

Hans-Leo Ross

Funktionale Sicherheit im Automobil

Die Herausforderung für Elektromobilität
und automatisiertes Fahren



2., vollständig überarbeitete Auflage

HANSER

Ross

Funktionale Sicherheit im Automobil



Bleiben Sie auf dem Laufenden!

Hanser Newsletter informieren Sie regelmäßig über neue Bücher und Termine aus den verschiedenen Bereichen der Technik. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter

www.hanser-fachbuch.de/newsletter

Hans-Leo Ross

Funktionale Sicherheit im Automobil

Die Herausforderung für Elektromobilität
und automatisiertes Fahren

2., vollständig überarbeitete Auflage

HANSER

Der Autor:
Hans-Leo Ross, Lorsch



Alle in diesem Buch enthaltenen Informationen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt geprüft und getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Buch enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor und Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht.

Ebenso wenig übernehmen Autor und Verlag die Gewähr dafür, dass beschriebene Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

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.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2019 Carl Hanser Verlag München

www.hanser-fachbuch.de

Lektorat: Dipl.-Ing. Volker Herzberg, Julia Stepp

Herstellung: Björn Gallinge

Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München

Titelillustration: © Sebastian Völkel,

unter Verwendung von Grafiken von © shutterstock.com/Andrey Suslov

Coverrealisation: Max Kostopoulos

Satz: le-tex publishing services GmbH

Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen

Printed in Germany

Print-ISBN: 978-3-446-45841-3

E-Book-ISBN: 978-3-446-45842-0

Vorwort

Wenn man das Vorwort der ersten Auflage meines Buches liest und diese Gedanken auf die zweite, vollständig überarbeitete Auflage überträgt, dann gibt es viele Punkte, die einen komplett neuen Inhalt erfahren, wenn man sie aus einem anderen Blickwinkel betrachtet.

Sprach ich im Vorwort der ersten Auflage noch von 20 Jahren Erfahrung im Bereich Funktionssicherheit, so sind es heute Aspekte aus über 35 Jahren Berufserfahrung. Dazu zählen auch Aspekte aus meiner Berufsausbildung als Fernmeldehandwerker – so hieß damals die Ausbildung bei der Deutschen Bundespost (nun Telekom), heute würde man wohl sagen: Ausbildung zum Kommunikationselektroniker –, die heute in einem neuen Licht erscheinen. Als ich mich 1992 als Diplom-Ingenieur ins Berufsleben stürzte, war der Anlagenbau von verschiedenen Katastrophen wie Bhopal und Seveso geprägt. Dass nun in der zweiten Auflage sogar die Seveso-III-Richtlinie erwähnt wird, zeigt, wie sich das Thema Sicherheit über viele Jahre verändert hat. In der ersten Auflage verwies ich auf die VDI/VDE-Richtlinie 2180 „Sicherung von Anlagen der Verfahrenstechnik“ aus dem Jahr 1966, meinem Geburtsjahr. Durch die Elektromobilität muss man auch auf die VDE 100 eingehen, die ihren Ursprung laut VDE im Jahre 1895 hat. Sie handelte damals nicht nur von elektrischen Verbrauchern, sondern auch von Transformatoren, Kabeln/Schienen sowie dem Einsatz von Messtechnik. Im Jahr 1984 wurde die VDE/VDE-Richtlinie 2180 erweitert. Der Begriff „Anlagensicherung mit Mitteln der Mess- und Regeltechnik“ wurde in der Norm eingebracht. Welche Aufgabe haben Sensoren in Fahrzeugregelsystemen wie Lenkung, Bremse und Antrieb? Dies wird heute für Radar, Lidar oder Kamerasysteme im Auto hinterfragt. Welche neuen Sicherheits- oder Schutzfunktionen braucht man für automatisierte Fahrfunktionen? Wie automatisierte man Funktionen, die bisher der Fahrer ausgeführt hat? Man machte einen Unterschied zwischen Betriebs- und Sicherungseinrichtungen sowie Überwachungs- und Schutzeinrichtungen. In der zweiten Auflage wird nun neben den Funktionssicherheitskonzepten auch auf Betriebssicherheits-, Fahrzeugsicherheits- und Datensicherheitskonzepte verwiesen. Das heißt, die alten Perspektiven werden auf neue Technik angewendet.

Die DIN VDE 31000 „Allgemeine Leitsätze für das sicherheitsgerichtete Gestalten technischer Erzeugnisse“ wird heute mit ganz neuen Augen betrachtet. Die Zusammenhänge zwischen Risiko, Sicherheit und Gefahr, die hier beschrieben wurden, müssen nun auf das automatisierte Fahren abgebildet werden. Die Frage nach dem Grenzkrisiko, die in der Norm eingeführt wurde, wird ganz neu gestellt. Zu dieser Zeit waren noch Maschinenstandards gültig, die die Nutzung von Mikrocontrollern für Sicherheitsaufgaben verboten haben. Es gab jedoch bereits einen akzeptierten Markt für Sicherheitssteuerungen. Verschiedene Normen und Standards definierten die Grundlage für Prüfung, Zertifizierung und Auslegung dieser Sicherheitssteuerungen. Sie wurden in Anforderungsklassen (AK 1–8) gemäß der DIN V 19250 klassifiziert. Diese Norm war anwendungs- und technologieunabhängig und beschrieb anhand eines Risikographen ein qualitatives Verfahren zur Risikoabschätzung. Die Beschäftigung mit Risiken, Prüfung und Zertifizierung sind neue Themen, die heute aktuell auch auf die Fahrzeugtechnik abgebildet werden müssen. 1990 erschien die DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“. In der Revision von 1994 wurden Begriffe wie „betriebsbewährt“ und der Einsatz einer „Betrachtungseinheit“ eingeführt. Als Antwort auf die unterschiedlichen Risiko- oder Anforderungsklassen kannte man aber weitgehend nur Redundanz. Scheinbar ist beim Einsatz von Mikroprozessoren und Multi- bzw. Many-Core-Konzepten Redundanz heutzutage die einzige Möglichkeit, solche hochkomplexen Daten- und rechenintensive Systeme noch beherrschen zu können. Selbst der Mensch mit seinen zwei Gehirnhälften setzt auf Redundanz, um sich zu vergewissern, ob er Situationen richtig erfasst. Scheinbar erfasst die eine Gehirnhälfte mehr den Kontext und die andere fokussiert sich auf das Erfassen von konkreten Informationen wie zum Beispiel der Schrift. Bei Zwillingen kann man oft feststellen, dass der oder die eine besser in der Kontexterfassung ist und der oder die andere besser beim Erfassen der beabsichtigten Information. Wer ist die oder der Intelligenter? Oder ist es so, dass die Güte zwischen den beiden Gehirnhälften die wahre Intelligenz ausmacht? Wahrscheinlich wird der eine Zwilling bei jedem Intelligenztest die besseren Ergebnisse haben, der andere wird wohl den höheren EQ haben. Welche Fähigkeit wird bei welchem Test tatsächlich gemessen? Ist dies auch eine Antwort auf die Ideen zur künstlichen Intelligenz? In der Mess- und Regelungstechnik wurden jedoch auch schon diversitäre Messprinzipien genutzt, um Gefahrenszenarien frühzeitig zu entdecken. Heutzutage hat man die Erfahrung gemacht, dass es ein perfektes Messsystem zur Erfassung der Verkehrsumgebung nicht geben kann. Wahrscheinlich wird man auch auf intelligente Sensorfusionen basierende, diversitäre Sensorik und verschiedene logische Algorithmen setzen müssen. Die technischen Regeln für Dampf oder Richtlinien für Druckbehälter schrieben schon die redundante Messung von Druck und Temperatur aus Sicherheitsgründen vor. Selbst das Wasserhaushaltsgesetz kannte die Begrenzung der Füllmenge von Behältern durch Vorschrift oder Regelung sowie die unabhängige

