Funktionale Sicherheit in Serienprodukten

In Serie

Peter Löw, Roland Pabst, Erwin Petry

In technischen Anlagen, Autos und medizinischen Geräten arbeiten zahlreiche Steuergeräte. Sie müssen zuverlässig funktionieren, denn Ausfälle oder Fehlfunktionen der elektronischen Helfer können Menschen gefährden. Die nagelneue Norm ISO 26262 für die Automobilbranche arbeitet auf Basis der Grundnorm IEC 61508 und kümmert sich um die speziellen Bedingungen in Fahrzeugen.

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 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 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. Da fragt sich der besorgte Kunde, wie es möglich ist, dass Schienenfahrzeuge mit Sicherheitslücken überhaupt in Betrieb gehen und der Konstruktionsfehler erst nach einem Unfall, verursacht durch einen Achsenbruch, erkannt wurde.

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.

Immer mehr elektronische Helfer

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 in einem Artikel der Stuttgarter Zeitung vom 17. Oktober 2009 zu lesen, der sich mit der technologischen Entwicklung bei Elektrofahrzeugen befasst. Auch in anderen Bereichen, beispielsweise in 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.

Um vor diesem Hintergrund die gesetzlichen Anforderungen an die Sicherheit von Produkten erfüllen zu können,

ist die Anwendung von Sicherheitsnormen unumgänglich. Sie 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 (Capability Maturity Model Integration) oder SPICE (Software-Process Improvement and Capability Determination) orientieren, können die Sicherheitsziele zudem auf effiziente Art und Weise erreicht werden.

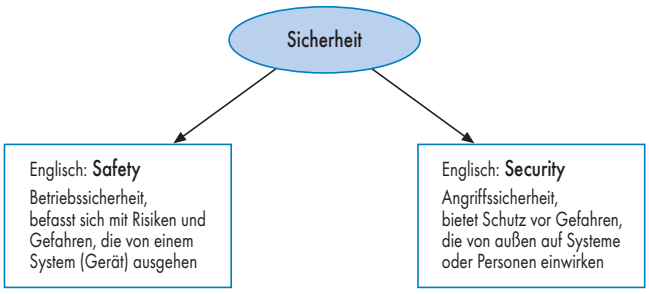
Der Begriff Sicherheit hat eine Vielzahl unterschiedlicher Bedeutungen. Das aus dem Lateinischen entlehnte Wort wurde ursprünglich in der Rechtsprechung im Sinne von „frei von Schuld oder Pflichten“ verwendet. Im heutigen Sprachgebrauch wird Sicherheit meist in der Bedeutung von „Sichersein vor Gefahr oder Schaden“ oder „Freisein von Fehlern oder Irrtümern“ gebraucht. Ein Pfand, das für einen Kredit hinterlegt wird, bezeichnet man ebenfalls als Sicherheit. Das Wort ist auch in einer Vielzahl von Zusammensetzungen wie Fahrsicherheit, Flugsicherheit oder Treffsicherheit zu finden. Im Alltagsleben hat man es mit einer Reihe unterschiedlicher Aspekte der Sicherheit zu tun, wie öffentlicher Sicherheit, wirtschaftlicher Sicherheit oder technischer Sicherheit. Die technische Sicherheit von Systemen, mit der wir uns hier beschäftigen, umfasst die beiden Aspekte Betriebssicherheit und Angriffssicherheit (Abbildung 1).

Freiheit von unvertretbaren Risiken

Die Sicherheitsnorm DIN EN 61508 definiert Sicherheit im Sinne von Betriebssicherheit als „Freiheit von unvertretbaren Risiken“. Funktionale Sicherheit ist derjenige Teil der Gesamtsicherheit, der von der korrekten Funktion des sicherheitsbezogenen Systems abhängt. Die Türsteuerung eines Schienenfahrzeugs oder Autobusses ist ein solches System, das die funktionale Sicherheit beeinträchtigt, wenn es nicht korrekt funktioniert. Öffnet sich die Tür unbeabsichtigt während der Fahrt, so ist das eine Gefahr für die Passagiere.

