unabhängigen Assessment unterzogen. Diese Entwicklungen erfüllen die höchsten Sicherheitsanforderungen gemäß dem Stand der Technik.

Nachweisführung

1.1.4 ISO 26262:2011 – eine anwendbare Norm

Die steigende Zahl von Rückruf- und Serviceaktionen in den letzten Jahren bekräftigen die Entscheidung für die Anwendung dieses aktuellen Sicherheitsstandards für funktionale Sicherheit von Straßenfahrzeugen < 3,5 t und die darin geforderte Einführung eines funktionalen Sicherheitsmanagements (FSM) bei allen beteiligten Firmen vor Projektstart.

*Produktvertrauen
und Sicherheit*

Eine im Jahr 2010 veröffentlichte Statistik des Kraftfahrt-Bundesamtes (KBA) bezifferte mit 185 Rückrufaktionen einen Rekord. Im Jahr 2000 mussten die Hersteller im Vergleich nur 72-mal Fahrzeuge zurückrufen. Wie das Beispiel einer Gaspedal-Rückrufaktion eines asiatischen OEM zeigt, kann das Vertrauen des Konsumenten in eine Fahrzeugmarke im Extremfall zu Absatzeinbußen und zum Imageschaden führen.

Produkthaftung

Seit der Veröffentlichung der ISO 26262:2011 steht der Automobilbranche eine anwendbare Norm zur funktionalen Sicherheit zur Verfügung, die unter Beteiligung der Automobilindustrie entstand und deren speziellen Belange berücksichtigt. Es gibt derzeit keine Richtlinie und kein Gesetz, das OEMs, Supplier oder Second Tiers zur Anwendung der ISO 26262:2011 verpflichtet. Allerdings definiert eine Norm wie diese immer den Mindeststand der Technik, d.h., im Falle einer Produkthaftung muss nachgewiesen werden, dass der Stand der Technik erreicht wurde. Ohne Anwendung der ISO 26262:2011 wird es im Produkthaftungsfall für die beteiligten Firmen schwierig werden, den Nachweis zu führen, dass der Stand der Technik bzw. Stand der Wissenschaft und Technik eingehalten wurde. Selbst bei deren Umsetzung ist man bei einem Produkthaftungsfall nicht auf der sicheren Seite, weil eben nur dieser Mindeststand der Technik durch eine Norm wie die ISO 26262:2011 repräsentiert wird.

*Stand von Wissenschaft
und Technik*

Der OEM (in unserem Beispiel die Fa. Drivesmart AG) und der Supplier (in unserem Beispiel die Fa. safehicle GmbH) haben also nach wie vor die Verpflichtung, sich nach der Weiterentwicklung des Stands von Wissenschaft und Technik zu erkundigen und sich danach zu richten.

1.1.5 Beweislastumkehr

Werden die Anforderungen einer Norm wie der ISO 26262:2011 bei einer gemeinsamen Entwicklung des elektronischen Lenksystems nicht erfüllt und es kommt in einem Produkthaftungsfall zu dem Vorwurf, der Schaden sei entstanden, weil das Produkt nicht dem Stand von Wissenschaft und Technik entsprochen habe, so ist man gezwungen, das Gegenteil zu beweisen – **Beweislastumkehr**. Dies kann sich beliebig schwierig bis unmöglich gestalten.

1.2 Stufenweise zum ASIL-konformen Produkt

Die ISO 26262:2011 stellt erhebliche Anforderungen an die Verantwortlichkeiten, Entwicklungsprozesse, Dokumentation und Techniken bei der Entwicklung sicherheitsrelevanter Systeme.

Um professionelle Lösungen im sicherheitsrelevanten Bereich zeitnah zu entwickeln, ist fundiertes Know-how durch berufliche Qualifikation und Projekterfahrung notwendig.

Hier unterscheidet sich die Norm nicht wirklich von den Anforderungen an Projekte aus dem nicht sicherheitskritischen Bereich, aber sie verlangt eindeutige Nachweise für diese Qualifikationen.

Nachweispflicht

Es bedarf integrierter, normkonformer und phasenorientierter Prozesse mit methodischen Ansätzen für alle Phasen der Entwicklung, Produktion und Außerbetriebnahme. Also Prozesse, die wirklich über den gesamten Sicherheitslebenszyklus eines Produkts definiert, eingeführt, etabliert, steuerbar, kontrollierbar und verfolgbar sind. Zusätzlich werden die verwendeten Prozesse durch moderne Werkzeuge unterstützt. Definierte und nachvollziehbare Meilensteine und Freigaben sind unabdingbar.

