Peter Löw · Roland Pabst · Erwin Petry

Funktionale Sicherheit in der Praxis

Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten

dpunkt.verlag

Peter Löw
Peter.Loew@kuglermaag.com
Roland Pabst
Roland.Pabst@kuglermaag.com
Erwin Petry
Erwin.Petry@kuglermaag.com

Lektorat: Christa Preisendanz
Copy-Editing: Melanie Hasselbring, Kiel
Herstellung: Nadine Thiele
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: Media-Print Informationstechnologie, 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 978-3-89864-570-6

1. Auflage 2010

Ringstraße 19 B
69115 Heidelberg

5 4 3 2 1 0

Vorwort

Während unserer langjährigen Arbeit als Berater für Prozess- und Qualitätsverbesserung im Umfeld von Entwicklungsprojekten haben wir uns in zunehmendem Maße auch mit Fragen zur funktionalen Sicherheit befasst, nachdem in Deutschland mit dem Geräte- und Produktsicherheitsgesetz ein gesetzlicher Rahmen für die Umsetzung von Sicherheitsanforderungen geschaffen worden war. Häufig ging es um eine Interpretation der Anforderungen der Sicherheitsgrundnorm DIN EN 61508 und die daraus resultierenden zusätzlichen Maßnahmen, die für die Erreichung von Sicherheitszielen notwendig waren. Immer wieder haben wir festgestellt, dass die Forderungen der Grundnorm nicht einfach zu verstehen und direkt umzusetzen waren, sondern im Anwendungskontext interpretiert werden mussten. Die Notwendigkeit der Interpretation liegt im Wesen der Grundnorm, die allgemeingültige Anforderungen sowohl an die Systemarchitektur als auch an die Prozesse stellt und die für die Entwicklung und Installation von Großanlagen, wie beispielsweise Sicherheitseinrichtungen von Kraftwerken, besser geeignet ist als für Serienprodukte, mit denen wir es vor allem zu tun hatten. Allgemeingültige Forderungen der Sicherheitsnorm müssen daher verstanden und in geeignete Maßnahmen für Serienprodukte umgesetzt werden. Die tägliche Arbeit in diesem Umfeld hat uns motiviert, unsere Erfahrungen in einem Buch zu beschreiben, das von Ingenieuren, Qualitätsmanagern und Prozessverbesserern als Interpretationshilfe genutzt werden kann.

Die Einführung der anwendungsspezifischen Sicherheitsnorm ISO/DIS 26262 für Personenkraftwagen, die in englischer Sprache vorliegt, sehen wir als einen weiteren Grund an für die Notwendigkeit einer deutschsprachigen Interpretationshilfe und einer Darstellung von ersten praktischen Erfahrungen mit dieser neuen Sicherheitsnorm, die wir in unserem Buch realisieren wollen.

In unserer Arbeit im Umfeld von Entwicklungsprojekten war es immer wieder notwendig, die Zusammenhänge zwischen den Prozessverbesserungsmaßnahmen nach CMMI oder SPICE und den Anforderungen der Sicherheitsnormen zu erklären. Dabei konnten wir zeigen, wie durch eine konsequente Umsetzung von Prozessverbesserungen auch viele Forderungen der Sicherheitsnormen erfüllt werden können und wie der Zusatzaufwand für die Erreichung von Sicherheitszielen dadurch minimiert werden kann. Auch diese Erkenntnisse haben uns ermutigt, die Zusammenhänge in einem Buch zu beschreiben und den Lesern damit einen Praxisnutzen zu bieten.

Unsere Erfahrungen mit der Umsetzung von Prozessverbesserungen und Sicherheitsanforderungen haben wir bei der Mitarbeit in einer Vielzahl von Software- und Elektronik-Entwicklungsprojekten vor allem bei Automobilherstellern und deren Zulieferern in Europa, USA und Japan gesammelt. Der Gedankenaustausch mit Kollegen in den Projektteams hat uns darin bestärkt, die vielfältigen Anregungen, Sichtweisen und spezifischen Vorgehensweisen für die Leser unseres Buches zu beschreiben.

So ist nun ein Buch entstanden, mit dem wir einerseits dem Leser die notwendigen theoretischen Grundlagen erklären, indem wir die Anforderungen verschiedener Sicherheitsnormen erläutern, und andererseits anhand von Beispielen und Interpretationen, die auf unserer praktischen Erfahrung beruhen, die verschiedenen Aspekte der Umsetzung von Sicherheitsanforderungen in der Praxis darstellen.