Es kann durchaus Überschneidungen zwischen Betriebs- und Angriffssicherheit geben, etwa wenn bei mangelnder Angriffssicherheit durch Missbrauch oder Manipulationen ein System in einen gefährlichen Zustand versetzt werden kann. Solche Gefahren sind auch im Sinne der Betriebssicherheit zu verhindern.

Die Sicherheitsnormen zielen darauf ab, die von Systemen ausgehenden Gefahren und Risiken auf ein vertretbares oder tolerierbares Maß zu senken. Es wird immer ein Restrisiko vorhanden sein, das jedoch von der Gesellschaft akzeptiert werden kann, solange es geringer ist als bereits vorhandene Risiken, denen man täglich, etwa bei der Fahrt zur Arbeit oder in der Freizeit, ausgesetzt ist.



Zwei Seiten der Medaille: Betriebssicherheit und Angriffssicherheit (Abb. 1)

Im Folgenden geben wir einen Überblick zum Aufbau und zu den grundsätzlichen Anforderungen der Grundnorm DIN EN 61508 sowie der abgeleiteten Norm ISO/DIS 26262-Personenkraftwagen.

Die internationale Norm IEC 61508 wurde im Jahr 2001 als deutsche Norm DIN EN 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme übernommen. Sie definiert als Grundnorm (auch Typ-A-Norm genannt) die allgemeingültigen Anforderungen zur funktionalen Sicherheit. Bereichsspezifische Normen wurden aus dieser Grundnorm abgeleitet (Abbildung 2). Diese bereichsspezifischen Normen werden auch als Typ-B- oder Typ-C-Norm bezeichnet.

Grundnorm 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

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.

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

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:

- Durchführung einer Risikoanalyse und Spezifikation der Sicherheitsanforderungen, das heißt 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 (zum Beispiel durch fehlertolerante

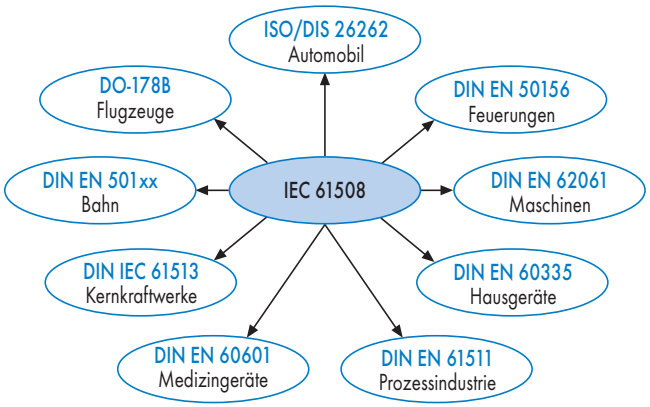
mehrkanalige Systeme zur Beherrschung von zufälligen Hardwareausfällen)
- planbare und nachvollziehbare Umsetzung über definierte Prozesse (zum Beispiel für Projektmanagement, Konfigurationsmanagement, Entwurf, Test et cetera)
- Anwendung von bestimmten Techniken und Maßnahmen zur Vermeidung oder Erkennung von systematischen Fehlern (zum Beispiel Entwurfsmethoden, Testverfahren)

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 (Abbildung 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.

ISO 26262: Stand der Technik

Die ISO/DIS 26262 „Road Vehicles – Functional Safety“ ist die Norm zur funktionalen Sicherheit von elektrisch-elektronischen Systemen in Personenkraftwagen (Pkw). Sie ist die



Aus der Grundnorm IEC 61508 leiten sich etliche andere Normen ab (Abb. 2).

