Heinsohn, Jana Maria; Kostrzewa, Thorsten; Hieronymus, Martin

Working Paper

Einführung in die ISO 26262 "Functional Safety - Road Vehicles"

Arbeitspapiere der Nordakademie, No. 2011-07

Provided in Cooperation with:
Nordakademie - Hochschule der Wirtschaft, Elmshorn

ARBEITSPAPIERE DER NORDAKADEMIE

ISSN 1860-0360

Nr. 2011-07

Einführung in die ISO 26262 „Functional Safety – Road Vehicles“

Jana Maria Heinsohn, Thorsten Kostrzewa, Martin Hieronymus

Dezember 2011

Eine elektronische Version dieses Arbeitspapiers ist verfügbar unter:
http://www.nordakademie.de/arbeitspapier.html

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT
THEORIE PRAXIS

Köllner Chaussee 11
25337 Elmshorn
http://www.nordakademie.de

Einführung in die ISO 26262

„Functional Safety – Road vehicles“

Arbeitspapier der NORDAKADEMIE

7-2011

erarbeitet von

Jana Maria Heinsohn (W08b)

Thorsten Kostrzewa (W08b)

Martin Hieronymus

Elmshorn, 27. November 2011

Inhaltsverzeichnis

1 Einleitung

In der heutigen Zeit haben viele Menschen das Gefühl, dass alles auf der Welt geregelt ist. Es gibt Standards in jedem Land für nahezu jeden denkbaren Geltungsbereich. Beispielhaft hierfür ist die „Verordnung (EWG) Nr. 1677/88 vom 15. Juni 1988 zur Festsetzung von Qualitätsnormen für Gurken", die im Jahre 2009 außer Kraft gesetzt wurde. Diese Norm regelte u. a. Mindestgewicht, Färbung sowie zugelassene Krümmungsgrade von Gurken und stand als Synonym für eine ausufernde Bürokratie durch die Europäische Union[1].

Des Weiteren gibt es nationale Normen und internationale Normen, die nicht zwangsweise deckend sein müssen. Alleine in Deutschland gibt es daher weit mehr als 30.000 DIN-Normen, die es zu berücksichtigen gilt, mit steigender Tendenz[2].

Jeden Tag beschäftigen sich daher Mitarbeiter von Unternehmen, Experten aus den jeweiligen Fachgebieten und Hochschuldozenten damit, für einen Bereich einen allgemeingültigen Standard festzulegen oder auch umzusetzen. Dieser Prozess benötigt in der Regel Jahre, bis er abgeschlossen ist. Schwieriger und weitereichender wird es bei internationalen Normen. Dort müssen die jeweiligen Länder sich abstimmen und können die Norm mitgestalten, sodass manche Normen sogar 100 Mannjahre benötigten bis sie fertig verabschiedet worden sind.

Auf Basis der dargestellten Fakten ist es schwer vorstellbar, dass es gerade in Deutschland, dem Land der Automobilindustrie, keine eigene Norm für sicherheitsrelevante Komponenten in Automobilen gibt. Doch genau dieser Zustand einer fehlenden Norm wurde erst im Jahr 2011 beseitigt. Bis dahin wurde ein vergleichbarer Standard aus dem Maschinenbau beziehungsweise Anlagenbau genutzt und für die Automobilindustrie angewendet. Mit Einführung der ISO 26262 Mitte 2011 wurde eine eigene international gültige Norm für die Automobilindustrie geschaffen. Der offizielle englische Titel dieser Norm lautet „Functional Safety – Road vehicles“[3].

[1] Vgl. Bruckner, Regina (2010)
[2] Vgl. DIN Deutsches Institut für Normung e. V. (2005)
[3] Vgl. Sauler, Jürgen (2011), S. 489

2 Problemstellung und Zielsetzung

Die Problemstellung dieses Arbeitspapiers mit dem Titel „Einführung in die ISO 26262“ umfasst die Betrachtung der Neueinführung einer international gültigen Norm für die Automobilbranche für sicherheitsrelevante Komponenten.

Da zuvor die benannte Norm aus dem Maschinenbau in diesem Bereich angewendet wurde, die jedoch aufgrund der verschiedenen Branchen, in denen sie eingesetzt wurde, nicht praxistauglich war, sollen in diesem Arbeitspapier Hintergründe zu der internationalen ISO-Norm aufgezeigt werden. Dafür wird die ISO 26262 inhaltlich vorgestellt und wichtige Elemente näher betrachtet. Anhand von einem ausgewählten Beispiel soll des Weiteren verdeutlicht werden, wie bei der Entwicklung sicherheitsrelevanter Komponenten derzeit die neue ISO-Norm umgesetzt wird.

3 ISO 26262

Der Vorgänger der im Jahr 2011 erschienenen ISO 26262 ist die IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme", die ihren Ursprung im Jahr 1998 hat.

Beide Normen beschäftigen sich mit der Entwicklung von elektrischen, elektronischen und programmierbaren elektronischen Systemen, die eine Sicherheitsfunktion ausführen. Die IEC-Norm wurde seit der ersten Veröffentlichung regelmäßig aktualisiert und war für mehrere Branchen gültig, wie zum Beispiel im Anlagenbau und in der Automobilindustrie.

Ursprünglich wurde die IEC 61508 jedoch nur für den Maschinenbau entwickelt. Die Unterschiede in der Praxis von der heutigen Automobilindustrie zum Maschinenbau sind jedoch eklatant. Zum Beispiel wird im Maschinenbau eine Validierung der Funktionen erst bei Fertigstellung der Maschine durchgeführt. Dieses stellt in der Regel keine Schwierigkeiten dar, da es sich meist um Einzelanfertigungen für einen Kunden handelt. Beispielhaft hierfür sind die Konstruktion und Fertigung eines Hochofens oder eines Atomkraftwerks zu nennen. In der Automobilindustrie ist dieses Vorgehen der Validierung bei Fertigstellung schwierig, da es sich beim Auto um ein Massenprodukt für Konsumenten handelt. Hieraus folgt, dass eine Validierung nicht erst geschehen sollte, wenn bereits mehrere tausend Fahrzeuge produziert worden sind.

Daher hat BMW, aus den vorher genannten Gründen, im Jahre 2002 als Initiator eine eigenständige Norm für die Automobilindustrie gefordert. Im Jahr 2005 hat

die internationale Organisation für Normung (ISO) die Arbeit an dieser Norm übernommen, sodass eine weltweit einheitliche ISO-Norm im Jahr 2011 veröffentlicht wurde[4].

3.1 Anwendungsbereich

Wie in dem vorherigen Abschnitt beschrieben handelt es sich bei der ISO-Norm um eine speziell für die Automobilindustrie entwickelte Norm für PKW bis 3500 kg. Daher ist der Anwendungsbereich vielfältig und muss von jedem Lieferanten, der eine sicherheitsrelevante Komponente herstellt, nach der Veröffentlichung umgesetzt werden. In der Norm wurden spezielle Interessen der Automobilindustrie berücksichtigt, wie zum Beispiel:

- der typische Lebenszyklus eines Personenkraftfahrzeuges mit dessen Verifizierungen bzw. Validierungen.
- die Zuweisung der Sicherheitsverantwortung bei verteilter Entwicklung über mehrere Zulieferebenen.
- die Möglichkeit des Einsatzes von konfigurierbarer Software, deren Verhalten eventuell erst nach dem Serienstart durch Kalibrierdaten bestimmt wird.

Infolge der Diskussion um die Entwicklung und Einführung der neuen ISO-Norm 26262 sollten die Hersteller sicherheitsrelevanter Komponenten seit 2009 damit beginnen, neue Produkte nach der ISO 26262 zu entwickeln. Diese vorgezogene Anwendung der Norm hat den Sinn, im Falle eines Rechtsstreites durch die Beweislastumkehr argumentieren zu können, dass das Produkt normgerecht und damit sicher entwickelt wurde. Spätestens jedoch mit der Einführung Mitte 2011 sollten die Hersteller flächendeckend beginnen, die Norm in ihre Entwicklungsprozesse zu integrieren[5].