An dieser Stelle möchten wir allen danken, die uns während der Entstehungsphase dieses Buches unterstützt haben. Unser Dank gilt vor allem den Kollegen und Geschäftspartnern, die in vielen konstruktiven Diskussionen geholfen haben, die Inhalte des Buches klarer auszuarbeiten. Besonders bedanken wir uns bei Frau Christa Preisendanz vom dpunkt.verlag für die vielen nützlichen Hinweise zum Aufbau und zur Gestaltung des Buches. Bei unseren Familien und Angehörigen bedanken wir uns für das Verständnis und die Geduld angesichts der Einschränkungen, die mit dem Verfassen dieses Buches verbunden waren.

Die Autoren hoffen, dass das Buch den Lesern und Anwendern einen praktischen Nutzen bietet, und würden sich über Rückmeldungen und Verbesserungsvorschläge an folgende Adresse freuen:
functional.safety@dpunkt.de.

Peter Löw, Roland Pabst, Erwin Petry
April 2010

Inhaltsverzeichnis

1 Einleitung

Risiken

Die Themen Sicherheit und Risiko rücken immer dann in den Mittelpunkt des öffentlichen Interesses, wenn durch Fehler in Geräten oder technischen Systemen Menschen zu Schaden gekommen sind. Durch diese Fehler werden mögliche Gefährdungen aufgezeigt, denen jeder einzelne Mensch im Alltagsleben ausgesetzt ist. Unfälle und Gefahren können durch menschliches Versagen ausgelöst werden, aber auch durch technische Defekte in Systemen unterschiedlicher Art, wie Produktionsanlagen, Fahrzeugen oder auch Haushaltsgeräten. Systeme, die nicht vor Missbrauch geschützt sind oder technische Defizite aufweisen, sind nicht sicher und stellen ein erhöhtes Risiko für Personen in ihrem Umfeld dar. Ein Straßenfahrzeug, dessen Bremsen wegen einer fehlerhaften Elektronik versagen, ist unsicher, ebenso wie ein Haushaltsgerät, das den Benutzer durch einen Stromschlag verletzt. Auch bei Schienenfahrzeugen können technische Mängel die Sicherheit beeinträchtigen. So hat die Deutsche Bahn die Neigetechnik zeitweise in allen Zügen abgeschaltet, um einen sicheren Eisenbahnbetrieb zu gewährleisten. Durch einen Konstruktionsfehler könnte es zu einer Überlastung der Achsen und zu konkreten Gefahrensituationen kommen, ließ die Bahn verlauten [Petersen 2009]. Da fragt sich der besorgte Bahnkunde, wie es möglich ist, dass Schienenfahrzeuge mit Sicherheitslücken überhaupt in Betrieb genommen werden und der Konstruktionsfehler erst nach einem Unfall, verursacht durch einen Achsenbruch, erkannt wurde.

Erwartungen

Die Gesellschaft allgemein und insbesondere die Kunden und Nutzer haben verständlicherweise hohe Erwartungen an die Sicherheit von Systemen und die Reduzierung der Risiken. Die Politik hat darauf reagiert und mit dem Geräte- und Produktsicherheitsgesetz (GPSG) einen gesetzlichen Rahmen für die Umsetzung von Sicherheitsanforderungen geschaffen. Auch die Hersteller und Inverkehrbringer von Geräten haben ein großes Interesse an der Vermeidung von Risiken. Sie wollen

sichere Produkte kostengünstig entwickeln und fertigen, Folgekosten durch Unfälle vermeiden und die Kundenzufriedenheit erhalten.