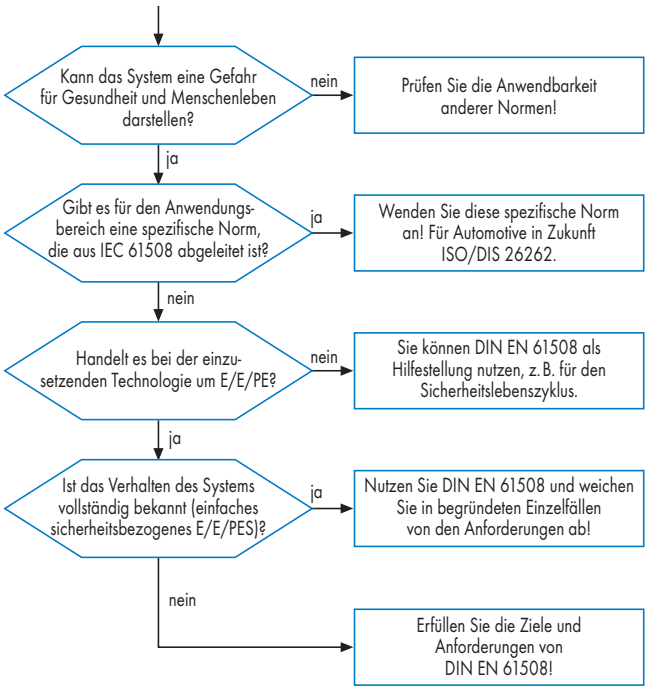
Anpassung der Grundnorm IEC 61508 für Pkw. Diese Norm erfüllt die Kriterien an eine anwendungsspezifische Norm (DIN EN 61508-1, Abschnitt 4.3) und wird daher für ihr Anwendungsgebiet die IEC 61508 als Stand der Technik ab Frühjahr 2011 ersetzen.

Spätestens mit der Publizierung von ISO 26262, voraussichtlich im Juni 2011, ist die Norm als Stand der Technik anzusehen und damit relevant in Produkthaftungsfällen. Es stellt sich nun für die Hersteller die Frage, welche Fahrzeuge bereits nach dieser Norm entwickelt werden müssen. Muss die Norm erst ab der Publizierung im Entwicklungsprozess beachtet werden, und wird sie somit erst auf Fahrzeugmodelle wirken, die Jahre später auf den Markt kommen? Es wäre überraschend, wenn sich ein Gericht einer solchen Argumentation anschließen würde.

Viel nahe liegender ist es anzunehmen, dass die Anwendung der Norm als Stand der Technik für alle Fahrzeuge erwartet wird, die ihren Produktionsstart (Start of Production, SOP) nach der Publizierung oder gar bereits nach dem FDIS (Final Draft International Standard) haben. Dies hat weitreichende Konsequenzen für die gesamte Branche, da eine Fahrzeugentwicklung typischerweise drei Jahre dauert. Die Konsequenz ist, dass bereits in den Jahren vor 2011 nach ISO/DIS 26262 oder den Vorgängerversionen wie ISO/CD 26262 (Committee Draft) gearbeitet wird, um das Produkthaftungsrisiko zu minimieren. In der Praxis kommt daher bis zum Zeitpunkt der Publikation von ISO 26262 in aller Regel eine gemischte Vorgehensweise mit dem heutigen und dem zukünftigen Stand der Technik DIN EN 61508 und ISO/DIS 26262 zum Einsatz. Dies auch schon aus dem einfachen Grund, weil eine derartige Norm weitreichende Konsequenzen auf die Arbeitsweise hat und nicht von einem Tag auf den anderen umgesetzt werden kann.

ISO/DIS 26262 selbst beinhaltet, dass die Norm für alle Systeme nicht anzuwenden ist, die vor dem Publizierungsdatum von ISO 26262 entwickelt wurden. Mit dieser Interpretation wäre eine spätere Anwendung der Norm möglich. Damit dürften die Autoren der Norm aber verkennen, dass der in der Norm beschriebene Stand der Technik in den Firmen bereits vor der Publizierung bekannt ist. Es ist außerdem unklar, wie zum Zeitpunkt der Publizierung von ISO 26262 laufende Projekte zu behandeln sind. Es ist sinnvoll, wenn die Anwender zu dieser Fragestellung den Hausjuristen hinzuziehen und für das Unternehmen eine ausdrückliche Entscheidung fällen, welche Norm worauf angewendet wird.