[4] Sauler, Jürgen (2011a)
[5] Sauler, Jürgen (2011), S. 489-490

3.2 Aufbau der ISO 26262

Die gesamte ISO-Norm ist in zehn Bände untergliedert. Diese sind in Abbildung 1 dargestellt:

Nr.	Band
1.	Vokabular
2.	Management der funktionalen Sicherheit
3.	Konzeptphase
4.	Produktentwicklung Systemebene
5.	Produktentwicklung Hardwareebene
6.	Produktentwicklung Softwareebene
7.	Produktion, Betrieb und Außerbetriebnahme
8.	Unterstützende Prozesse
9.	ASIL- und sicherheitsorientierte Analysen
10.	Guideline (informativ)

Abbildung 1: Inhaltsverzeichnis[6]

Das erste Band definiert verwendete Begriffe und legt somit eine Basis des verwendeten Vokabulars und seiner Terminologie. Band zwei umfasst die Anforderungen an das Management der funktionalen Sicherheit. Dieses beschreibt die Organisation des Projektmanagements über den gesamten Produktlebenszyklus hinweg und die Absicherungsmaßnahmen zum Nachweis der Normkonformität. Hierdurch werden eine übergeordnete Sichtweise für die Entwicklungsprozesse und Kriterien zur Bewertung dargestellt sowie der Bezug der einzelnen dargestellten Prozesse zueinander. Auf diese Weise soll Unternehmen ein Leitfaden an die Hand gegeben werden, mittels dessen sie sicherheitsrelevante Komponenten und Systeme entwickeln können. Beispielhaft zu nennen für ein vom Standard vorgegebenes Vorgehen ist die Ernennung von Sicherheitsverantwortlichen, die verantwortlich sind für die zeitliche Steuerung und Überwachung der Maßnahmen als eine Art Projektmanager. Des Weiteren werden durch Band zwei umfangreiche Dokumentationspflichten während jedes Entwicklungsschrittes festgehalten[7].

Die Bände Drei bis Sieben sind als übergreifende Einheit zusammenzufassen. Sie definieren den Produktlebenszyklus, beginnend mit der Konzeptphase über die Produktentwicklung auf System-, Hardware- und Softwareebene bis schluss-

[6] Eigene Darstellung, nach Glöe, Jung (2011)
[7] Vgl. FERCHAU Engineering GmbH (2011)

endlich zur Produktion, Betrieb und Außerbetriebnahme. Dabei orientieren sie sich an den Eckpunkten des V-Modells der Softwareentwicklung, das in Kapitel 4.1 „Softwareentwicklungsprozess – V-Modell“ auf Seite 7 dargestellt wird. Die Unterteilung der Bände ergibt sich anhand der einzelnen Abschnitte des Sicherheitslebenszyklus, der in Abbildung 2 dargestellt ist[8].

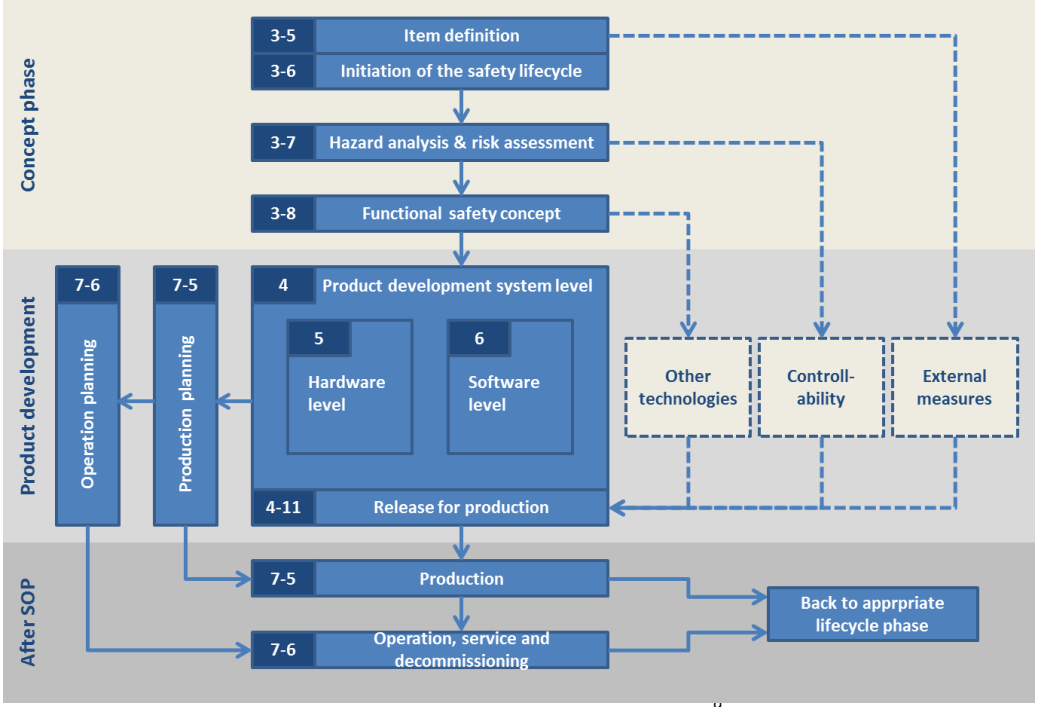

Abbildung 2: Sicherheitslebenszyklus[9]

Die hierbei auftretenden Entwicklungsphasen werden durch die Bände vier bis sechs repräsentiert. Sie sind stets in drei Abschnitte unterteilt. Die erste Phase ist die Planung der Aktivitäten. Im nächsten Schritt werden die geplanten Tätigkeiten durchgeführt, und zuletzt findet eine Verifikation beziehungsweise Validation des entstandenen Produkts statt.

Im dritten Band der ISO 26262 wird auf die Konzeptphase eingegangen. Das bedeutet, dass dieser Abschnitt mit der Definition des Bauteiles beziehungsweise Systems beginnt. Im Folgenden werden eine Gefährdungs- und Risikoanalyse durchgeführt und aus diesen Ergebnissen Sicherheitsziele abgeleitet, denen jeweils ein Automotive Safety Integrity Level (vgl. Kapitel 4.2 „Automotive Safety Integrity Level" auf Seite 8) zugeordnet wird. Entwickler müssen in dieser Phase des Entwicklungsprozesses alle möglichen Fehlfunktionen in ihrer Gesamtheit, die im neu zu entwickelnden Produkt auftreten können, und alle Situationen, in

[8] Vgl. FERCHAU Engineering GmbH (2011)
[9] Eigene Darstellung in Anlehnung an Sauler, Kriso (2011c)

denen ihr Auftreten relevant sein kann, prüfen. Abgeschlossen wird die Konzeptphase mit einem fertigen Sicherheitskonzept[10].

Im vierten Band wird die Systementwicklung beschrieben. Das bedeutet, dass das Sicherheitskonzept, das im vorangehenden Band Drei entwickelt wurde, aufgegriffen und erweitert wird. Nach der ISO-Norm ist das Sicherheitskonzept eine Sicht von außen auf das System. Die Weiterentwicklung, die im Band Vier stattfindet wird technisches Sicherheitskonzept genannt und soll eine Innensicht des Systems darstellen. Somit werden in diesem Band Handhabungen, Arbeitsweisen und zu erreichende Arbeitsergebnisse vorgeschrieben und durch die drei Bemessungsgrundlagen „optional", „recommended" und „highly recommended" klassifiziert.