Überfüllsicherung als Sicherheitsmaßnahme. Viele dieser Sicherheitsprinzipien waren in den Sicherheitsstandards der Anlagenbetreiber entstanden und dienten sogar als Grundlage für behördliche Genehmigungen. An all diese Prinzipien müssen wir uns nun bei den Themen Wasserstoff im Fahrzeug oder der Brennstoffzelle zurückerinnern. Als ich 1998 mit dem Vertrieb von Sicherheitssteuerungen begann, wurden besonders in England, den Niederlanden und Norwegen die Entwürfe der IEC 61508 diskutiert. Man kannte die skalierbare Redundanz und es wurde zwischen Redundanz für Sicherheit und Verfügbarkeit unterschieden. Mikrocontroller wurden auch im Lockstep-Prinzip gekoppelt und konnten im laufenden Betrieb der Anlage den Programmablauf oder die Steuerungslogik ändern. Es waren Programmierprogramme verfügbar, die die Sicherheitslogik zwischen einer definierten Laufzeitumgebung konfigurieren konnten. Leider hat man heute feststellen müssen, dass ein Lockstep absolut keine Lösung zur Beherrschung von systematischen Fehlern ist. Wer dies für Software-Fehler nutzen möchte, unterliegt wohl einem systematischen Irrtum.

Mit der Veröffentlichung der IEC 61508 wurde ein Lebenszyklusansatz für Sicherheitssysteme vorgestellt. Des Weiteren wurden die Prozessbetrachtung der Produktentwicklung und der Bezug zu den Qualitätsmanagementsystemen formuliert. Während meines Masterstudiums am Wirtschaftswissenschaftlichen Institut der Universität Basel durfte ich auch die Vorlesung von Professor Dr. Walter Masing genießen, der die Qualitätsmanagementsysteme in Deutschland sehr geprägt hat. Wo sind unsere standardisierten Prozesse für die automatisierten Fahrfunktionen? Wo sind diese für die neuen Antriebssysteme? Wer harmonisiert die Prozesse, um die Fahrzeuge in die neue Verkehrsumgebung systematisch einzubringen? Kann man mit Big-Data und Agilität dies alles ohne Prozesse umsetzen? Die IEC 61508 kannte die Unterscheidung zwischen der beabsichtigten Funktion und den notwendigen Sicherheitsintegritätsmaßnahmen, um eine Anlage oder Maschine absichern zu können. Das „Equipment under Control“, also die zu steuernde Anlage oder Maschine, stand im Fokus der Betrachtung. Ist nicht das automatisierte Fahrzeug im Verkehrsumfeld die zu sichernde Mobilitätsmaschine? Die Einführung der Diagnose zur Sicherung der Funktion bzw. der elektrischen Trägersysteme der Funktion erweiterte den Gedanken der Sicherheitsarchitektur. Heute ergänzen wir die Ideen aus der Medizin- und Flugzeugtechnik. Man setzt auf prädiktive Gesundheitsvorsorge für technische Systeme. Das heißt, man versucht Systemschwächen zu entdecken, bevor sie sich gefährlich auswirken können. 1998 durfte ich in Birmingham das erste passive elektronische System vorstellen, welches bis SIL 4 gemäß IEC 61508 zertifiziert war. Auf einer VDMA-Veranstaltung berichtete ich über die Erfahrung mit der IEC 61508 im Anlagenbau und deren Einfluss auf die Entwicklung von sicherheitsgerichteten Steuerungssystemen. Die ersten Erfahrungen mit Ethernet in der Sicherheitstechnik verwunderte doch viele. Die Maschinenbauindustrie war damals noch sehr stark von Relaistechnik geprägt. Dass die software-

basierende Sicherheitstechnik diese Branche so schnell mit neuen Lösungen und Systemen verändern würde, wollte damals kaum jemand glauben. 80 % der Kommunikation im Fahrzeug sind CAN-Busse, Ethernet existiert in den heutigen Systemen noch immer nicht als Netzwerk. Als ich 2001 die Leitung des Produktmanagements übernahm, galt es, neue Anwendungen für neue Sicherheitssysteme zu finden. Ein weiterer Themenschwerpunkt wurde die vernetzte Sicherheitstechnik, die bis dahin auf seriellen Datenbussen beruhte. Jetzt mussten verteilte und dezentrale Sicherheit sowie dynamische, situations- oder zustandsabhängige Sicherheitssysteme realisiert werden. Als Lösung kam nur noch Ethernet in Frage. Wichtig war hier, die vorhandene Datentechnik für die Sicherheitstechnik handhabbar zu machen. Im Rahmen von Diplomarbeiten wurden Sicherheitssteuerungen in ganz Norwegen verteilt, die auf dem Datennetz der norwegischen Mineralölgesellschaft Statoil sicherheitsrelevante Daten austauschten. Die Erfahrungen mit Datenübertragung über Satelliten zwischen Ölplattformen und Landanlagen oder zwischen Norwegen und Deutschland sowie verschiedenen Lösungen zur Pipelineüberwachung über Funksysteme zeigten, dass sicherheitstechnische Datensysteme auch auf Basis von Ethernet realisierbar sind.