Wachsende Komplexität

Angesichts der wachsenden Komplexität der Systeme werden die Anforderungen an die Entwicklung sicherer Geräte immer anspruchsvoller. Der Anteil der sicherheitsbezogenen, elektronischen Steuerungen und der Software in den Produkten ist in den vergangenen Jahren stark angestiegen, ohne dass ein Ende absehbar ist. In heutigen Kraftfahrzeugen sorgen bis zu 80 elektronische Steuergeräte für Komfort und Sicherheit. Dieser Anteil wird durch die Einführung des Elektroautos in der Zukunft noch weiter ansteigen. »Das Fahrzeug der Zukunft stammt vom Chiphersteller« ist dazu in einem Zeitungsartikel [Magenheim 2009] zu lesen, der sich mit der technologischen Entwicklung bei Elektrofahrzeugen befasst. Auch in anderen Bereichen, wie beispielsweise bei Medizingeräten oder Werkzeugmaschinen, ist immer mehr Elektronik und Software anzutreffen. Vielleicht kommen in der Zukunft auch die Rasenmäher und die Kühlschränke vom Chiphersteller. Die Software in diesen Chips, die zu einem sicheren Betrieb der Geräte beiträgt, muss dann jedoch stabiler und zuverlässiger funktionieren als etwa das Betriebssystem eines heutigen Laptops, das den Betrieb ab und zu durch einen Neustart unterbricht, wenn es meint, überlastet zu sein.

Sicherheitsnormen als Hilfsmittel

Um vor diesem Hintergrund die gesetzlichen Anforderungen an die Sicherheit von Produkten erfüllen zu können, ist die Anwendung von Sicherheitsnormen unumgänglich. Diese beschreiben den Stand der Technik, also das, was von der Mehrzahl der Fachleute als richtig anerkannt wird und sich in der Praxis bewährt hat. Die Anwendung dieser Regeln unterstützt die nachweisbare Erfüllung der Sicherheitsanforderungen. Zusammen mit optimierten Prozessen, die sich an Prozessmodellen wie CMMI oder SPICE orientieren, können die Sicherheitsziele zudem auf effiziente Art und Weise erreicht werden.

Sicherheitsgrundnorm und Serienprodukte

Wir behandeln in diesem Buch die Sicherheitsgrundnorm DIN EN 61508 und weitere wichtige Normen für Serienprodukte (z. B. elektronische Steuergeräte im Automobil), nicht jedoch die Anwendung von Sicherheitsnormen in Großanlagen, wie beispielsweise Raffinerien oder Kraftwerken.

An wen wendet sich dieses Buch

Dieses Buch beschreibt die wesentlichen Anforderungen und Regeln von Sicherheitsnormen für Serienprodukte und erläutert die praktische Anwendung anhand von Beispielen. Es wendet sich insbesondere an

- Ingenieure, die Anforderungen der Sicherheitsnormen (z. B. Anwendung bestimmter Methoden) im Produktlebenszyklus umsetzen müssen,

- Praktiker, die eine Interpretationshilfe bei der Anwendung von Normen zur funktionalen Sicherheit benötigen,
- Produktmanager und Projektleiter, die wissen wollen, welche Auswirkungen die Sicherheitsnormen in der Praxis haben (z. B. bei der Vertragsprüfung oder im Kunden-Lieferanten-Verhältnis),
- Qualitätsmanager und Prozessverbesserer, die wissen wollen, wie die Anforderungen der Sicherheitsnormen in einer CMMI- oder SPICE-Umgebung umgesetzt werden können.

Aufbau des Buchs

Nach der Einleitung gibt das Buch in Kapitel 2 einen Überblick zur funktionalen Sicherheit. Diese Übersicht erläutert zunächst, was funktionale Sicherheit ist. Anschließend werden der Aufbau und wesentliche Anforderungen der Grundnorm DIN EN 61508 dargestellt. Stellvertretend für Normen für Serienprodukte geben wir eine kurze Einführung in ISO/DIS 26262 für Personenkraftwagen. Es werden die in der Industrie am häufigsten verwendeten Reifegradmodelle CMMI und SPICE vorgestellt, weil diese große Überschneidungen mit den Anforderungen der Sicherheitsnormen haben. Anschließend werden die wesentlichen Querbeziehungen zwischen Gesetzen und Sicherheitsnormen beschrieben.

Es folgen drei Kapitel, in denen die Anforderungen der DIN EN 61508 analog zu den Teilen 1 bis 3 der Norm erläutert werden. Kapitel 3 behandelt allgemeine Anforderungen, Kapitel 4 Anforderungen an die Systemebene und die Elektronik, und Kapitel 5 deckt die gesamte Softwareentwicklung einschließlich der Integration in die Hardware ab.