Aus dem Sicherheitskonzept lassen sich ebenfalls Anforderungen an die Hardware sowie Software festlegen. Analog zu Band Vier wird in Band Fünf die Hardware- und in Band Sechs die Softwareentwicklung beschrieben, das jeweilige technische Sicherheitskonzept festgelegt sowie die Handhabungen, Arbeitsweisen und zu erreichende Arbeitsergebnisse mit ihren Bemessungsgrundlagen vorgeschrieben[11].

Die Anforderungen für die Produktion, den Betrieb, den Service, den Reparaturfall, die Wartung sowieso die Außerbetriebnahme des Systems sind im Band 7 unter dem Aspekt der funktionalen Sicherheit beschrieben. Der Aspekt der Außerbetriebnahme ist in die ISO 26262 aufgenommen worden, um sicherzustellen, dass die Stilllegung beziehungsweise die Entsorgung eines Produktes unter Einhaltung der Sicherheitsaspekte stattfindet und nicht in einem undefinierten Bereich angesiedelt wird. Des Weiteren wird die Vorgehensweise für sicherheitsrelevante Systeme zum Erstellen der benötigten Produktions- und Installationspläne beschrieben.

Im achten Band werden unterstützende Prozesse wie Konfigurations- oder Anforderungsmanagement beschrieben. Des Weiteren werden neue Methoden der Qualifizierung von Tools, Software- oder Hardware-Komponenten dargestellt. Das bedeutet, dass hier die Verantwortungsbereiche der unterschiedlichen Entwicklungsbereiche sowie die anzuwendenden Verfahren bei der Dokumentation beschrieben werden. Des Weiteren werden Verifikationsschritte empfohlen,

[10] Vgl. FERCHAU Engineering GmbH (2011)
[11] Vgl. FERCHAU Engineering GmbH (2011)

durch die eine betrachtete Menge an Risiken, die durch defekte Softwaretools und Compiler verursacht werden könnten, reduziert werden können[12].

Das neunte Band greift das Problem der Automotive Safety Integrity Level (A-SIL)-Einstufung auf und beschreibt die Möglichkeit der Koexistenz von Elementen mit unterschiedlichen ASIL-Einstufungen sowie die übliche Methodik bei der Durchführung solcher Sicherheitsuntersuchungen in Abhängigkeit von der Phase des Produktlebenszyklus. Beispielshaft für Sicherheitsuntersuchungen sind hier die Fehler-Möglichkeits- und Einflussanalyse (FMEA) sowie die Fehlerbaumanalyse (FTA) zu nennen.

Im zehnten Band werden verschiedene Erklärungen zu Begriffen und Konzepten beschrieben. Des Weiteren beinhaltet es Beispiele zu den zuvor vorgestellten Konzepten und Prozessen, damit Unternehmen die ISO 26262 besser umsetzen können. Der Grundgedanke des zehnten Bandes ist es, eine Guideline für die Unternehmen zu bieten. Daher wird in diesem Band eine exemplarische ASIL-Bewertung vorgenommen[13].

[12] Vgl. ebd.
[13] Vgl. FERCHAU Engineering GmbH (2011)

4 Elemente der ISO 2626

Nachdem im vorangegangenen Kapitel die ISO-Norm 26262 mittels ihres Anwendungsbereichs und Aufbaus grundlegend vorgestellt wurde, dient dieses Kapitel der näheren Betrachtung wichtiger in der Norm vorgestellter Aspekte. Daher werden im Folgenden das für die Softwareentwicklung anzuwendende V-Modell, das Automotive Safety Integrity Level sowie die Rückwirkungsfreiheit betrachtet.

4.1 Softwareentwicklungsprozess – V-Modell

Die Softwareentwicklung für sicherheitsrelevante Software wird in der ISO 26262 durch das V-Modell realisiert, welches im Folgenden erläutert wird.

Das V-Modell ist ein Standard zur Entwicklung einer Software. Zudem ist es eine Weiterentwicklung des Wasserfallmodells. Im Englischen steht das V für „Validation“ und „Verification“. In Deutschland ist dieses Modell weit verbreitet als Entwicklungsstandard für die Planung und Durchführung von IT-Systementwicklungsprojekten der öffentlichen Hand. In der Abbildung 3 sind die einzelnen Phasen des V-Modells dargestellt.

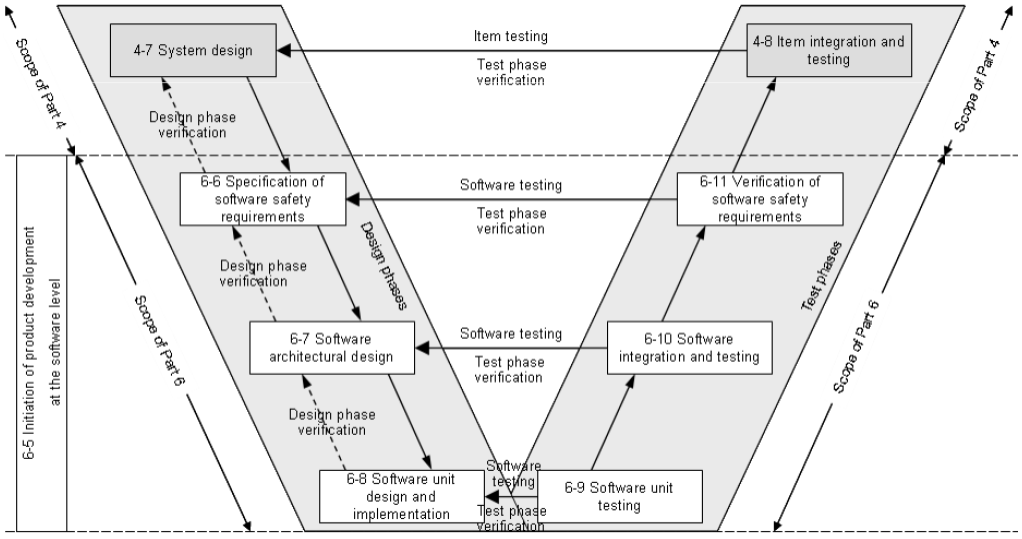

Abbildung 3: Aufbau des V-Modells[14]

Aus der Abbildung lässt sich erkennen, dass sich der Name aus der Form des Modells ableitet. Die linke Seite des V spiegelt die Projektdefinition wieder. Daher werden diese Phasen Spezifizierungsphasen genannt. Die Spezifizierungsphasen beinhalteten die Anforderungsdefinitionen des Systems. Das bedeutet, es muss zunächst ein Konzept mit den jeweiligen Anforderungen an das Produkt erstellt werden. Im nächsten Schritt werden die Vorausetzungen und die Architektur des Produktes in einem Grobentwurf definiert. Sobald dieses festgelegt

[14] Fürst (2010): S. 27

wurde, beginnt die Detaillierung des festgelegten Designs zu einem Feinentwurf, bevor dieser im letzten Schritt umgesetzt wird.

Wie im Wasserfallmodell muss jede Phase abgeschlossen werden, bevor das Projekt in die nächste Phase übergehen kann. Die Erweiterung des Wasserfallmodells ergibt sich aus der rechten Seite des „V“. Dieses sind die Realisierungsphasen. Das bedeutet, dass der Software-Entwurf zunächst einige Testphasen durchlaufen muss, bevor er veröffentlicht werden kann. Wie auf der Gegenseite, den Spezifizierungsphasen, gibt es mehrere Testphasen, die sequentiell durchgeführt werden, bevor das Produkt veröffentlicht wird[15].