Durch die Veröffentlichung der IEC 61508 als DIN EN 61508 (VDE 0803) „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ im Jahre 2001 wurde die deutsche Automobilindustrie auf das Thema aufmerksam. Öffentlicher Schriftverkehr zwischen dem VDA und den VDTÜVs führte zur Gründung des AK16 im FAKRA (Facharbeitskreis Automobil). Durch meinen Wechsel zu Continental Teves wurde ich 2004 Mitglied in diesem Arbeitskreis. Noch im selben Jahr wurden die ersten Strukturen für die spätere ISO 26262 entworfen und man nahm Kontakt zu weiteren Automobilnormungsgremien in anderen Ländern auf. Insbesondere mit Frankreich wurden konkrete Rahmenbedingungen für die Norm ausgearbeitet. Die erste Sitzung der ISO/TC22/SC03/WG16 fand vom 31.10. bis 2.11.2005 in Berlin statt. Die Arbeitsgruppen aus Frankreich und Deutschland bildeten die größten Fraktionen neben anderen Ländervertretungen aus Japan, USA, Schweden, Großbritannien usw. Bis zu diesem Zeitpunkt kursierte die ISO 26262 unter dem Namen „FAKRA-Norm“. Die safetronic 2005 adressierte bereits die ersten Ideen der zukünftigen Automobilnorm und es wurden Vorträge zu „Best Practices“ und Methoden präsentiert. So konnte ich mit einem Kollegen die neuen Ideen der Sicherheitstechnik zeigen, beispielsweise wie eine Hinterachslenkung die Fahrdynamik erhöhen oder eine Steer-by-Wire-Lösung den Fahrkomfort verbessern kann. Richtige Steer-by-Wire-Systeme sind bisher in keinem Großserienfahrzeug eingesetzt. Für zukünftige automatisierte Fahrfunktionen werden by-Wire-Systeme unumgänglich sein. Woher nehmen wir die Erfahrung, wie solche Systeme in der Verkehrsumgebung und auf den Fahrer einwirken? Es zeigt sich, dass viele Errungenschaften aus der Ingenieurwissenschaften immer wieder neu erfunden werden müssen, weil sich der Kontext ändert, früher sagte

man, weil sich die Zeiten ändern. Wir müssen uns wohl an die alten Philosophen zurückerinnern, die durch Beobachten der Natur bestimmte Zusammenhänge erklären wollten. Durch Induktion wollte man vom Speziellen auf das Allgemeine schließen. Es sieht so aus, dass wir wieder mehr beobachten müssen und das Gesehene in dem wahrgenommenen Kontext beschreiben. Die Metaphysis hat so ihre Hypothesen erstellt.

Viele dieser Aspekte haben gezeigt, dass die ISO 26262 ein wirklich sehr umfangreiches Rahmenwerk ist, doch für die neuen Mobilitätssysteme werden wir alle Risiken betrachten müssen. Dabei müssen wir auch auf das Sicherheitsbedürfnis der Gesellschaft achten und werden die neue Technik aus sehr vielen Perspektiven betrachten müssen. Gesetze wie auch Systeme können nur im beabsichtigten Zielkontext betrachtet und bewertet werden, daher müssen wir lernen, wie sich der Kontext auf die Systeme auswirkt. Ohne eine hinreichende Kontextbetrachtung wird eine Sicherheitsargumentation immer unvollständig sein und weitere Risiken für Leib und Leben in sich bergen.

Dankwort des Autors

Die Erfahrung, die ich in all den Projekten gesammelt habe, die Diskussionen mit den Experten, den Kollegen, in den Arbeitskreisen, mit Hochschulen und bei Vorträgen sowie die Erkenntnisse aus Diplomarbeiten und Förderprojekten haben zu diesem Buch beigetragen. All den beteiligten Menschen möchte ich für die Leidenschaft danken, mit der sie das Thema Mobilität und Sicherheit mit mir betrachtet haben. Neben all den Experten gilt der besondere Dank meiner Familie. Meiner Frau, weil sie geduldig meine Arbeiten begleitet hat und auch meinen Kindern, die zu vielen Zeitpunkten lieber mit mir gespielt hätten. Ich habe es aber auch sehr genossen, mit meiner Tochter auf dem Schoß die lustigen Bilder in diesem Buch anzuschauen. Meine Familie brachte viel Verständnis auf und gab mir den Freiraum, dieses Buch zu schreiben.

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

Der Autor



Hans-Leo Ross ist seit 2019 bei der Robert Bosch GmbH für Fahrzeugsicherheit verantwortlich. Von 2015 bis 2018 war er bei der Bosch Engineering GmbH unter anderem für die Sicherheitsaktivitäten in Fahrzeug- und Luftfahrtprojekten verantwortlich. Dabei entwickelte er auch erste Sicherheitskonzepte für hochautomatisierte Fahrfunktionen. Von 2014 bis 2015 war er bei der Mando Europe verantwortlich für den Infrastrukturaufbau der europäischen Entwicklungsaktivitäten. Dabei wurden in seinem Bereich auch die Basis-Software für zukünftige ESP-Systeme sowie die ersten

Kundenprojekte für elektronische Parkbremsen nach Sicherheitsstandards aktueller Normen und gemäß dem Autosar-Standard entwickelt. Davor war der Autor 10 Jahre bei Continental für die Einführung der Funktionalen Sicherheit verantwortlich und koordinierte alle geschäftsbereichsübergreifenden Sicherheitsaktivitäten. Während dieser Zeit leitete er unter anderem die deutsche Arbeitsgruppe zur ISO 26262 im VDA und vertrat die Interessen vor internationalen Gremien. Zeitweise leitet er auch die Abteilung für Entwicklungsprozesse, Methoden und Tools in den Continental Automotive-Bereichen. Für die Preussag-Noell-LGA Gastechnik plante und realisierte er sicherheitsrelevante Anlagen und Systeme für die Öl- und Gasindustrie. In der Firma HIMA war er zuerst für den Vertrieb von sicherheitsrelevanten Steuerungen in UK sowie Nord- und Osteuropa zuständig, bevor er die Leitung des Produktmanagements übernahm.

Hans-Leo Ross absolvierte sein Ingenieurstudium an der Uni-GH-Paderborn im Fachbereich Elektrotechnik mit dem Schwerpunkt Nachrichtentechnik. Einen Master of Advanced Studies mit Schwerpunkt Betriebswirtschaft und Marketing schloss er berufsbegleitend an der Uni Basel ab.

Sicherheit als Grundlage der Mobilität

Mobilität bedeutet oft, dass Menschen einen Vorteil zum Nachteil anderer haben. Insbesondere die heutige Verkehrssituation zeigt, dass Lärm, Geruch, Abgase und auch der Raum, den unsere Straßen, aber auch Eisenbahntrassen einnehmen, nicht einfach von der Gesellschaft akzeptiert werden. Wenn wir heute auch schon über Luft-Taxis und in Pressemitteilungen bereits über autonome Drohnen sprechen, dann sehen wir, dass hier ein Bedürfnis geschaffen werden soll. Wie schnell wie viele Menschen von einem Ort zum anderen geschafft werden sollen, ist seit Jules Verne Bestandteil eines jeden Science-Fiction-Romans. Aber wie so oft waren die Phantasien aus den Romanen die Vorlage für die heutige Technologie.