In Kapitel 6 werden einige spezifische Normen für Serienprodukte erläutert und Unterschiede zur Grundnorm DIN EN 61508 herausgearbeitet. Dabei wird detailliert auf die ISO/DIS 26262 für Personenkraftwagen eingegangen. Auch die Norm DIN EN 62061 für Maschinen wird mit einigem Tiefgang behandelt. Eine Reihe weiterer Normen stellen wir nur kurz vor und erläutern wesentliche Unterschiede zu anderen Normen: ISO/DIS 25119 für land- und forstwirtschaftliche Maschinen, DIN EN 501xx für Bahnanwendungen, Normenreihen [IEC 60601] für Medizingeräte und IEC 60335 für Hausgeräte.

Da die Umsetzung jeder Sicherheitsnorm in Projekten eine Vielzahl von prozessorientierten Themen umfasst, wird auf diesen Aspekt in Kapitel 7 über die Umsetzung in einer SPICE- oder CMMI-Umgebung detailliert eingegangen.

In einem umfangreichen Kapitel 8 wird eine Vielzahl von Beispielen für alle sicherheitsbezogenen Aktivitäten über die gesamte Entwicklungszeit beschrieben. Kapitel 9 gibt Hinweise und Beispiele zum Einsatz von Softwarewerkzeugen über den gesamten Entwicklungs-

prozess. Das Buch schließt mit einer Zusammenfassung, einem Abkürzungsverzeichnis, Glossar, Literaturverzeichnis und Index ab.

Wie wird das Buch gelesen

Zunächst empfiehlt es sich, das Kapitel 2 zu lesen, um ein Grundverständnis für die Thematik der funktionalen Sicherheit zu erlangen. Leser ohne Grundkenntnisse der Sicherheitsnormen sollten sich dann mit den Anforderungen der DIN EN 61508 in den Kapiteln 3 bis 5 befassen, um sich detailliert in die funktionale Sicherheit einzuarbeiten. Dabei ist es nützlich, zu den behandelten Themen zur Veranschaulichung immer wieder in die zugehörigen Praxisbeispiele in Kapitel 8 zu schauen. Wer die Grundnorm DIN EN 61508 bereits kennt, kann sich auch direkt mit einer für ihn relevanten, bereichsspezifischen Norm aus Kapitel 6 befassen. Wenn am Ende von Kapitel 6 ausreichend fundierte Kenntnisse über die Anforderungen der Sicherheitsnormen vorhanden sind, empfiehlt sich die Lektüre von Kapitel 7 über die Umsetzung in einer SPICE- oder CMMI-Umgebung. Projektleiter, Qualitätsmanager und Prozessverbesserer erhalten hier Informationen zur Vorbereitung und Begleitung der Planung und Durchführung sicherheitsbezogener Projekte. Leser, die sich für ihre Praxis vor allem für Beispiele interessieren, können die Lektüre auch direkt in Kapitel 8 beginnen.

Praxisrelevante Hinweise

Dies ist ein Buch für Praktiker, die mit der Entwicklung von sicherheitsbezogenen Produkten für Endverbraucher zu tun haben. Es werden daher die Erläuterungen zu den verschiedenen Normen mit praxisrelevanten Hinweisen angereichert, und in vielen Kapiteln findet sich eine Vielzahl von Praxisbeispielen aus allen Phasen der Produktentwicklung.

Es sei darauf hingewiesen, dass die Lektüre dieses Buchs nicht den konkreten Einsatz der jeweils relevanten Sicherheitsnorm ersetzt. Das Buch erhebt nicht den Anspruch, Norminhalte vollständig wiederzugeben. Es hilft aber, einen schnellen Einstieg in die behandelten Sicherheitsnormen zu finden. Und vor allem hilft es dabei, diese zu interpretieren. Die Normen stellen viele Forderungen, die die Entwicklung und das Produkt verteuern können. Es kommt bei der Anwendung der Normen daher darauf an, diese Forderungen angemessen umzusetzen. Dies gelingt aber eigenständig nur dem, der bereits viel Erfahrung besitzt. Dieses Buch hilft durch seine Hinweise zur Umsetzung, durch seine Praxisbeispiele und durch Praxistipps bei einer angemessenen Interpretation.