4.2 Automotive Safety Integrity Level

Der Automotive Safety Integrity Level (ASIL) ist ein Maß für die Sicherheitsrelevanz eines Bauteils. Eine Fehlfunktion kann in der Regel in jedem Bauteil auftreten. Beispiele für Fehlfunktionen sind etwa das ungewollte Öffnen der Fensterscheiben oder die automatische Auslösung einer Vollbremsung. Diese beiden Beispiele zeigen, dass jede Fehlfunktion unterschiedlich schwerwiegende Konsequenzen haben kann. Zudem hängt die Konsequenz von der jeweiligen Situation zum Eintrittszeitpunkt der Fehlfunktion ab. Aus diesen Beispielen ergibt sich, dass die ASIL-Einstufung essentiell für die Entwicklung und Auslegung einer Produktreihe ist und eine falsche ASIL-Einstufung weitreichende Konsequenzen für den Endkonsumenten haben kann[16].

Die Einstufung ergibt sich zunächst aus drei folgenden Parametern:

- Exposure (E): Beschreibt die Häufigkeit von Situationen, in denen die Fehlfunktion relevant ist.
- Controllability (C): Falls die Fehlfunktion auftritt, gibt dieser Wert an, wie gut sie im Folgenden beherrscht werden kann.
- Severity (S): Im Falle des Auftritts der Fehlfunktion ist dies ein Indikator für die Schwere der Auswirkungen.

In der ISO-Norm 26262 ist gefordert, dass jede der benannten Komponenten eine ASIL-Einstufung erhält. In der Abbildung4 ist die Einstufungstabelle der ISO- Norm 26262 abgebildet, nach der sich die Einstufung ergibt.

[15] Vgl. Bauer, Bernhard (2011), S. 482-483
[16] Sauler, Jürgen (2011), S. 494-495

Risk matrix ISO/DIS 26262-3		C - Controllability		
S - Severity	E - Exposure	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Abbildung 4: Einstufungstabelle[17]

Aus den zugeordneten Werten dieser drei Parameter ergibt sich die ASIL-Einstufung auf einer Skala von A bis D. A spiegelt bei dem ASIL-Level die niedrigste Einstufung wieder und D die höchste. Des Weiteren gibt es das Level QM für nicht sicherheitsrelevante Systeme.

Problematisch an dieser Bewertung ist, dass in der Norm keine konkreten Hinweise gegeben sind, wie die Parameter Exposure, Controllability und Severity zu bestimmen sind, beziehungsweise welche ASIL-Einstufung daraus resultiert. Diese Einschätzung liegt im subjektiven Ermessen des Herstellers. Daher ist es legitim, dass ein Hersteller aus Schleswig-Holstein, beispielhaft für ein Bundesland mit wenigen Gefällen und Anstiegen, den Exposure-Wert für das „Anfahren am Berg“ mit einem geringeren Wert einstufen würde, als möglicherweise ein Hersteller aus Bayern, welches ein Bundesland mit deutlich mehr Anstiegen und Gefällen ist, die bewältigt werden müssen. Basierend auf dieser unterschiedlichen Bewertung, ergibt sich eine gewisse Möglichkeit für Automobilhersteller, Einfluss auf die Automobilsicherheit zu nehmen durch niedrig angesetzte ASIL-Bewertungen und so möglicherweise benötigte Sicherheitsmaßnahmen zu umgehen[18].

[17] In Anlehnung an die Matrix der TÜV SÜD Automotive GmbH beim Automotive Forum Regensburg (14.042010)
[18] Vgl. Sauler, Jürgen (2011), S. 494

4.3 Rückwirkungsfreiheit

Einer der größten zu lösenden Aspekte für Hersteller sicherheitsrelevanter Komponenten ist die in Band Sechs „Produktentwicklung Softwareebene" beschriebene Rückwirkungsfreiheit.

Diese Bestätigung der Rückwirkungsfreiheit ist notwendig, wenn mehrere Softwarekomponenten mit unterschiedlicher ASIL-Einstufung gemeinsam in einem Steuergerät verwendet werden sollen. Es wird dadurch nachgewiesen, bspw. durch den Einsatz von Software-Partitionen, dass die einzelnen Softwarekomponenten sich nicht gegenseitig durch die Nutzung gemeinsamer Ressourcen, wie Speicher oder Laufzeiten, negativ beeinflussen. Im Falle des Nichtvorliegens der Rückwirkungsfreiheit, muss jede Komponente jedoch nach der höchsten ASIL-Einstufung D umgesetzt werden.

Durch die somit vorgeschriebene Rückwirkungsfreiheit wird sichergestellt, dass das System eine gewisse Redundanz besitzt. Hierfür werden in der neuen ISO-Norm 26262 verschiedene Anforderungen an Softwaretests gestellt, durch die mögliche Testvorgänge und auch Methoden zur Ermittlung von zu testenden Situationen definiert werden[19].

[19] Vgl. Sauler; Kriso (2011b)

5 Praktische Anwendung der ISO 26262 anhand einer elektronischen Keilbremse

Im folgenden Abschnitt soll die Umsetzung der ISO 26262 anhand einer elektronischen Keilbremse der Firma Siemens VDO erläutert werden. Sie muss als sicherheitsrelevantes Fahrzeugsystem den Ansprüchen der ISO 26262 während der Entwicklung und des gesamten Produktlebenszyklus genügen, da sie sowohl die normalen Bremsfunktionen wie auch die elektrische Parkbremse im Stillstand steuert. Hierfür wird zunächst die Funktionsweise der elektronischen Keilbremse dargestellt, bevor eine ASIL-Einstufung und das daraus entwickelte elektronische Sicherheitskonzept erläutert werden.

5.1 Funktionsweise

Die elektronische Keilbremse besitzt als elektromechanische, mechatronische Bremse **(**Brake-by-Wire-System) Bremsklötze, die durch schräg gestellte Keile aneinander gekoppelt sind. Ein solches System verwendet keine fluidtechnischen Systeme und verzichtet somit auf jegliche Art von Pneumatik und Hydraulik[20]. In Abbildung5 ist dieser Aufbau in einem 3D-Modell der Keilbremse dargestellt.

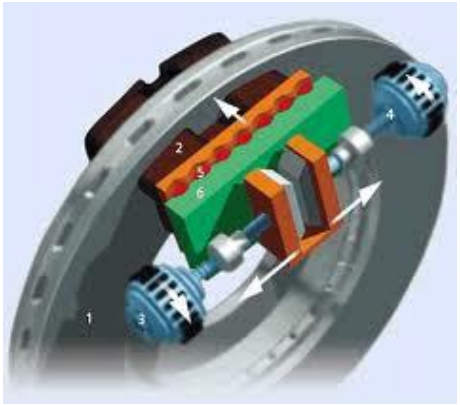

Abbildung 5: Elektronische Keilbremse[21]

Beim Bremsprozess werden durch einen elektrisch angetriebenen Motor die Bremskeile in die Fuge zwischen die geneigten Bremszangen und die rotierende Bremsschreibe geschoben. Dadurch entsteht Reibung, die die benötigte Bremswirkung verstärkt. In dessen Folge sinkt die erforderliche Aktuatorleistung erheblich, die benötigt wird, um die aufzubringende Bremsleistung zu erzeugen, im Vergleich zu herkömmlichen Bremsklötzen. Die Bremskraft bei einer elektronischen Keilbremse kann daher bis zu 60 kN betragen. Herkömmlich verwendete

[20] Vgl. Schaffner (2007): S. 48
[21] Aschenbrenner (2005)

Magnetschienenbremsen bringen im Vergleich hierzu bei 160km/h eine Bremskraft von lediglich 16,4 kN und bei 250 km/h eine Kraft von 14,4 kN auf[22].