Die Gerda Henkel Stiftung fördert Programme zu politischen und sozialwissenschaftlichen Themen. In diesem Zusammenhang hat man ein Sonderprogramm „SICHERHEIT, GESELLSCHAFT UND STAAT“ aufgesetzt. Die Einleitung weist auf die zerfallenden Staaten und die militärischen Konflikte hin, aber die Themen adressieren wohl auch die zukünftige Mobilität.

Hier zwei Beispiele aus den Ausschreibungen (Quelle: <https://www.gerda-henkel-stiftung.de/spsss>):

1. HERAUSFORDERUNGEN DURCH NEUE TECHNOLOGIEN

Sicherheit wird üblicherweise als technisches Problem angesehen, das in erster Linie auf technologische Weise zu lösen ist. Damit Bedrohungen nicht Realität werden, wird der Versuch unternommen, diese mit Hilfe hochentwickelter Waffen- und komplexer Überwachungssysteme sowie umfangreicher Datensammlungen zu identifizieren und auszuschalten. Der Einsatz von Sicherheitstechnologien führt allerdings oftmals zu widersprüchlichen Ergebnissen. Neuere Forschungsansätze weisen daher darauf hin, dass gefährdete Akteure sowohl maßgeblich in die Erzeugung eigener Unsicherheit, als auch in deren Reduzierung oder Beseitigung involviert sind. Im Forschungsfeld „Herausforderungen durch neue Technologien“ sollen Untersuchungen gefördert werden, die sich mit den Beziehungen zwischen der Sicherheit einer Gesellschaft und den zu ihrer Bewahrung eingesetzten technologischen Maßnahmen beschäftigen. Mögliche Forschungsthemen sollen die Verbindungen zwi-

schen der Sicherheit von Staaten und Gesellschaften und jenen technologischen Innovationen untersuchen, die sich sowohl auf die jeweilige Bedrohung selbst als auch auf den Umgang mit ihr auswirken. In Frage kommen könnten hier unter anderem die Bereiche: Cyber-Sicherheit, Überwachung, biometrische Identifizierung, Informationsaustausch, der Schutz kritischer Infrastrukturen, ABC- und Bio-Sicherheit, sowie Krisenmanagement.

2. ÖFFENTLICHE VERWALTUNG UND HUMAN SECURITY

Zur physischen Sicherheit von Menschen und Sachen leisten weite Bereiche der öffentlichen Ordnungs- und Leistungsverwaltung einen Beitrag. Die Relativierung des staatlichen Gewaltmonopols im Bereich Militär und Polizei ist daher nicht gleichbedeutend mit einem Zusammenbruch der öffentlichen Ordnung, wie etwa die Verwaltungs- und Versorgungstätigkeit bewaffneter Gruppen in Bürgerkriegsgesellschaften zeigt. Andererseits kann es auch in stabilen Rechtsstaaten mit sehr leistungsfähigen Verwaltungen zu Sicherheitslücken kommen, wenn vorgesehene Kontrollen aus politischen oder wirtschaftlichen Gründen nicht greifen, Behörden nicht kooperieren oder Warnsignale missachtet werden. Im Forschungsfeld „Öffentliche Verwaltung und Human Security“ sollen Untersuchungen gefördert werden, die sich der Leistung oder dem Versagen der öffentlichen Verwaltung außerhalb von Militär, Polizei und Justiz im Bereich sicherheitsrelevanter Funktionen widmen.

Das erste Thema zeigt die Ängste, die die Menschen gegenüber den neuen Waffensystemen hegen. Diese haben den einen Aspekt, dass sie einen besonderen Schutz für die Anwender bieten. Klar ist der Soldat, der eine ferngelenkte Rakete steuert, nicht mehr selbst gefährdet. Beschießt er fälschlicherweise ein Krankenhaus, so wird er es selber vielleicht nie erfahren. Ein weiterer Aspekt spricht die Ängste an, die geschürt werden, wenn man die Waffen nicht anwendet, oder die Überlegung, wie viele Menschenleben gerettet werden durch die Nutzung solcher Waffensysteme. Daraus entsteht schnell die Frage: Brauchen wir die neue Technik auch, um die Risiken im Verkehr zu mindern?

Das zweite Ausschreibungsthema „ÖFFENTLICHE VERWALTUNG UND HUMAN SECURITY“ spricht die Datensicherheit an. Heute wird es kein besonderes Risiko für die Verkehrsteilnehmer sein, wenn beim Kraftfahrtbundesamt die Datenbanken der Verkehrssünder, die Fahrzeugdatenbank oder die der Führerscheinhalter von Hackern geknackt werden. Insbesondere in den USA gibt es jedoch sehr viele Veröffentlichungen, wie durch Hacker-Angriffe auch Verkehrssysteme zu gefährlichen Waffen von Terroristen werden können.

Daher werden die relevanten Themen für unsere zukünftige Sicherheit im öffentlichen Verkehr wesentlich breiter. Insbesondere die Ingenieure, die sich mit der Technik auseinandersetzen, müssen sich auch mit den gesellschaftlichen Bedürfnissen z. B. zur Sicherheit vertraut machen.

■ 1.1 Anmerkungen zu diesem Buch

Sicherheit war schon immer ein wichtiger Faktor für die Regeln im Verkehrswesen. Das Design des Fahrzeugs sowie aktive Sicherheitssysteme nahmen schon sehr früh einen wesentlichen Schwerpunkt in der Fahrzeugentwicklung ein. In den siebziger Jahren begann dann die Elektronik mit dem Einzug in die Automobile. In den achtziger Jahren gab es die ersten Mikrocontroller im Fahrzeug.

Als 2011 die ISO 26262 als internationaler Standard veröffentlicht wurde, waren bestimmte elektronische Systeme im Fahrzeug bereits sehr weit fortentwickelt. Einige solcher Systeme wie der Airbag oder das Antiblockiersystem wurden sogar schon von den Zulassungsgesetzen gefordert. Zu Beginn des 21. Jahrhunderts, als die erste deutsche Arbeitsgruppe im VDA (Verband der Automobilindustrie) begann, sich mit funktionaler Sicherheit von EE-Systemen zu beschäftigen, war ein schlanker Standard für Produktsicherheit für die elektronischen Systeme das Ziel.