2.2 Normen zur funktionalen Sicherheit

In den folgenden Abschnitten geben wir einen Überblick zum Aufbau und zu den grundsätzlichen Anforderungen der Grundnorm DIN EN 61508 sowie der abgeleiteten Norm ISO/DIS 26262-Personenkraftwagen und anderen bereichsspezifischen Normen wie DIN EN 62061-Maschinen.

2.2.1 Grundnorm DIN EN 61508: Funktionale Sicherheit

Die internationale Norm IEC 61508 [IEC 61508] wurde im Jahr 2001 als deutsche Norm DIN EN 61508 *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme* übernommen. In diesem Buch beziehen sich die Beschreibungen und spezifischen Erläuterungen zur funktionalen Sicherheit auf die Teile und Kapitel der deutschen Version. Bei Vergleichen mit anderen internationalen Normen oder Prozessmodellen wird auch direkt Bezug auf die Grundnorm [IEC 61508] genommen. Der Nachfolger der IEC und DIN EN 61508, die Edition 2.0, befindet sich in der Entwicklung. In einigen Fällen wird daher auch auf die Neuerungen im Entwurf für diese neue Ausgabe [DIN EN 61508 Ed2] Bezug genommen.

Internationale Norm IEC 61508

Die internationale Norm IEC 61508 definiert als Grundnorm (auch Typ-A-Norm genannt) die allgemeingültigen Anforderungen zur funktionalen Sicherheit. Bereichsspezifische Normen wurden aus dieser Grundnorm abgeleitet (siehe Abb. 2–2). Diese bereichsspezifischen Normen werden auch als Typ-B- oder Typ-C-Norm bezeichnet.

Entsprechende deutsche Norm DIN EN 61508

Auch die deutsche Norm DIN EN 61508 ist als Grundnorm (Typ-A-Norm) anzusehen und ist wie die internationale Norm in sieben Teile gegliedert:

1. [DIN EN 61508-1] Allgemeine Anforderungen
2. [DIN EN 61508-2] Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische (E/E/PE) Systeme
3. [DIN EN 61508-3] Anforderungen an Software
4. [DIN EN 61508-4] Begriffe und Abkürzungen
5. [DIN EN 61508-5] Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität
6. [DIN EN 61508-6] Anwendungsrichtlinie für Teil 2 und Teil 3
7. [DIN EN 61508-7] Anwendungshinweise über Verfahren und Maßnahmen

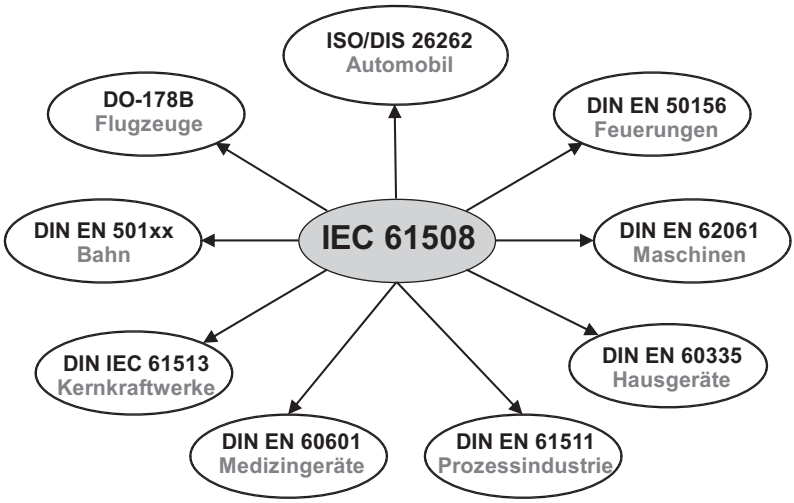


Abb. 2–2
Grundnorm IEC 61508 und einige abgeleitete Normen

Sicherheitsziel

Die Norm stellt Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme mit der Zielsetzung, definierte Sicherheitsziele zu erreichen, indem das vom System ausgehende Risiko auf ein tolerierbares Restrisiko vermindert wird.

Vorgehensweise zur Risikominderung

Die grundsätzliche Vorgehensweise zur Risikominderung besteht darin, gefährliche Ausfälle des Systems zu vermeiden oder zu beherrschen. Derartige Ausfälle können durch systematische Fehler oder durch zufällige Hardwareausfälle verursacht werden.