*Notwendigkeit von
Prozessen*

1.2.1 Klare Zuordnung von Verantwortung

Wichtigster Aspekt, um ein Projekt nach den Anforderungen dieser ISO-Norm erfolgreich zu bewältigen, sind die Zustimmung und Verpflichtung der Entscheidungsträger und die klare Zuordnung von Verantwortung.

Die Norm behandelt diese Anforderungen ausführlich und verlangt eine Kultur des sicherheitsbewussten Denkens und Vorgehens im Unternehmen. Abbildung 1–1 zeigt aufeinander aufbauende Schritte, die im Sicherheitslebenszyklus unerlässlich sind.

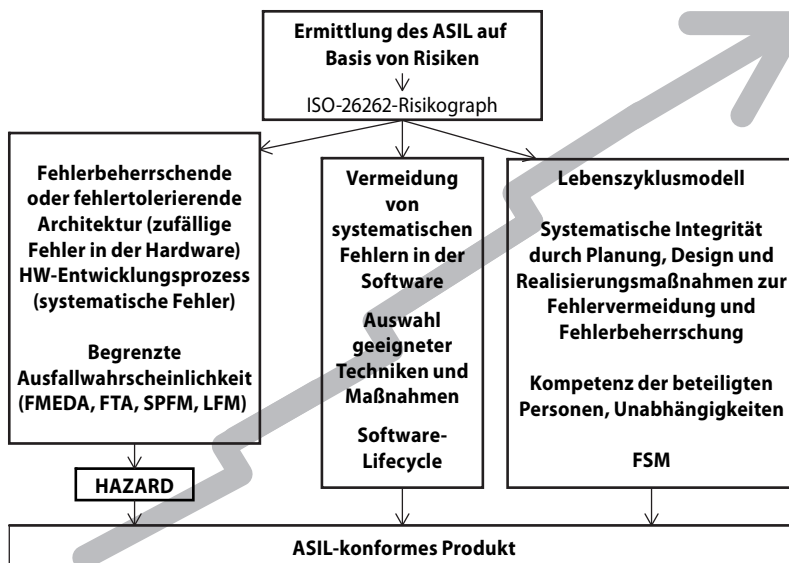


Abb. 1–1

Grundpfeiler der
ISO 26262:2011



Im Verlauf dieses Fachbuches stellen wir Ihnen die Planungsaktivitäten sowie abhängige Arbeitsprodukte samt Methoden und Verfahren vor.

G&R

Im Rahmen der Gefährdungs- und Risikoanalyse (G&R) werden die Gefährdungsszenarien erarbeitet und auf Basis der erkannten Risiken der ASIL ermittelt.



Hierauf gehen wir in Kapitel 8 »Gefährdungs- und Risikoanalyse« detailliert ein.

Zielsetzung

Ziel ist immer, dass zufällige Fehler, systematische Fehler und Common-Cause-Fehler nicht zu einer Fehlfunktion des sicherheitsrelevanten Systems führen und dass als Ergebnis dadurch die Verletzung oder der Tod von Menschen verhindert wird.

*Item-Definition und
Sicherheitslebenszyklus*

Mit der Item-Definition erfolgt die Feststellung, ob es sich um eine Neuentwicklung oder um eine Modifikation handelt, und daraus resultierend muss der gesamte Sicherheitslebenszyklus oder ein geteilter Sicherheitslebenszyklus angewendet werden.

1.2.2 Prozessmodell und Reifegrade von Prozessen

V-Modell

Ein mögliches phasenorientiertes Prozessmodell für die Entwicklungsphasen ist das V-Modell 97 bzw. das V-Modell XT.

Die phasenorientierte und qualitätsgesicherte Projektbearbeitung ist eine zwingende Voraussetzung zur Entwicklung sicherheitsrelevanter eingebetteter Systeme.

Prozessreife

Der Reifegrad der angewandten und gelebten Entwicklungsprozesse kann beispielsweise durch Assessments nach Automotive SPICE bzw. nach CMMI bestimmt werden, um aus den daraus abgeleiteten Optimierungsmaßnahmen die Voraussetzungen für Safety-Compliant-Prozesse zu unterstützen. Allerdings reichen die Maßnahmen aus solchen Reifegrad-Assessments nicht aus, da nicht alle Teile der ISO 26262:2011 durch die geprüften Prozesse adressiert werden. Wir gehen in diesem Buch nicht weiter auf Assessments und Prozesse nach diesen Reifegradmodellen ein, da es hierzu bereits ausreichende und vielseitige Literatur gibt, die wir in Anhang F gerne empfehlen.



Genannte Fachbegriffe erläutern wir Ihnen im Verlauf des Buches bzw. sie sind im Glossar enthalten.

Das nächste Kapitel gibt einen Überblick zum Umfang, zum angesprochenen Leserkreis und zur effektiven Nutzung dieses Fachbuches und führt Sie in die Projektstory ein.