In den folgenden zehn Jahren vor der endgültigen Veröffentlichung der ISO 26262 im Jahre 2011 kompilierten diese Arbeitsgruppen zehn Bände mit annähernd 1.000 Anforderungen. Auch wenn viele einschlägige Kenntnisse, Methoden und Ansätze im Laufe der Jahre diskutiert wurden, so fand man nur einen Bruchteil davon in der ISO 26262. Einige Informationen wurden als Fußnoten aufgenommen, einige verschwanden vollständig, bis die endgültige Veröffentlichung des ersten Standards erfolgte.

Weltweit wurden verschiedene Normungsprojekte initiiert, um den Standard in die jeweilige Landessprache zu übersetzen, ins Deutsche wurde die Norm nie übersetzt.

Die ISO 26262 sollte nie als Leitfaden dienen, sondern Anforderungen an Aktivitäten und Methoden anhand eines Lebenszyklusmodells formulieren.

2018 wurde dann die erste Überarbeitung der Norm veröffentlicht. Bewusst wurde der Umfang der Norm im Wesentlichen nur um kommerzielle Fahrzeuge, wie LKWs und Busse, sowie um Zweiräder (oder Dreiräder) ergänzt. Neben einigen redaktionellen und informativen Änderungen wurde versucht die Struktur beizubehalten. Ein Band 11 wurde ergänzt, der sich mit der Sicherheit von Halbleitern beschäftigt, in Band 10 gab es neue Beispiele, wie man mit sicherheitsrelevanter Verfügbarkeit umgehen könnte, neue Beispiele zur Quantifizierung und zur Analyse der Abhängigkeit im Fehlerfall. Der Band 12 beschreibt eine mögliche Anpassung des Sicherheitslebenszyklus für Zweiräder, wohingegen die Erweiterung für die kommerziellen Fahrzeuge in die Bände 1-9 integriert wurde.

Parallel zur Überarbeitung der Norm gab es einen massiven Aufschwung der Elektromobilität und der Begriff des „automatisierten Fahrens“ oder gar „autonomen Fahrens“ prägte die öffentliche Diskussion zur zukünftigen Mobilität.

Die Aspekte zur Gebrauchs-, Hochvolt- und Aktiven-Sicherheit für die Elektromobilität wurde in der ISO 6469 „Elektrisch angetriebene Straßenfahrzeuge – Sicherheitsspezifikation“ normiert, daher wurden die Themen nicht in der ISO 26262 behandelt.

Rund um das Thema „automatisiertes Fahren“ entwickelte sich eine intensive Diskussion, die in ein Normierungsvorhaben mündete unter dem Namen: „Road vehicles – Safety of the intended functionality“, welches als ISO/PRF PAS 21448 (Public Available Specification) veröffentlicht wurde. Übersetzt heißt der Titel: „Straßenfahrzeuge – Sicherheit der beabsichtigten Funktion“, oft wird die beabsichtigte Funktion auch als Nominalfunktion beschrieben. Im Wesentlichen gehen hier die typischen Aspekte der aktiven Sicherheit, der Schutzsysteme und deren Leistungsmerkmale und der Gebrauchssicherheit ein. Waren bisher Insassenschutzsysteme der Schwerpunkt der aktiven und passiven Sicherheit, so werden nunmehr auch Schutzsysteme für andere Verkehrsteilnehmer in den Fokus gebracht. Neben all den Normen können die Anwendungen für die zukünftige Mobilität nicht mehr unabhängig von den jeweiligen Straßenverkehrsgesetzen betrachtet werden, da Radfahrer und Fußgänger allgemein als die zu schützenden schwächeren Verkehrsteilnehmer zu betrachten sind.

Anforderungen, Hinweise und auch die Ziele der Normen werden oft in einer sehr komplexen und abstrakten Weise beschrieben. Die Wortwahl ist ein Kompromiss der Experten, die diese Sicherheitsstandards entwickeln und nicht unbedingt Muttersprachler sind. Insbesondere die Übersetzungen in diesem Buch aus dem Englischen müssen bereits als Interpretationen des Autors gesehen werden. Jeder Leser geht auf Basis eines anderen Kontexts an die Sicherheitsthemen heran; ob dies auf dem sozialen, beruflichen oder fachlichen Schwerpunkt beruht, kann zu anderen Interpretationen und Bedeutungen der Inhalte der Normen und Gesetze führen. Bindend für die tägliche Arbeit kann nur der Wortlaut der relevanten Gesetze oder Normen sein, die Interpretationshilfen in diesem Buch können lediglich Denkanstöße und Hilfestellungen für den Sicherheitsfachmann bieten.

■ 1.2 Sicherheit als gesellschaftliches Recht

Einer der wesentlichen Punkte staatlicher Ordnung sind die Grundrechte, die den Bürgern in dem jeweiligen Staatengebilde zustehen und auch für Menschen gelten, die sich aus beliebigen Gründen in dem jeweiligen Staatengebilde aufhalten oder auch Handel treiben etc.

In Deutschland gilt das Verständnis, dass Grundrechte folgende Gemeinsamkeiten aufzeigen:

- Sie verpflichten primär den Staat, und zwar unabhängig davon, ob es sich um Exekutive, Legislative oder Judikative, Bund, Land oder Kommune handelt. Verpflichten bedeutet, dass die Grundrechte beachtet werden müssen.
- Es wird nicht unterschieden, ob der Staat im Wege der unmittelbaren oder mittelbaren Staatsverwaltung agiert oder ob er privatrechtlich oder öffentlich-rechtlich oder mittels juristischer Personen des Privatrechts tätig wird.
- Die Grundrechtsberechtigung ist ein Merkmal für die Grundrechtsträgereigenschaft (persönlicher Schutzbereich). Vergleichbar mit der zivilrechtlichen „Rechtsfähigkeit“ muss der Grundrechtsträger das Grundrecht innehaben können, er muss es darüber hinaus aber auch durchsetzen können. Neben der Grundrechtsfähigkeit bedarf er damit einer Grundrechtsmündigkeit, mit der in etwa die zivilrechtliche „Geschäftsfähigkeit“ korreliert. Die beiden Rechtseigenschaften koinzidieren, wo auf die Einsichts- und Entscheidungsfreiheit des Einzelnen nicht abgestellt werden muss, etwa bei Grundrechten, die an der bloßen menschlichen Existenz gemäß der Art. 1 Abs. 1 und 2 Abs. 2 GG haften. Eine Rolle spielt sie, wo einfachgesetzliche Regelungen Altersbestimmungen vorsehen, die eine geistige Auseinandersetzung mit der Regelungsmaterie erforderlich machen, etwa beim Eherecht (Art. 6 GG) oder der religiösen Selbstbestimmung (Art. 4 GG).

