Seminar Sommersemester 2011:
Automobile Systeme in der Automatisierung
Prof. Dr. Dieter Zöbel, Universität Koblenz-Landau, FB Informatik

Funktionale Sicherheit elektronischer Systeme in Kraftfahrzeugen

Juliane Barjenbruch

Eingereicht: 27.06.2011 / Fertiggestellt: 25.08.11

Zusammenfassung Die Entwicklung und Produktion elektrischer und elektronischer Systeme gewinnt bei der Fahrzeugentwicklung einen immer größeren Stellenwert. Mit diesem Trend geht das Bedürfnis einher, diese Systeme möglichst sicher und robust zu gestalten. In dieser Arbeit wird zunächst definiert, was Sicherheit allgemein und konkret, was Funktionale Sicherheit bedeutet. Anschließend wird die Grundnorm DIN EN 61508 für Funktionale Sicherheit elektrischer und elektronischer Systeme vorgestellt. Der Fokus dieser Arbeit liegt auf der ISO 26262 Norm für Funktionale Sicherheit elektrischer und elektronischer Systeme in Kraftfahrzeugen. Hierbei wird vor allem auf die Anforderungen der Norm bezüglich der Gefährdungs- und Risikoanalyse, der Entwicklung auf System- und Softwareebene und der Bewertung der Funktionalen Sicherheit eingegangen. Anschließend werden die Probleme bei der Umsetzung der Norm und die Akzeptanz der Norm diskutiert.

Schlüsselwörter Funktionale Sicherheit, ISO 26262, Gefährdungs- und Risikoanalyse, ASIL

1 Einleitung

In einem durchschnittlichen Mittelklassewagen sind heutzutage ca. 80 elektronische Steuergeräte verbaut. Die korrekte Funktion der Geräte selbst und deren Zusammenspiel sind für den sicheren Betrieb eines Fahrzeugs unabdingbar.

Um bewerten zu können, wie sicher ein System ist, ist ein allgemein anerkanntes Verfahren zur Bewertung von sicherheitskritischen Systemen notwendig. Außerdem müssen Anforderungen definiert werden, die an diese Systeme gestellt werden. Auch die Anforderungen müssen Hersteller-übergreifend und international anerkannt sein, um wirklich objektive Vergleichskriterien schaffen zu können.

Juliane Barjenbruch
Universität Koblenz-Landau
E-Mail: jbarjenbruch@uni-koblenz.de

1.1 Motivation für Sicherheitsnormen

Sicherheitsnormen dienen dazu, den aktuellen Stand der Technik widerzuspiegeln. Sie legen fest, welche Anforderungen an sicherheitskritische Systeme gestellt werden und wie bewertet werden kann, wie sicher ein System ist. Sie zielen darauf ab, dass durch ihre Umsetzung Gefahren und Risiken, die von den sicherheitskritischen Systemen ausgehen, auf ein tolerierbares Maß gesenkt werden.

Das Risiko, das von einem System ausgeht, ergibt sich aus der Eintrittswahrscheinlichkeit für einen gefährdenden Zustand multipliziert mit der Höhe des potentiellen Schadens. Das Ziel ist es, das Risiko zu minimieren, indem entweder die Wahrscheinlichkeit für einen Fehlerfall oder der potentielle Schaden durch Verbesserung der Reaktion eines Systems auf einen Fehler verringert wird.

Nachfolgend werden vorrangig zwei Sicherheitsnormen in Betracht gezogen. Zum einen die Grundnorm für Funktionale Sicherheit DIN EN 61508 und zum anderen die im Laufe des Jahres 2011 veröffentlichte Spezialisierung dieser Norm für die Automobilindustrie: die ISO 26262.

1.2 Motivation der Automobil-Hersteller für die Umsetzung der Normen

Ein wichtiger Grund, für die Hersteller elektronischer Systeme in Kraftfahrzeugen Sicherheitsnormen umzusetzen, ist es ihr Produkthaftungsrisiko zu minimieren.