Da die DIN EN 61508 bereits seit etlichen Jahren Stand der Technik ist, hätten alle in den letzten Jahren entwickelten Produkte danach entwickelt werden müssen. Es ist nicht realistisch, den Sicherheitsnachweis nachträglich zu führen. Wir empfehlen, vorbeugend für eventuelle Haftungsfälle die Betriebsbewährtheit zu dokumentieren.



Vor dem Projektstart sollte man die richtige Norm ermittelt haben (Abb. 3).

ISO/DIS 26262 ist anwendbar auf sicherheitsbezogene Systeme, die ein oder mehrere E/E-Systeme einschließen und die in Serien-Personenkraftwagen mit einem maximalen zulässigen Gesamtgewicht von 3,5 Tonnen installiert werden.

Die Norm versteht unter einem Personenkraftwagen ein Fahrzeug, das vor allem zum Transport von Personen einschließlich ihres Gepäcks und ihrer Waren konstruiert ist und neben dem Fahrer nicht mehr als acht Sitzplätze und keine Stehplätze hat.

Ausdrücklich ausgenommen sind Spezialentwicklungen von E/E-Systemen für Sonderfahrzeuge, wie zum Beispiel Behindertenfahrzeuge. Lastwagen und Busse liegen außerhalb des Anwendungsbereichs, genauso wie Motorräder und landwirtschaftliche Zug- und Arbeitsmaschinen. Für Gefahrguttransporter gelten zusätzliche Anforderungen.

ISO/DIS 26262 behandelt mögliche Gefährdungen, die durch Ausfälle der sicherheitsbezogenen E/E-Systeme bedingt sind. Die Norm ist die Reaktion auf die große Unsicherheit der Automotive-Industrie, wie die in den 1990er-Jahren verabschiedete IEC 61508 für Straßenfahrzeuge zu interpretieren ist. Sie soll die Risiken aus der Produkthaftung kalkulierbarer machen und die Aufwände zur Erzielung funktionaler Sicherheit auf ein sinnvolles Maß beschränken. Weiter soll ein Konsens über die Interpretation von Sicherheit, Risiko und Maßnahmen zur funktionalen Sicherheit in der Automotive-Industrie erzielt werden. Ohne die ISO/DIS 26262 ist der Stand der Technik in der Branche unklar.

Die DIN EN 61508 ist primär unter der impliziten Annahme aufgestellt worden, dass es sich bei ihrer Anwendung um die Entwicklung, Inbetriebnahme und Nutzung einer Anlage (zum Beispiel einer chemischen Anlage) handelt. Straßenfahrzeuge, und speziell Pkw, werden aber nicht nur einmal installiert und dann betrieben, sondern auch in einer sehr viel größeren Stückzahl, zum Beispiel einige hunderttausend Mal. Es ist naheliegend, dass der eigentliche Entwicklungsprozess die redundante Auslegung von Komponenten im Fahrzeug berücksichtigen muss und auch zum Beispiel Sicherheitsprüfungen dadurch eine ganz andere Ausgestaltung erfahren müssen. Man kann nicht jedes einzelne produzierte Fahrzeug einer Sicherheits-Gesamtvalidierung unterziehen. Wie ist also zum Beispiel die Sicherheits-Gesamtvalidierung aus der DIN EN 61508 im Automotive-Kontext zu interpretieren? Die Antwort ist das Produkt-Release in der ISO/DIS 26262, mit dem in die Serienproduktion gegangen wird.

Man kann auch nicht alle Systeme im Fahrzeug doppelt auslegen. Schließlich ist es offensichtlich gesellschaftlich akzeptiert, wie Autos heute konstruiert sind, und offensichtlich ist ein akzeptables Maß an Sicherheit auch ohne massive Redundanz zu erzielen. Ist Redundanz eine Lösung in einer einmal installierten chemischen Anlage, so ist sie keine Standardantwort im Automobil. Das Fahrzeug würde schwerer, teurer, komplizierter, und es ist noch die Frage, ob es sicherer würde. Insofern stand auch der Slogan „Nicht alles, was machbar ist, muss auch gefordert werden“ Pate bei der ISO/DIS 26262.