Man spricht auch von „Jedermann-Grundrechten“, deren Träger jeder Mensch ist, daher auch der Begriff „Menschenrechte“.

Die Menschenwürde ist nach allgemeiner Auffassung zum einen der Wert, der allen Menschen gleichermaßen und unabhängig von ihren Unterscheidungsmerkmalen wie Herkunft, Geschlecht, Alter oder Status zugeschrieben wird; und zum anderen der Wert, mit dem sich der Mensch als Art über alle anderen Lebewesen und Dinge stellt.

In der Antike hat man die Grundrechte aus der Vernunft (z. B. Aristoteles) der jeweils Stärkeren abgeleitet; diese Prinzipien sind insbesondere auch ins Straßenverkehrsrecht eingeflossen.

Das heißt, jeder Mensch, auch der, der sich auf öffentlichen Straßen bewegt, steht unter einem gewissen Schutz, der durch die Staatsgewalt zu gewährleisten ist.

In allen Lebenssituationen und auch somit in allen Branchen, in denen Unternehmen Produkte liefern oder Dienstleistungen anbieten, gilt es, die Sicherheit der Menschen zu einem gewissen Grad zu garantieren. Damit verbunden ist eine Verpflichtung, einen Schutz für die Menschen bei den jeweils handelnden Parteien umzusetzen, damit Gefährdungen ausgeschlossen sind und Behinderungen nur in dem Maße in Kauf genommen werden müssen, das in dem jeweiligen Kontext als zumutbar gilt.

Somit leiten sich diese Grundrechte auch in alle Bereiche ab, in denen Produkte und Dienstleistungen angeboten werden. Dies hat natürlich dahingehend massive Auswirkungen auf die Gesetze und Regelungen in den verschiedenen Anwendungsbereichen und Branchen.

■ 1.3 Gesetzliche Grundlagen zu Automobilität

Es gibt viele gesetzliche Regelwerke, die den öffentlichen Verkehrsraum betreffen. Hier werden die wesentlichen Gesetze angesprochen, die beachtet werden müssen, um zukünftige Mobilisierungskonzepte erfolgreich in den Markt zu bringen.

1.3.1 Das deutsche Straßenverkehrsgesetz (StVG)

Die Grundlagen, denen zufolge sich Fahrzeuge überhaupt im öffentlichen Straßenverkehr bewegen dürfen, basieren in Deutschland immer noch auf dem Straßenverkehrsgesetz.

Das Straßenverkehrsgesetz (StVG) ist ein Bundesgesetz, es bildet die Grundlagen des Straßenverkehrsrechts in Deutschland. Es regelt weitgehend dieses Rechtsgebiet zusammen mit der Fahrerlaubnis-Verordnung (FeV), der Fahrzeug-Zulassungsverordnung (FZV), der Straßenverkehrs-Ordnung (StVO) und der Straßenverkehrs-Zulassungs-Ordnung (StVZO).

Im Straßenverkehrsgesetz zeigt sich wie in allen Branchen, dass ein sinnvolles Zusammenspiel zwischen Infrastruktur (maßgeblich durch die Straßenverkehrsordnung StVO abgedeckt) und dem mobilen System (im Kraftfahrzeug maßgeblich die StVZO oder später die Fahrzeug-Zulassungsordnung) definiert wird.

Die bekannte StVZO wurde aktuell bereits teilweise durch die FeV und die FZV ersetzt und soll mit Einführung einer Fahrzeug-Genehmigungs-Verordnung (FGV) und einer Fahrzeug-Betriebs-Verordnung (FBV) endgültig abgeschafft werden.

Das Straßenverkehrsgesetz besteht aus folgenden Teilen:

Teil 1 Verkehrsvorschriften

Hier sind die grundlegenden Verkehrsvorschriften zur Zulassung von Kraftfahrzeugen und Anhängern enthalten (näher ausgeführt in der Straßenverkehrs-Zulassungs-Ordnung) sowie zur Zulassung von Personen zum Straßenverkehr als Basis des Fahrerlaubnisrechtes (detailliert ausgeführt in der Fahrerlaubnis-Verordnung). Eine wichtige Vorschrift ist § 6 StVG, die das Bundesverkehrsministerium ermächtigt, weitere Rechtsverordnungen zur Regelung des Straßenverkehrs zu erlassen. Beispiele für Verordnungen aufgrund dieser Vorschrift sind die Straßenverkehrs-Ordnung, die Fahrerlaubnis-Verordnung und die Straßenverkehrs-Zulassungs-Ordnung.

Teil 2 Haftpflicht

Hier werden die Grundlagen zur Haftpflicht für Personen- und Sachschäden bei einem Verkehrsunfall (Gefährdungshaftung) geregelt.

Teil 3 Straf- und Bußgeldvorschriften

Hier sind die Straf- und Bußgeldvorschriften beschrieben, z. B. für das Fahren ohne Fahrerlaubnis, den Kennzeichenmissbrauch und das Fahren unter Einfluss psychoaktiver Substanzen (0,5-Promille-Grenzwert, § 24a StVG).

Teil 4 Fahreignungsregister

Hier sind die Vorschriften für das Fahreignungsregister beschrieben (Eintragung, Verwaltung und Löschung der „Flensburg-Punkte“).

Teil 5 Fahrzeugregister

Hier ist das Fahrzeugregister beschrieben, das Daten der Fahrzeuge und Fahrzeughalter aller in der Bundesrepublik Deutschland zugelassenen Kraftfahrzeuge enthält.

Teil 6 Fahrerlaubnisregister

Hier sind die örtlichen und das zentrale Fahrerlaubnisregister geregelt, das Daten aller in der Bundesrepublik Deutschland ausgegebenen Führerscheine verwaltet und dokumentiert, zeigt, ob diese noch gültig bzw. entzogen sind, etc.

Teil 7 Sonstiges

Hier sind gemeinsame Vorschriften und Übergangsregelungen enthalten.

1.3.2 Entstehung des StVG

Seinen Ursprung hatte das deutsche Straßenverkehrsgesetz mit dem „Gesetz über den Verkehr mit Kraftfahrzeugen“ vom 3. Mai 1909. Hiermit übte ein Gesetzgeber auf dem Gebiet des heutigen Deutschlands erstmalig die generelle Gesetzgebungskompetenz im Verkehrsrecht aus. Durch die Zunahme der Motorisierung regelte man vorrangig die Haftung bei Verkehrsunfällen mit Kraftfahrzeugen, die immer dringlicher wurde. Das Gesetz enthielt aber auch schon erste Verhaltensvorschriften im Straßenverkehr.