Jedem Hersteller von Verbraucherprodukten, in diesem Fall Serienkraftfahrzeugen, obliegt die Verkehrssicherungspflicht. Demnach ist er verpflichtet, ein Produkt nur dann in Verkehr zu bringen, wenn er die Erwartungen, die ein Verbraucher nach dem aktuellen Stand von Wissenschaft und Technik an ein Produkt hat, erfüllen kann [SKa]. Durch die nachweisbare Umsetzung einer entsprechenden Sicherheitsnorm kann ein Hersteller beweisen, dass sein Produkt die Anforderungen nach aktuellem Stand von Wissenschaft und Technik erfüllt. „In Deutschland (nicht notwendigerweise international) kann nach §1 Abs.2 ProdHaftG die Ersatzpflicht des Herstellers ausgeschlossen werden, wenn er den Produktfehler zum Zeitpunkt des Inverkehrbringens bei Einhaltung des „Stands der Wissenschaft und Technik“ nicht erkennen konnte. Es gilt hier allerdings die Beweislastumkehr: Nicht der Geschädigte muss einen Produktfehler nachweisen, vielmehr muss der Hersteller seine Konformität zum Stand der Wissenschaft und Technik, welcher Standards für Funktionale Sicherheit einschließt, dem Gericht nachweisen.“ [HMNS]. Erfüllt ein Hersteller jedoch nicht die Anforderungen der Sicherheitsnorm, muss er anderweitig nachweisen, dass er trotzdem alle Anforderungen des Verbrauchers zum Zeitpunkt des In-Verkehr-Bringens erfüllt hat [SKa]. Dies kann sich beliebig schwer bis unmöglich gestalten.

In der europäischen Union sind Manager von Firmen, die unsichere Produkte auf den Markt bringen, persönlich für mögliche Schäden haftbar [LPP10]. Managerhaftpflichtversicherungen bewerten die nicht Umsetzung von Sicherheitsnormen als Vorsatz bzw. grobe Fahrlässigkeit, weshalb sie im Produkthaftungsfall nicht schützen würden [LPP10].

Kommen durch ein unsicheres Produkt Personen zu Schaden oder gar zu Tode, wird unter Umständen auch strafrechtlich gegen die Mitarbeiter eines Unternehmens ermittelt. Erfolgt eine Verurteilung wegen fahrlässiger Körperverletzung, ggf. mit Todesfolge kann dies in Deutschland eine Freiheitsstrafe von bis zu 5 Jahren zur Folge haben. Als fahrlässig bzw. grob fahrlässig gilt in diesem Fall, wenn das

Management des Herstellers explizit die Einhaltung von Standards und entsprechenden Entwicklungsvorgaben verneint hat [HMNS].

2 Funktionale Sicherheit

Die Grundnorm für Funktionale Sicherheit DIN EN 61508 beschreibt Sicherheit allgemein als die Freiheit von unvertretbaren Risiken. Funktionale Sicherheit wird als der Teil der Gesamtsicherheit, der von der korrekten Funktion des sicherheitsbezogenen Systems abhängt, charakterisiert. Funktionale Sicherheit ergibt sich also aus der korrekten Funktion des Systems selbst heraus im Gegensatz zu externen Sicherheitsmaßnahmen wie Brand- oder Strahlenschutz. Auch ist sie abzugrenzen von der Angriffssicherheit, die nicht ausschließlich von der korrekten Funktion des Systems selbst abhängig ist.

In der Norm für Funktionale Sicherheit elektronischer Systeme in Kraftfahrzeugen wird der Begriff Funktionale Sicherheit als die Abwesenheit eines inakzeptablen Risikos aufgrund einer Gefährdung verursacht durch fehlerhaftes Verhalten von elektrischen und/oder elektronischen Systemen beschrieben [GS].

Die Grundnorm DIN EN 61508 und alle von ihr abgeleiteten bereichsspezifischen Normen zur Funktionalen Sicherheit fordern vier grundlegende Maßnahmen bei der Entwicklung sicherheitskritischer Systeme:

- Maßnahmen zum **Management** der Funktionalen Sicherheit
- Maßnahmen gegen zufällige **Hardwareausfälle**
- Maßnahmen gegen systematische **Systemausfälle**
- Maßnahmen zur **Beurteilung** der Funktionalen Sicherheit

3 Grundnorm DIN EN 61508: Funktionale Sicherheit

Die Grundnorm DIN EN 61508 mit dem Titel „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ definiert die konkreten notwendigen Anforderungen an die sicherheitskritischen Systeme, um die ebenfalls in der Norm festgelegten Sicherheitsziele zu erreichen und so das Gesamtrisiko, welches von dem System ausgeht, auf ein tolerierbares Maß zu senken.