Systematische Fehler

Systematische Fehler sind Fehler, die aufgrund menschlichen Versagens in den verschiedenen Stadien des Lebenszyklus entstehen. Dazu zählen Spezifikationsfehler, Entwurfsfehler, Implementierungsfehler und Installations- oder Bedienungsfehler.

Zufällige Hardwareausfälle

Zufällige Hardwareausfälle sind das Ergebnis der begrenzten Zuverlässigkeit von Hardwarebauteilen.

Vor diesem Hintergrund stellt die Norm die folgenden Anforderungen an eine systematische Vorgehensweise zur nachweislichen Erreichung der Sicherheitsziele:

Systematische Vorgehensweise

- Durchführung einer Risikoanalyse und Spezifikation der Sicherheitsanforderungen, d.h. der erforderlichen Risikominderung
- Management der Aktivitäten im Sicherheitslebenszyklus zur Sicherstellung einer vollständigen und nachweisbaren Umsetzung der Sicherheitsanforderungen
- Entwurf der Hardware- und der Softwarearchitektur nach vorgegebenen Prinzipien zur Vermeidung oder Beherrschung von Fehlern (z.B. durch fehlertolerante mehrkanalige Systeme zur Beherrschung von zufälligen Hardwareausfällen)

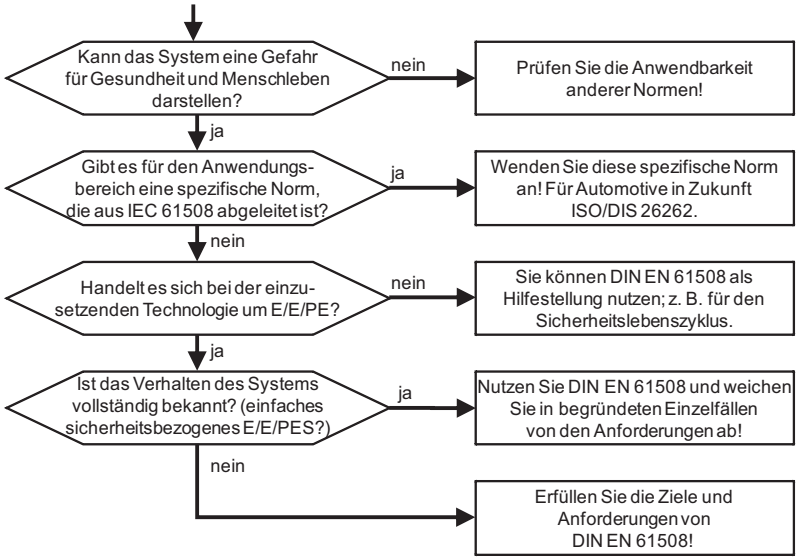
- Planbare und nachvollziehbare Umsetzung über definierte Prozesse (z.B. für Projektmanagement, Konfigurationsmanagement, Entwurf, Test etc.)
- Anwendung von bestimmten Techniken und Maßnahmen zur Vermeidung oder Erkennung von systematischen Fehlern (z.B. Entwurfsmethoden, Testverfahren)

Anwendung bereichsspezifischer Normen

Die abgeleiteten bereichsspezifischen Normen folgen grundsätzlich dieser Vorgehensweise, die von der Grundnorm vorgegeben wird. Ob in einem gegebenen Fall die Grundnorm oder eine bereichsspezifische Norm anzuwenden ist, muss rechtzeitig vor dem Projektstart ermittelt werden (siehe Abb. 2–3).

Es ist zu empfehlen, wenn möglich die bereichsspezifischen Normen einzusetzen, da dadurch kein, oder zumindest weniger Aufwand für Interpretation und Anpassung der Grundnorm an die spezifischen Anforderungen eines Projekts entsteht. So schreibt die Grundnorm keine bestimmte Methode für die Gefährdungs- und Risikoanalyse vor, sondern gibt nur allgemeine Kriterien und Beispiele, die spezifisch angepasst werden müssen.

Abb. 2–3
Anwendbarkeit der Grundnorm DIN EN 61508



2.2.2 ISO/DIS 26262: Personenkraftwagen (PKW)

Die ISO/DIS 26262 »Road vehicles – Functional Safety« ist die Norm zur funktionalen Sicherheit von elektrisch-elektronischen Systemen in Personenkraftwagen (PKW). Sie ist die Anpassung der Grundnorm