Durch diese neue von Siemens VDO entwickelte Technik wurde in Tests auf Eis ein 15 Prozent geringerer Bremsweg gemessen als bei Tests mit herkömmlichen Bremsen. Durch eine Steuerung der Keilposition durch den Elektromotor wird verhindert, dass bei einer Vollbremsung der Bremskeil komplett in den Spalt hineingezogen wird und als Konsequenz das Rad blockiert. Dadurch wird ein Zustand während der Bremsung erreicht, in dem vom Motor statt einer Druckkraft nun eine Zugkraft aufgebracht werden muss und somit die bestmögliche Bremswirkung besteht. Bis zu 1000-mal pro Sekunde wird zu diesem Zeitpunkt die Bremskeilposition verändert, um den ökonomischsten Bremspunkt zu erhalten[23].

5.2 Systemarchitektur und Anforderungen an das Ausfallverhalten

Zu Erreichung der benannten Vorteile und Umsetzung einer elektronischen Keilbremse werden in der Systemarchitektur der elektronischen Keilbremse folgende Komponenten aufeinander abgestimmt und verknüpft: „vier Radeinheiten, ein Bremspedal, der Bedienknopf für die Parkbremse und eine redundante Energieversorgung mit zwei Batterien und zwei Energiemanagement-Einheiten"[24] sowie ein zentrales Steuergerät mit drei Mikrocontrollern, das eine ausreichende Redundanz gewährleistet[25]. Daraus ergibt sich ein Aufbau der Systemarchitektur, der in der folgenden Grafik schematisch und mittels Energie- und Signalflüssen dargestellt wird.

[22] Vgl. Schaffner (2007): S. 48
[23] Vgl. ebd.
[24] ebd.: S. 49
[25] Vgl. ebd.

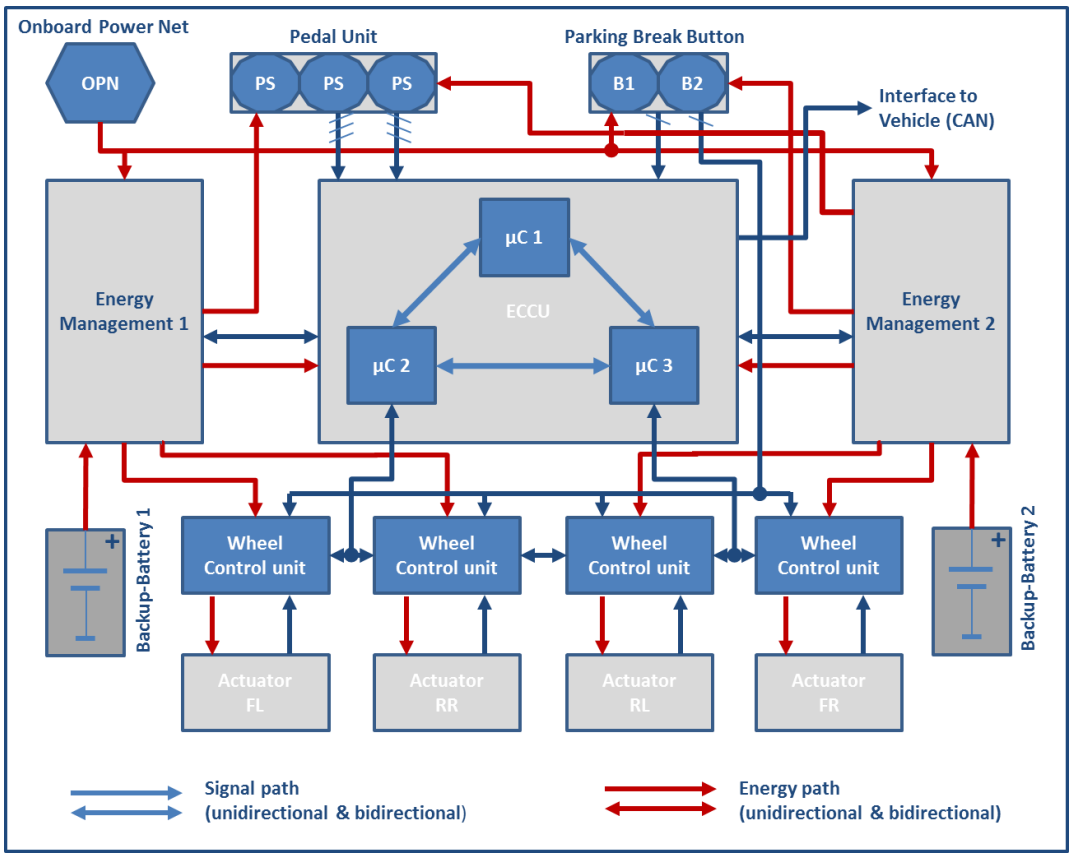

Abbildung 6: Systemarchitektur[26]

Aufgrund dieses Aufbaus ergeben sich bei der von Siemens VDO entwickelten elektronischen Keilbremse sowohl Funktionen, die der Erhaltung der grundständigen Funktionen dienen, z. B. normale Bremsvorgänge, wie auch höhere Funktionen der Keilbremse. In die sogenannten höheren Bremsfunktionen sind die VSC, das ABS sowie die TCS einzustufen. Diese geben dem Fahrer eine zusätzliche Möglichkeit zur Gewinnung und Erhaltung der Kontrolle über sein Fahrzeug, jedoch nehmen sie keinen Einfluss auf die Basisfunktionen der durchschnittlichen Bremsabläufe[27].

Basierend auf dieser Unterscheidung von Basisfunktionen und höheren Bremsfunktionen ergibt sich auch ein zweigeteiltes Konzept, das greift, sobald Störungen auftreten, die die Funktionen beeinträchtigen. Da die Basisbremsfunktionen essentiell für das kontrollierbare Verhalten des Automobils sind, dürfen diese im Falle einer Fehlfunktion, eines Ausfalls oder einer Störung nicht einfach abgeschaltet werden. Stattdessen müssen sie auch in einem dieser Zustände die Kontrollierbarkeit des Autos mittels einer eingeschränkten Funktionalität garantieren und somit die benötigten Bremsleistungen erbringen. Speziell für das Auftreten von Fehlern, die die Basisbremsfunktionen beeinflussen, wurde von Siemens

[26] Schaffner (2007): S. 49
[27] Vgl. ebd.

der sogenannte Fail-Safe-Mechanismus etabliert, der an der Keilbremse wirkt. Im Falle eines Auftretens einer Störung der Basisbremsfunktionen, die u. a. auch zu einem Blockieren der Bremse führen kann, wird das elektromechanische Betriebssystem in einen Zustand versetzt, in dem es ohne Strom arbeiten kann. Hierbei wird automatisch die Bremse wieder geöffnet[28].

Dem gegenüber stehen Ausfälle oder Beeinträchtigungen der höheren Bremsfunktionen. Da diese nicht die Aufgaben der Basisbremsfunktionen übernehmen, sondern stattdessen eine zusätzliche Hilfestellung für den Fahrer zur Kontrolle des Autos bieten, ist ein Fehler hier weniger gravierend. Daher werden die Systeme bei einer Fehlfunktion lediglich in einen sicheren Zustand überführt, in dem sie bis zur Fehlerbehebung verbleiben[29].

5.3 ASIL-Einstufung

Nachdem im vorangegangenen Abschnitt die Funktionsweise einer elektronischen Keilbremse sowie die Anforderungen an das Ausfallverhalten erläutert wurden, soll nun anhand der elektronischen Keilbremse eine ASIL-Einstufung exemplarisch nachvollzogen werden. Diese Einordnung erfolgt anhand der Risikomatrix (vgl. Kapitel 4.2 – Automotive Safety Integrity Level).

Zunächst findet eine Einstufung der Severity statt. In diesem Fall wird dadurch die Schwere der Auswirkung beim nicht beherrschbaren Auftreten einer Fehlfunktion bewertet. Im Falle eines totalen Ausfalls der Bremsanlage ist stets mit den schlimmsten Auswirkungen zu rechnen, daher kann es in diesem Falle nur eine Einstufung des S3 zur Folge haben.