Eingebettete Systeme mit Sensoren, Steuergeräten und Aktuatoren haben im Fahrzeug in den letzten 15 Jahren eine enorme Bedeutung bekommen. Erstens ist ihre Stückzahl in jedem Fahrzeug stark angestiegen, und zweitens sind sie häufig sicherheitsbezogen. Prominente Beispiele sind Antiblockiersysteme, elektronische Stabilitätsprogramme, Aktivlenkung, Abstandsregeltempomat oder auch die schon älteren Systeme wie Airbag und Fensterheber. In einem gut ausgestatteten Oberklassefahrzeug liegt die Anzahl der Steuergeräte im oberen zweistelligen Bereich. Entwicklung und Test sol-

cher Systeme sind in der DIN EN 61508 nicht angemessen berücksichtigt, weshalb die ISO/DIS 26262 benötigt wird.

DIN EN 61508 geht vom Modell der Anlage (Equipment Under Control, EUC) mit einem separaten Steuerungs- und Kontrollsystem aus. Dabei sind Sicherheitsfunktionen entweder im Steuerungssystem integriert oder separat umgesetzt. Dagegen hängt die Sicherheit des Fahrzeugs von der korrekten Arbeitsweise des elektronischen Systems selbst ab. Die Trennung zwischen elektronischem System und Sicherheitsfunktion ist im Automobil so nicht gegeben. ISO/DIS 26262 greift diese Realität auf und beschreibt die Anforderungen für diesen Kontext verständlich. Die ISO/DIS 26262 spricht daher auch konsequenterweise nicht von „Equipment Under Control" (EUC) und „EUC-Leit- und Steuerungssystem". ISO/DIS 26262 wird auf die „Betrachtungseinheit" (Item) angewendet. Die Betrachtungseinheit wiederum ist eine Menge von Systemen, ein einzelnes System oder eine oder mehrere Funktionen.

Ein hohes Maß an Arbeitsteilung und Zusammenarbeit in einer Entwicklungspartnerschaft kennzeichnet die Entwicklung neuer Fahrzeugmodelle durch einen Automobilhersteller und seine Lieferanten. Da die DIN EN 61508 für diese Konstellation keine Hilfestellung bietet, wurden in der ISO/DIS 26262 diese Anforderungen aufgegriffen.

Eine Gefährdungs- und Risikoanalyse nach DIN EN 61508 führt bei Straßenfahrzeugen häufig zu einem Sicherheits-Integritätslevel (SIL) zwischen 2 und 3, mit viel Bewertungsspielraum für die beteiligten Personen, je nach Interessenlage. SIL 2 oder SIL 3 macht für eine Entwicklung aber einen großen Unterschied. Es ist daher eine wichtige Zielsetzung für die ISO/DIS 26262, diese Unsicherheit zu beseitigen. ISO/DIS 26262 hat deshalb eine andere Abstufung für die Integritätslevel eingeführt. Es sind dies die Automotive-Sicherheits-Integritätslevel (Automotive Safety Integrity Level, kurz ASIL) A, B, C und D.

ASIL A ist die niedrigste und ASIL D die höchste Stufe der Sicherheitsintegrität. Dabei ist es Zielsetzung, dass ein ASIL C genau das geschilderte Problem löst und „zwischen SIL 2 und 3 liegt" (siehe Tabelle „Gegenüberstellung von SIL und ASIL" für eine Darstellung, wie sich SIL und ASIL in etwa entsprechen). SIL 4 der DIN EN 61508 ist solchen Gefährdungen vorbehalten, die eine Katastrophe mit vielen Toten auslösen können. Bei Personenkraftwagen geht man davon aus, dass sie solche Katastrophen nicht auslösen können. Insofern entspricht die höchste Stufe ASIL D von ISO/DIS 26262 in etwa SIL 3 von DIN EN 61508.

Mit der DIN EN 61508 gab es das große Problem, dass kein Beispiel für eine passende Art der Gefährdungs- und Risikoanalyse für die Automotive-Branche gegeben war. Die ISO/DIS 26262 löst dieses Problem und gibt eine Methode mit Beispielen vor.