2 Was Sie in diesem Buch erwartet

Anhand eines fiktiven Projektbeispiels aus dem Automotive-Bereich wird in diesem Buch ein anwendungsorientierter Kontext zur praktischen Nutzung der automotive-spezifischen Norm ISO 26262:2011 in den Planungsphasen der Produktentwicklung zu Lernzwecken bereitgestellt. Als Kontext dient das »Projekt Joy« mit einem »Joystick-Sensor« (JSS). Die ausgewählten Fallbeispiele entlang den Projektepisoden zeigen, wie die in der Automotive-Norm geforderten Planungsaktivitäten in einem Pilotprojekt im sicherheitsrelevanten Umfeld umgesetzt werden können.

2.1 Allgemeine Hinweise

Die vorgestellten Unternehmen und Projektteams müssen die Planungsschritte zur Entwicklung eines Lenkgebersystems (Joystick-Sensor), das ASIL-Anforderungen unterliegt, durchführen.

Die Story führt Sie praxisnah durch die Planung bestimmter Lebenszyklusphasen.

Im Einzelnen behandeln wir die folgenden Lebenszyklusphasen mit Bezug auf die entsprechenden Teilabschnitte der ISO 26262:2011:

*Behandelte Teile des
Standards*

- Planungsaktivitäten zur Entwicklung und Einführung eines funktionalen Sicherheitsmanagements in das Projekt Joy und zum Produkt »Joystick-Sensor«

Phase »**Management der funktionalen Sicherheit**« während der Konzeptphase ISO 26262:2011 (Teil 2-6) und die Konzeptphase mit den Teilphasen:

- Item-Definition (Teil 3-5)
- Initiierung des Sicherheitslebenszyklus (Teil 3-6)
- Gefährdungs- und Risikoanalyse (Teil 3-7)
- Funktionales Sicherheitskonzept (Teil 3-8)

Phase »Systementwicklung« – wesentliche Planungsschritte werden erläutert und Abhängigkeiten zwischen den Arbeitsprodukten dargestellt. Wir betrachten insbesondere die notwendige Dokumentation und die erforderlichen Arbeitsprodukte.

- Start der Phase »Systementwicklung« (Teil 4-5); hier schildern wir Aktivitäten und benennen die Verantwortlichen in dieser Phase.
- Die Spezifikation der technischen Sicherheitsanforderungen (Teil 4-6) betrachten wir auf Basis der Gefährdungs- und Risikoanalyse.
- Das Systemdesign (Teil 4-7) ist nicht im Fokus dieses Buches, da wir den Schwerpunkt auf die Planungsaktivitäten zur Umsetzung des funktionalen Sicherheitsmanagements legen. Eine grobe, stark vereinfachte Architektur dient zum Verständnis der sicherheitsrelevanten Items.
- Die Integration des Items (Teil 4-8) setzen wir für die Planungsaktivitäten im Rahmen der Projektstory voraus, behandeln aber nicht die konkrete Umsetzung.
- Das Thema Sicherheitsvalidierung (Teil 4-9) wird u.a. in Kapitel 10 »Verifikations- und Validationsplanung« dargestellt.
- Das funktionale Sicherheitsassessment (Teil 4-10) behandeln wir ausführlich mit Beispielen und Arbeitshilfen
- Die Freigabe des Produkts zur Produktion (Teil 4-11) ist nicht detailliert behandelt.

Zur Phase 5 »Produktentwicklung auf Hardwareebene« und der Phase 6 »Produktentwicklung auf Softwareebene« gehen wir, soweit ohne Abhängigkeit zu Ergebnissen aus der Umsetzung möglich, auf Planungsschritte ein.

Zur Produktion haben wir einen kleinen Exkurs in Kapitel 12 »Dokumentation und Arbeitsprodukte« bezüglich der Planung eingefügt, insgesamt wird der Teil 7 der Norm nicht behandelt.

Die unterstützenden Prozesse (Teil 8) werden anhand der Projektstory zur Anwendung gebracht. Vertiefendes Wissen und Verständnis werden durch Exkurse, Methoden, Rollenbeschreibungen und Arbeitshilfen vermittelt.

Zu Teil 9 erwartet Sie eine detaillierte Ausführung zur Dekomposition.

Stand der Technik

Das Projekt »Joy« mit dem Produkt »Joystick-Sensor« soll nach dem Stand der Technik entwickelt werden.

Hierzu wird die ISO 26262:2011 als branchenspezifische Sicherheitsnorm herangezogen. Die beteiligten Unternehmen wollen die notwendigen Methoden und Aktivitäten »safety compliant« (also in Übereinstimmung mit den normativen Anforderungen) umsetzen, damit ein sicheres Produkt mit den richtigen Prozessen entwickelt wird.