Im nächsten Schritt wird die „Exposure“ bewertet, bzw. die Frage geklärt, wie häufig Situationen auftreten, in denen die Fehlfunktion relevant ist? Da der Bremsvorgang einer der am häufigsten durchgeführten Vorgänge bei dem Führen eines PKWs ist, ist die Fehlfunktion der Bremsen in fast 100 % der Situationen relevant. Daher ergibt sich in diesem Falle eine Einstufung der E4 als höchste „Exposure“-Einstufung. Dieses bestätigt die vorherig getroffene Annahme, dass es sich um ein sicherheitsrelevantes Bauteil handelt, da unabhängig von der Bestimmung der Controllability eine Mindesteinstufung der ASIL B eintritt.

Um der Norm gerecht zu werden, muss jedoch eine vollständige Bestimmung des ASILs durchgeführt werden. Daher ist im folgenden Schritt die Controllability

[28] Vgl. Schaffner (2007): S. 48f.
[29] Vgl. ebd.

zu bestimmen. Diese Bewertung ist ein Indiz für die Beherrschbarkeit der Situation bei Eintritt der Fehlfunktion. Bei der Fehlfunktion einer Bremse gibt es mehrere Möglichkeiten, wann die Bremsfunktion ausfällt. In einem verkehrsberuhigten Bereich oder beim Anlassen des Motors ist die Fehlfunktion mit hoher Wahrscheinlichkeit beherrschbar. Da in solch einem Fall jedoch von dem Worst-Case-Szenario ausgegangen werden muss, sollte in diesem Fall eine C3-Einstufung gewählt werden. Daraus ergibt sich, dass die ASIL-Einstufung in die Kategorie „D“ fällt und somit die höchstmögliche Einstufung ist.

Nachdem ein allgemeines ASIL-Level für die elektronische Keilbremse ermittelt wurde, muss im Folgenden eine dreischrittige detaillierte Analyse einer spezifischen Situation erfolgen sowie für jeden Zustand die Auftrittswahrscheinlichkeit, die anzunehmenden Schäden im Falle eines Ausfalls der Bremsen und die Chancen des Fahrers, die Situation unter Kontrolle zu bringen, bestimmt werden. Basierend hierauf, ermittelt sich dann erneut der ASIL-Wert für jeden möglichen Ausfall der elektronischen Keilbremse. Siemens VDO führte diese Untersuchung zusammen mit einem Automobilhersteller durch, woraus sich neun mögliche Situationen ergaben, in denen die Bremsen versagen könnten, die die höchste ASIL-Einstufung D bekamen[30]. Diese Situationen ließen sich wiederum in die folgenden drei Gruppen eingliedern:

- „unerwartete Bremsvorgänge",
- „ungenügende Bremsleistungen" und
- „Stabilitätsprobleme bei der Fahrdynamik aufgrund eines EWB[31]-Fehlers"[32].

Auf Basis dieser Einteilung der Fehlervorfälle wurde von Siemens VDO ein Sicherheitskonzept entwickelt mit dem Ziel der Reduzierung von in solchen Situationen auftretenden Risiken auf einen akzeptierbaren Umfang. Daher wurden im Vorfeld der Gestaltung des Sicherheitskonzeptes bereits zwei Hauptanforderungen festgelegt.

1. Treten ein oder zwei Fehler während des Betriebs auf, muss eine gestufte Rückfallreaktion des Bremssystems gewährleistet werden.
2. Die Eintrittswahrscheinlichkeit einer Fehlfunktion des Systems muss unterhalb des in der Norm geforderten Grenzwertes liegen[33].

[30] Vgl. Schaffner (2007): S. 51f.
[31] EWB ist die von Siemens VDO benutzte Produktbezeichnung der elektronischen Keibremse
[32] Schaffner (2007): S. 52

5.4 Sicherheitskonzept

Da die elektronische Keilbremse folglich ein Bauteil mit der ASIL-Einstufung D ist, muss sie den höchsten Sicherheitsstandard bedienen, der in der ISO-Norm 26262 vorgesehen ist.

Das bedeutet, dass es möglich sein muss, das Fahrzeug in jeder Situation sicher zum Stillstand abzubremsen. Hierfür bedient sich die elektronische Keilbremse eines mehrstufigen Sicherheitssystems, das mehrere Rückfallebenen implementiert hat. In der Abbildung7 ist das Sicherheitskonzept der elektronischen Keilbremse dargestellt[34].

Verfügbarkeit	Kein Fehler	Der Folgefehler	
		führt zu keiner Gefahrensituation	kann zu einer Gefahrensituation führen
Auto im Stillstand	Das Auto kann gestartet und die Bremsen gelöst werden.	Das Auto kann gestartet und die Bremsen gelöst werden.	Das Auto kann gestartet werden. Die Bremsen lösen sich nicht.
Auto in Bewegung	Das Auto kann mit der Bremskraftunterstützung gebremst werden .	Das Auto kann mit der Bremskraftunterstützung (zweites System) gebremst werden .	Das Auto wird sicher zum Stillstand gebracht (Auto-Stopp).

Abbildung 7: Sicherheitskonzept[35]

Die erste Spalte des dargestellten Sicherheitskonzeptes zeigt die Lösungen an, falls kein Fehler besteht. Hierdurch werden die Möglichkeiten verdeutlicht, die es gibt, um das Fahrzeug während eines fehlerfreien Betriebszustandes zum Stillstand zu bringen, z. B. mittels der normalen Bremsfunktionen und durch die Parkbremse im Stillstand. Interessanter aus der Sicherheitsperspektive sind jedoch der zweite und dritte Teil der Abbildung. Dort wurde festgelegt, wie das Fahrzeug bei einem oder zwei auftretenden Fehlern mittels einer stufenförmigen Rückfallreaktion zum Stillstand gebracht werden kann. Hierdurch wird das Risiko eines gefährlichen Ausfalls mithilfe der Sicherheitsfunktionen auf ein akzeptables ASIL-Level gebracht. Das Sicherheitskonzept wird weiterhin unterteilt in gefährliche, also nicht beherrschbare, und beherrschbare Situationen. In der Regel wird bei Eintritt einer beherrschbaren Situationen versucht, sämtliche Bremsvorgänge sowie die Funktion der Parkbremse zu erhalten. Im Falle, dass dieses nicht mehr möglich ist, werden Sekundärbremsfunktionen aufgerufen, durch die das Fahr-

[33] Vgl. ebd.
[34] Vgl. ebd.: S. 50
[35] Vgl. Schaffner (2007): S. 50

zeug kontrolliert gestoppt werden kann, bei voller Funktionsfähigkeit, jedoch geringerer Leistung[36].

Tritt allerdings ein Fehler auf, durch den die Bremsleistung auf ein kritisches Niveau herabgesenkt wird und somit eine gefährliche, nicht beherrschbare Situation vorliegt, oder ist vorhersehbar, dass weitere Fehlfunktionen auftreten werden, wird der sogenannte „Auto-Stopp"-Mechanismus ausgelöst. Das bedeutet, dass das Fahrzeug auf kontrollierte Weise zum Stillstand gebracht wird. Der Fahrer des PKWs wird vorher darauf aufmerksam gemacht, dass das Bremssystem nicht in der Lage ist, seine Funktion sicher durchzuführen. Sollte das Fahrzeug nach einer definierten Zeit nicht durch den Fahrer zum Stillstand gebracht worden sein, wird durch eine Softwareregelung das Motordrehmoment gesenkt und das Fahrzeug durch Nutzung der Motorbremse und einer stetigen Verminderung des Motordrehmoments zum Stillstand gebracht[37].