Sicherheit wird in der DIN EN 61508 wesentlich durch die Begrenzung der Hardwareausfallraten erzielt. Nun gibt es damit bei Fahrzeugen das praktische Problem, dass diese, einmal ausgeliefert, nicht mehr der Kontrolle des Herstellers unterliegen und somit kein systematischer Rückfluss von ausgefallenen Hardwareteilen möglich ist. Zufällige Hardwareausfälle sind im Detail nicht bekannt und können nicht systematisch analysiert werden. Die ISO/DIS 26262 geht daher anstelle eines eher quantitativen Wegs einen stärker qualitativ orientierten Weg. Sie hebt mit ihren Anforderungen viel stärker auf die Vermeidung systematischer Fehler im gesamten Entwicklungsprozess ab. Es geht stärker um die Vermeidung von Fehlern in der Spezifikation der Anforderungen, im Design, in der Konstruktion der Hardware und der Implementierung der Software und in der Integration und den Tests. Für jede Phase des Lebenszyklus enthält die ISO/DIS 26262 eine Tabelle mit Methoden die, bezogen auf den jeweiligen ASIL, einzusetzen sind.

Gegenüberstellung von SIL und ASIL

DIN EN 61508 Safety Integrity Level	ISO/DIS 26262 Automotive Safety Integrity Level	Anmerkungen
	QM	
SIL 1	ASIL A	
SIL 2	ASIL B	
–	ASIL C	Entwurfsanforderungen in etwa SIL 2; Verifikationsanforderungen in etwa SIL 3
SIL 3	ASIL D	ein ASIL-D-System ist ein SIL-3-System, nicht aber umgekehrt
SIL 4		in Automotive keine elektronischen Systeme mit SIL-4-Anforderungen

Dies ist nur eine Leitlinie. Dennoch müssen die ASIL-x-Anforderungen erfüllt sein, wenn ein als SIL y entwickeltes System in einer ASIL-x-Anwendung eingesetzt werden soll, und umgekehrt.

Norm mit Lebenszyklus

ISO/DIS 26262 hat ein Lebenszyklusmodell, das genau zu den wesentlichen Phasen einer Fahrzeuggeneration passt, und damit das Problem des unpassenden Modells der DIN EN 61508 löst. Es besteht auf oberster Ebene aus der Konzeptphase, der Serienentwicklungsphase und der Produktions- und Betriebsphase nach dem SOP. Das Modell der DIN EN 61508 dagegen geht davon aus, dass ein System einmal installiert und in Betrieb genommen und anschließend einer Sicherheits-Gesamtvalidierung unterzogen wird, um dann betrieben zu werden.

Dem Lebenszyklusmodell der ISO/DIS 26262 liegt das V-Modell zugrunde, das in der Branche weitverbreitet ist. Auf der linken Seite des Vs werden Anforderungen spezifiziert und ein Design entwickelt. Am unteren Scheitelpunkt wird implementiert. Auf der rechten Seite des Vs wird integriert, getestet, validiert und die funktionale Sicherheit beurteilt. Es wird zwischen der Systemebene und den darunter liegenden Ebenen für die Hardware- und für die Softwareentwicklung unterschieden. Im Gegensatz dazu unterscheidet DIN EN 61508 nur zwischen der Systementwicklung (Teil 2) und der Softwareentwicklung (Teil 3). Die Strukturierung der Anforderungen in der DIN EN 61508 ist nicht so klar auf die Phasen des V-Modells abbildbar. Gleiches trifft auf die Prozesse im Lebenszyklus von Software zu, wie sie in ISO/IEC 12207 beschrieben und weithin anerkannt sind.

Neben der vorgenannten Strukturierung kennt die ISO/DIS 26262 Anforderungen zum Management der funktionalen Sicherheit, zu unterstützenden Prozessen und sicherheitsorientierten Analysen in jeweils eigenen Teilen der Norm. (jd)

Quelle

Der Artikel ist ein überarbeiteter Auszug aus diesem Buch:

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 2010

Webseite des Buches: www.dpunkt.de/buecher/2929.html