Am 23. Januar 1953 trat das Straßenverkehrsgesetz (StVG) der Bundesrepublik Deutschland in Kraft. Es enthielt bereits einige Vorschriften zur Berücksichtigung der aktuellen Rechtsentwicklung, die sich bis heute auswirken. So entspricht die Haftung, abgesehen von mehrfachen Anpassungen ihrer Grenzen oder Detaillierungen des Anwendungsbereichs, heute noch weitgehend unverändert den Regelungen von 1909.

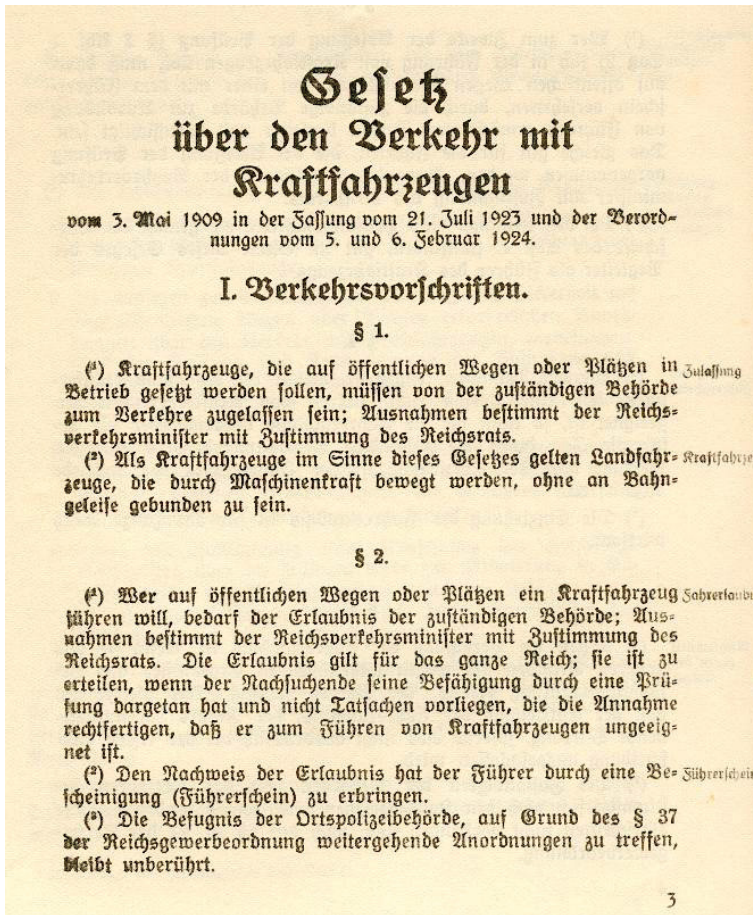


Bild 1.1 Auszug aus „Gesetz über den Verkehr mit Kraftfahrzeugen“ (Quelle: http://www.wikiwand.com/de/Geschichte_des_Führerscheins)

Unter http://www.wikiwand.com/de/Geschichte_des_Führerscheins erfährt man wesentliche Details zur Geschichte des Führerscheins. Nähere Einzelheiten zum Straßenverkehrsrecht sind in (Hentschel et. al 2015) zu finden. Die beiden Quellen sind bestimmt sinnvoll für Nostalgiker, aber für die zukünftigen Mobilisierungskonzepte ist es notwendig, sich mit den Weiterentwicklungen dieser Gesetze zu beschäftigen.

1.3.3 Anpassung des Straßenverkehrsrechts an den Globalisierungstrend

Das StVG muss sich für die Herausforderungen der Europäisierung sowie der weltweiten Wirtschaftsräume kontinuierlichen Anpassungsprozessen unterziehen. Daher wurden Programme aufgelegt, um hier weitere Harmonisierungen zu

erzielen. 2005 waren es in erster Linie der wachsende, auch grenzüberschreitende Verkehr und die Notwendigkeit zur Anerkennung von Regelungen, Verordnungen etc. weltweit.

Hier ein Auszug aus einer Veröffentlichung des Bundes (Quelle: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52004IE1630>):

Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Europäische Straßenverkehrsordnung und europäisches Kfz-Register“ (2005/C 157/04)

3. Kurzer Abriss des auf internationalen Übereinkommen beruhenden Rechts und seines Geltungsbereichs

3.1 Das internationale Straßenverkehrsrecht ist in verschiedenen Abkommen geregelt, von denen das Pariser Abkommen von 1926, das Genfer Abkommen von 1949 und das Wiener Übereinkommen von 1968 hervorzuheben sind.

3.2 Das Internationale Abkommen über Kraftverkehr, das am 24. April 1926 in Paris von 40 Staaten mit dem Ziel geschlossen wurde, den internationalen Tourismus zu fördern, ist derzeit in mehr als 50 Ländern in Kraft.

3.2.1 Dieses Abkommen regelt im Wesentlichen Folgendes:

a) die technischen Mindestanforderungen für Kraftfahrzeuge sowie für die Zulassungskennzeichen, die Beleuchtung und die Unterscheidungszeichen für die Kennlichmachung in anderen Ländern;

b) die Ausstellung und Gültigkeit der internationalen Zulassungsscheine für Kraftfahrzeuge, die freie Zulassung zum Verkehr in allen anderen Vertragsstaaten gewähren;

c) die Anerkennung bestimmter nationaler Führerscheine sowie die Festlegung der Merkmale internationaler Führerscheine; diese gelten in denjenigen Vertragsstaaten, in denen die nationalen Führerscheine nicht anerkannt werden, wobei letztere jedoch mitgeführt werden müssen;

d) die Festlegung von einigen (sechs) Zeichen für die Kennzeichnung gefährlicher Stellen, die die Vertragsstaaten auf ihren Straßen verwenden müssen;

e) die Schaffung eines Systems für die Mitteilung von Auskünften über die Inhaber von internationalen Zulassungsscheinen oder internationalen Führerscheinen, wenn deren Kraftfahrzeug an einem schweren Unfall beteiligt war oder sie sich einer Zuwiderhandlung gegen nationale Verkehrsvorschriften schuldig gemacht haben.

3.2.2 Dieses Abkommen hat zwar die Zollverfahren erleichtert, aber die Fahrzeugführer nicht von der Verpflichtung entbunden, die jeweiligen nationalen Straßenverkehrsvorschriften zu kennen und einzuhalten.