Zur Information des Fahrers wurde ebenfalls ein mehrstufiges Informationssystem entwickelt. Sicherheitsrelevante Informationen werden hierdurch dem Fahrer in sogenannten Level-Kategorien präsentiert und stehen ebenfalls Werkstätten im Falle einer Reparatur zur Verfügung. Hierbei wird unter den folgenden drei Leveln unterschieden:

- Level 1 zeigt Fehler an, die durch eine zuständige Werkstatt behoben werden müssen, jedoch keinen negativen Einfluss auf die benötigte Bremsleistung haben.
- Level 2 meldet Fehler, die dringend behoben werden sollten, da sie die Bremsleistung der elektronischen Keilbremse vermindern.
- Level 3 wirkt bei einem einschneidenden Fehler. Hierdurch wird der Fahrer auf die stark eingeschränkte Funktion des Bremssystems hingewiesen und ihm angeraten, den Wagen schnellstmöglichst zum Stillstand zu bringen, da sonst die "Auto-Stopp"-Funktion aktiviert wird[38].

Durch diese benannten Maßnahmen im Falle eines fehlerfreien bzw. fehlerhaften Zustandes des Automobils wurde sichergestellt, dass selbst bei einer Fehlfunktion das Fahrzeug kontrolliert zum Stillstand gebracht werden kann. Trotz allem ist dadurch nicht zu 100 Prozent ausgeschlossen, dass unerwartete gefährliche Situationen entstehen. Diese möglichen weiteren Situationen könnten möglicherweise in der Sicherheitsplanung übergangen worden sein, auf Basis einer gerin-

[36] Vgl. ebd.
[37] Vgl. Schaffner (2007): S. 51
[38] Vgl. ebd.

geren ASIL-Einstufung. Alternativ hierzu können auch neue, bisher unbekannte Fehler auftreten. Daher wurde für die elektronische Keilbremse ein umfangreiches Überwachungssystem initiiert[39].

Zur Vermeidung möglicher weiterer Fehlfunktionen hat Siemens VDO daher ein zweistufiges Überwachungskonzept entwickelt, das sich zusammensetzt aus

- einer Überwachungsfunktion über die Bremskräfte und
- den sogenannten Predrive-Tests.

Mittels der Bremskraftüberwachung wird abgeglichen, ob die Soll-Bremskraft der Ist-Bremskraft an jedem Rad entspricht und ggf. Korrekturmaßnahmen initiiert. Um wiederum diese Funktionen abzusichern, sind mehrere Sensoren und Plausibilitätstests im Einsatz, die die Eingangssignale überprüfen. Die Rechenalgorithmen und ihre Ausgangswerte auf der anderen Seite werden durch mehrere Controller überwacht, die sich gegenseitig überprüfen, sowie durch Memory-Tests, die funktionelle Fehler von Speichereinheiten feststellen können[40].

In der zweiten Kategorie des Überwachungskonzepts, den Predrive-Tests, wird vor jeder Fahrt getestet, ob eine ausreichende Energieversorgung anliegt, ob aufgetretene Fehler während der letzten Fahrt die kommende Fahrt beeinflussen könnten und ob im Falle einer Fehlfunktion alle Radbremsen einzeln und ohne Probleme abgeschaltet werden können[41].

[39] Vgl. ebd.
[40] Vgl. Schaffner (2007): S. 52
[41] Vgl. ebd.

6 Diskussion

Die ISO 26262 „Functional Safety – Road vehicles“, als der neue Standard für die Automobilbranche, wird einiges in der Entwicklung von sicherheitsrelevanten Komponenten verändern. Doch wie jede grundlegende Veränderung beinhaltet dieses nicht ausschließlich positive Folgen für die Hersteller der Komponenten.

Da es sich hierbei um eine neue Norm handelt und diese den aktuellen Stand der Wissenschaft und Technik beschreibt, müssen die Hersteller die ISO 26262 befolgen, wenngleich dieses nicht mit einem Gesetz gleichgesetzt werden kann. Dennoch werden Gerichte, im Falle eines fehlerhaften Produktes, sich auf die ISO-Norm 26262 stützen und verlangen, dass das Unternehmen nachweist, dass dieser Stand der Technik und Wissenschaft als Mindeststandard umgesetzt wurde. Sollte dieses nicht erfüllt sein, werden sie es schwer haben, die vorgeschriebene Sicherheit des Produktes nachzuweisen und somit die Haftungsschäden voll tragen müssen. Durch diese Tatsache müssen die Hersteller sich der ISO 26262 anpassen und ihre Entwicklungsprozesse ggf. verändern.

Problematisch an dieser Ausrichtung ist, dass die Norm mit der Veröffentlichung im Jahr 2011 bereits veraltet ist. Diese Aussage beruht auf der Tatsache, dass die inhaltlichen Arbeiten an der Norm schon im Jahr 2010 beendet wurden und daher den Stand der Technik und Wissenschaft aus 2010 und nicht 2011 abbilden. Hieraus folgt, dass Produkte, die die ISO 26262 erfüllen, noch nicht endgültig sicher sind, da sie stets dem neuesten Stand der Technik und Wissenschaft genügen müssen. Zudem beinhaltet die Norm Visionen, die zurzeit nicht erfüllt werden können. Hierfür muss erst einige Zeit vergehen, damit sich die Technik der Wissenschaft anpassen kann. Dieses wurde jedoch wissentlich getätigt, damit die Norm für eine längere Zeit ohne Aktualisierungen verwendet werden kann. Das Problem bei diesem Vorgehen ist, dass bei der Veröffentlichung diese Visionen per Definition als Stand der Wissenschaft und Technik eingestuft werden.

Ebenfalls nachteilig ist, dass Unternehmen, die nicht an der Entwicklung der Norm beteiligt waren, erst seit diesem Jahr einen inhaltlichen Entwurf betrachten konnten. Dieser Entwurf wurde weniger als ein Jahr später bereits zum offiziellen Stand der Wissenschaft und Technik ernannt. Gerade diese, oftmals kleinen, Unternehmen sind erheblich in der Umsetzung des Standards benachteiligt, da sie eine kürzere Zeit der Implementierung von Maßnahmen zur Umsetzung der

ISO 26262 hatten, nun jedoch von ihnen gefordert wird, ihre Produkte nach diesem Standard entwickelt zu haben. Für diese geforderte Umsetzung der Norm wird jedoch ein gewisses Maß an Verständnis benötigt, das diese Unternehmen von Experten, bspw. dem TÜV, einkaufen können, um fehlendes Knowhow zu erhalten. Dieses kann sich sowohl auf die Vorgehensweise wie auch auf die inhaltliche Umsetzung der Norm beziehen. Der hierdurch entstehende Vorteil wäre, dass der TÜV als Zertifizierungsinstitut Einblicke in die Entwicklung der Produkte erhält und dieses mit anderen Mitbewerbern des Herstellers teilen kann, ohne produktspezifische Kenndaten weiterzugeben.

Mit Einführung der Norm müssen Hersteller, die bisher die Norm IEC 61508 erfüllt haben, all ihre Produkte an die neue Norm anpassen. Dabei kann es passieren, dass formale Dokumente nachgereicht beziehungsweise neu erstellt werden müssen, damit diese Produkte, obwohl sie seit Jahren als sicher gelten, normgerecht sind. Dieses birgt die Gefahr, dass die Produkte durch die Norm unsicherer gemacht werden, da ggf. Softwareveränderungen vorgenommen werden müssen. Insgesamt müssen die Unternehmen hierbei mit einem Mehraufwand, im Vergleich zur bisherigen IEC 61508, von circa drei bis zehn Prozent kalkulieren, um die Produkte ISO-26262-gerecht zu produzieren bzw. zu entwickeln[42].

Der Vorteil der neuen ISO 26262-Norm besteht vor allem in der Tatsache, dass es nach der Veröffentlichung einen ersten Standard speziell für die Automobilindustrie gibt. Somit werden die Beziehungen und Rangordnungen der Prozesse in der Entwicklung berücksichtigt. In der IEC 61508 gab es diese Prozesse nicht, so dass diese stets an die spezifischen Bedürfnisse und Situationen in der Automobilindustrie angepasst werden musste. Seit dem 14. November 2011 gibt es für Hersteller eine verbindliche und einheitliche Vorgabe, an der sie sich orientieren müssen (ausgenommen Band Zehn). Zudem wurde der aktuellste Stand der Wissenschaft und Technik festgeschrieben, sodass es für Universitäten und Fachhochschulen möglich ist, sich mit Experten aus aller Welt über diesen Standard auszutauschen, diesen Standard weiterzuentwickeln und so lebenslanges Lernen und Forschen zu praktizieren.

Der Grundgedanke der ISO 26262 ist es, die Produkte sicherer zu machen und damit den Endkunden besser zu schützen. Da diese Norm von den Herstellern umgesetzt werden muss, wird der Endkunde hierdurch sicherere Produkte erhalten und damit den größten Nutzen aus dieser neuen Norm durch einen stetigen Zuwachs von Qualität und Sicherheit in der Automobilbranche erhalten. Dieses

[42] Vgl. Sauler, Jürgen (2011a)

basiert auf der Idee der Norm, die Hersteller bereits im Vorfeld einer Entwicklung zu zwingen, sich Gedanken zur Sicherheit zu machen und dieses zu dokumentieren. Auf diese Weise wird eine vorschnelle Entwicklung, in die erst im Nachhinein Sicherheitsmechanismen implementiert werden, verhindert. Außerdem können Produkthaftungen einfacher und besser entschieden werden, da die ISO 26262 der Mindeststandard für Produkte ist.

Entscheidend für die ISO-Norm 26262 werden jedoch der Austausch und die Weitergabe des Knowhows sein. Das Problem an der Norm ist, dass sie in einigen Bereichen, wie zum Beispiel die Bestimmung der ASIL-Einstufung und den anzuwendenden Tools, weitgehend offen gestaltet wurde. Dadurch erhalten Unternehmen einen gewissen Freiheitsgrad, den sie eigentlich nicht gefordert haben. Auf Basis dieser Tatsache können Produktentwicklungen, mit einer korrekten Argumentation, unterschiedlich ausfallen und auch Wettbewerbsspielräume entstehen. Dieses betrifft nicht ausschließlich das Design, sondern auch die wichtigen Sicherheitsfunktionen. Insgesamt wird es jedoch für die Unternehmen und vor allem für den Endkunden positive Effekte haben, sodass die ISO-Norm 26262 wahrscheinlich eher ein Segen für die Industrie sein wird als ein Fluch[43].

[43] In Anlehnung an die Podiumsdiskussion ISO 26262 – Fluch oder Segen? beim ESE-Kongress 2010 in Sindelfingen

Quellenverzeichnis

Internetquellen

Aschenbrenner, Norbert (2005). *Auto Electronics – Braking Systems - Wonder Wedge* [Online-Dokument]. Verfügbar unter: http://www.siemens.com/innovationen/publikationen/publications_pof/pof_fall_2005/auto_electronics/braking_systems.htm, letzter Zugriff am: 27.11.2011

Bruckner, Regina (2010). Sprache des Handels – Warum die Gurke nicht mehr krumm ist [Online-Dokument]. Verfügbar unter: http://derstandard.at/1271377518032/Sprache-des-Handels-Warum-die-Gurke-nicht-mehr-krumm-ist?sap=2&_seite=15, letzter Zugriff am: 27.10.2011

DIN Deutsches Institut für Normung e. V. (Hrsg.) (2005): Hannover Messe 2005 – Normen sind das Öl im Getriebe des Welthandels [Online-Dokument]. verfügbar unter: http://www.din.de/cmd?level=tpl-artikel&languageid=de&cmstextid=hmi_05, letzter Zugriff am: 27.10.2011

FERCHAU Engineering GmbH (Hrsg.) (2011). *Funktionale Sicherheit im Zehnerpack: ISO* 26262 [Online-Dokument]. Verfügbar unter: http://www.ferchau.de/news/details/funktionale-sicherheit-im-zehnerpack-iso-26262-969/, letzter Zugriff am: 27.11.2011

Fürst, Simon (2010). ISO 26262 and AUTOSAR – Requirements and Solutions for Safety Related Software [Online-Dokument]. Verfügbar unter: http://www.vector.com/portal/medien/cmc/events/commercial_events/VectorCongress_2010/AUTOSAR_2_Fuerst_Lecture.pdf, letzter Zugriff: 27.11.2011

Glöe, Günther; Jung, Christoph (2011). *Einführung in die Inhalte der ISO FDIS 26262: Road Vehicles – Functional Safety* [Online-Dokument]. Verfügbar unter: http://www.euroforum-fachwissen.de/industrie-und-automobil/iso-26262/einfuhrung-in-die-inhalte-der-iso-fdis-26262-road-vehicles-functional-safety.html, letzter Zugriff am: 27.11.2011

Hafner, Martina (2010). Interview Bosch – Alle Fakten zur ISO 26262 [Online-Dokument]. Verfügbar unter: http://www.elektronikpraxis.vogel.de/index.cfm?pid=906&pk=248663&p=2, letzter Zugriff am: 27.11.2011

Sauler, Jürgen; Kriso, Stefan (2011a): *ISO 26262 – Die zukünftige Norm zur funktionalen* Sicherheit von Straßenfahrzeugen [Online-Dokument]. Verfügbar unter: http://www.elektronikpraxis.vogel.de/index.cfm?pid=904&pk=242243&p=1, letzter Zugriff am: 27.11.2011

Sauler, Jürgen; Kriso, Stefan (2011b): *ISO 26262 – Die zukünftige Norm zur funktionalen Sicherheit von Straßenfahrzeugen* [Online-Dokument]. Verfügbar unter: http://www.elektronikpraxis.vogel.de/index.cfm?pid=904&pk=242243&p=2, letzter Zugriff am: 27.11.2011

Sauler, Jürgen; Kriso, Stefan (2011c): *Sicherheitslebenszyklus in der ISO 26262* [Online-Dokument]. Verfügbar unter: http://www.elektronikpraxis.vogel.de/index.cfm?none=1&pid=5414&pk=263884&fk=242243&ct=10, letzter Zugriff am: 27.11.2011

TÜV SÜD Automotive GmbH (Hrsg.) (2010). ISO 26262 – *Der neue Automotive Standard für Funktionale Sicherheit* [Online-Dokument]. Verfügbar unter: http://www.it-speicher.de/it-speicher/Media/3/153/1/104003.pdf, letzter Zugriff am: 27.11.2011

Wikimedia Foundation Inc. (Hrsg.) (2011). *ISO 26262* [Online-Dokument]. Verfügbar unter: http://de.wikipedia.org/wiki/ISO_26262, letzter Zugriff am: 27.11.2011

Fachzeitschriften

Schaffner, Johanna (2007). Sicher bremsen - Bremsen sichern. Funktionaler Sicherheitsnachweis der elektronischen Keilbremse. in: Automotive 9.2007, Verleger: Carl Hanser Verlag GmbH & Co. KG, München, S. 48-52

Bauer, Bernhard: Die ISO 26262 für Automotive kommt! Bedeutung und Auswirkungen auf das Embedded Engineering, 2011

Sauler, Jürgen: Funktionale Sicherheit für Straßenfahrzeuge – ISO 26262 aus Sicht eines Automobilzulieferers, 2011

Kongresse

Embedded Software Engineering Kongress: Sauler, Jürgen: ISO 26262 – Fluch oder Segen?, 2010 Sindelfingen