3.2.3 Auf der anderen Seite war das Inkrafttreten des Abkommens von seiner Ratifizierung durch die einzelnen Unterzeichnerstaaten und der Hinterlegung der Ratifizierungsurkunde abhängig. In der Regel gilt das Abkommen lediglich im Mutter-

land, während es in anderen in irgendeiner Form von dem betreffenden Staat verwalteten Gebieten nur durch eine ausdrückliche Erklärung wirksam wird.

3.3 Mit dem Abkommen über den Straßenverkehr, das am 19. September 1949 von 17 Staaten geschlossen wurde und heute in mehr als 120 Ländern in Kraft ist, wurde in den Unterzeichner- und Beitrittsstaaten das Abkommen von 1926 aufgehoben.

3.3.1 In diesem Abkommen, in dem die Grundprinzipien des früheren Abkommens im Einklang mit der Entwicklung der Automobilindustrie weiter ausgestaltet wurden, wurde eine zunehmende Sorge um die Straßenverkehrssicherheit deutlich.

3.3.2 Es wurden keine Verkehrszeichen verankert, sondern lediglich festgelegt, dass die Staaten ihre Verkehrszeichen vereinheitlichen und deren Verwendung auf das absolute Minimum beschränken müssen.

3.3.3 In dem Abkommen werden nur wenige Verkehrsvorschriften festgelegt, und abgesehen von den Regelungen betreffend die Vorsichtsmaßnahmen an Kreuzungen sowie die Vorfahrt und Beleuchtung enthält es keine größeren Neuerungen.

3.3.4 Für das Inkrafttreten dieses Abkommens galten die gleichen Bedingungen wie oben beschrieben, und seine Harmonisierungswirkung wurde dadurch eingeschränkt, dass die Staaten nicht zur Anwendung aller Bestimmungen verpflichtet waren und auch die Änderungen zu dem Abkommen ablehnen konnten.

3.4 Das Übereinkommen über den Straßenverkehr, das am 8. November 1968 in Wien von 37 Staaten unterzeichnet wurde, ist derzeit in rund 100 Staaten in Kraft. Mit der Ratifizierung dieses Übereinkommens und der Hinterlegung der Ratifizierungsurkunden wurden zwischen den jeweiligen Vertragsstaaten untereinander die Abkommen von 1926 und 1949 außer Kraft gesetzt.

3.4.1 Es handelt sich hierbei um das bisher umfassendste Abkommen über die Verkehrsregelung, der ein 30 Artikel enthaltendes Kapitel mit Bestimmungen für die verschiedenen Manöver gewidmet ist, die den wesentlichen Kern moderner Straßenverkehrsordnungen bilden. Das Übereinkommen von 1968 geht über die minimalistischen Zielsetzungen der früheren Abkommen hinaus, die sich auf Verkehrskreuzungen und die diesbezüglichen Verkehrszeichen beschränkten. Es legte nicht nur die Grundsätze fest, die die Fahrzeugführer bei riskanten Manövern beachten müssen (z. B. Überholen, Fahrtrichtungsänderung, Vorsichtsmaßnahmen gegenüber Fußgängern), sondern regelte auch Dinge wie Halten und Parken, Ein- und Aussteigen von Fahrgästen, Fahren in Tunneln – summa summarum alle Standardsituationen im Straßenverkehr.

3.4.2 Es ging insofern weiter als die früheren Abkommen, als die Unterzeichner- und Beitrittsstaaten verpflichtet wurden, die erforderlichen Maßnahmen zu treffen, damit die in ihrem Hoheitsgebiet geltenden Verkehrsregeln in ihrem sachlichen Gehalt mit den in Kapitel II enthaltenen Bestimmungen übereinstimmen, was den Vorteil mit sich bringt, dass die Führer von Fahrzeugen bei Fahrten in anderen Vertragsstaaten mit dem wesentlichen Inhalt der Verkehrsregeln vertraut sind.

3.4.3 Es wurde jedoch die Möglichkeit offengelassen, dass die Staaten Änderungen zum Übereinkommen ablehnen.

3.5 Anhand dieser Übersicht ist unschwer zu erkennen, dass im mittlerweile bereits um 10 neue Mitgliedstaaten erweiterten Unionsgebiet drei internationale Abkommen in Kraft sind, allerdings nicht in allen Staaten gleichermaßen (12). Die Europäische Union ist daher noch weit von einer Harmonisierung der Straßenverkehrsvorschriften entfernt, insbesondere da zu den Bestimmungen dieser Abkommen noch 25 nationale Rechtsvorschriften hinzuzurechnen sind, die sich ständig ändern (13).

3.6 Einige Hemmnisse wurden bereits bzw. werden derzeit beseitigt, z. B. durch die Abschaffung der Binnengrenzen, die Angleichung der Zulassungsbedingungen für Fahrzeuge und Fahrzeugbauteile sowie die gegenseitige Anerkennung der Führerscheine und die Harmonisierung der einschlägigen Bedingungen. Getan werden muss jedoch noch etwas beim wesentlichen Kern des Straßenverkehrs: bei den Verkehrsregeln und den Verkehrszeichen.

3.7 Für die anderen Länder erleichtern die Abkommen zwar die Zollverfahren und das Führen von Fahrzeugen im Unionsgebiet, aber die Angehörigen von Drittstaaten, die die Europäische Union bereisen, haben es mit ebenso vielen unterschiedlichen Straßenverkehrsordnungen zu tun wie die Union Mitgliedstaaten zählt.

Dieser Auszug zeigt, dass auch der Gesetzgeber erkannt hat, dass die heutigen Gesetze viele Abhängigkeiten haben und selbst Fachleute, z. B. Juristen, vor große Schwierigkeiten stellen, den richtigen Weg für eine Entwicklung festzulegen.

1.3.4 Anpassung des Straßenverkehrsgesetzes an zukünftige Mobilitätslösungen

Der Paragraph 1 des StVG befasst sich im Wesentlichen mit dem Anwendungsbereich des Straßenverkehrsgesetzes (Quelle: https://www.gesetze-im-internet.de/stvg/_1.html).

Straßenverkehrsgesetz (StVG)

§ 1 Zulassung

(1) Kraftfahrzeuge und ihre Anhänger, die auf öffentlichen Straßen in Betrieb gesetzt werden sollen, müssen von der zuständigen Behörde (Zulassungsbehörde) zum Verkehr zugelassen sein. Die Zulassung erfolgt auf Antrag des Verfügungsberechtigten des Fahrzeugs bei Vorliegen einer Betriebserlaubnis, Einzelgenehmigung oder EG-Typgenehmigung durch Zuteilung eines amtlichen Kennzeichens.

(2) Als Kraftfahrzeuge im Sinne dieses Gesetzes gelten Landfahrzeuge, die durch Maschinenkraft bewegt werden, ohne an Bahngleise gebunden zu sein.