Das Gesamtrisiko soll gesenkt werden, indem Systemausfälle möglichst vermieden werden oder, falls dies nicht vollständig möglich ist, beherrschbar gemacht werden können. Die Beherrschbarkeit stellt sich meist so dar, dass das System in eine Art sicheren Zustand versetzt wird, indem weitere Ausfälle und Schäden verhindert werden sollen und ein möglichst sicherer weitere Betrieb des Systems ermöglicht wird.

Bei den Ursachen für Systemausfälle wird zwischen systematischen Fehlern und zufälligen Hardwareausfällen unterschieden. Die systematischen Fehler sind zum Beispiel Spezifikations-, Entwurfs- oder Implementierungsfehler [LPP10]. Diese können durch kontinuierliche Prozessoptimierung und Sorgfalt bei der Entwicklung eines Systems reduziert werden [GS]. Zufällige Hardwareausfälle entstehen auf Grund unzuverlässiger Bauteile. Diese können unter Umständen nicht ohne weiteres reduziert werden. Der Fokus sollte deshalb auf dem Erkennen und dem Umgang mit diesen Ausfällen liegen [GS].

Allgemein ist es erstrebenswert, eine systematische Entwicklung mit Hilfe eines Sicherheitslebenszyklus zu forcieren. Durch die systematische Entwicklung soll es möglich

sein, potentielle Systemausfälle identifizieren zu können und sie anschließend vermeidbar bzw. beherrschbar machen zu können.

Die DIN EN 61508 wurde ursprünglich für Großanlagen zum Beispiel in der chemischen Industrie entwickelt. Die in der Norm vorgeschlagenen Prozessmodelle sind daher nur schwer auf Serienproduktionen übertragbar. Des Weiteren wird die Redundanz von Bauteilen als Möglichkeit zur Beherrschbarkeit von Systemausfällen aufgeführt. Dies ist jedoch konkret in der Automobilindustrie nicht anwendbar, da hierdurch Kosten und Gewicht eines Fahrzeugs übermäßig in die Höhe getrieben würden. Auch werden in Großanlagen häufig externe Sicherheitssysteme und Kontrollfunktionen eingesetzt, um die Sicherheit der Anlage zu gewährleisten. Im Automobil hängt die Sicherheit allerdings eher von der korrekten Arbeitsweise des Systems selbst ab.

Die hier beschriebenen und noch viele weitere Unsicherheiten und Unklarheiten über die Interpretation der DIN EN 61508 für die Automobilindustrie führten zu den Bestrebungen eine eigene Norm für Funktionale Sicherheit in der Automobilindustrie zu entwickeln.

4 ISO/DIS 26262: „Road vehicles – Functional safety“

Die ISO 26262 mit dem Titel „Road vehicles – Functional safety“ ist die Anpassung der Grundnorm DIN EN 61508 für die Automobilindustrie. Sie ersetzt ab ihrem Veröffentlichungszeitpunkt die Grundnorm als Nachweis für den aktuellen Stand von Wissenschaft und Technik. Die Norm gilt für alle elektrischen und elektronischen Systeme in Personenkraftwagen bis 3,5 Tonnen Gesamtgewicht. Das Sicherheitslebenszyklusmodell ist an die Serienproduktion in der Automobilindustrie angepasst. Auch alle weiteren Anforderungen sind konkretisiert und adaptiert für die besonderen Gegebenheiten in der Automobilindustrie [HG].

4.1 Inhalt

Die ISO 26262 enthält Anforderungen an jede Phase des kompletten Produktlebenszyklus [Sau]. Zum Beispiel an die:

- Konzeptphase
- System-, Hardware- und Softwareentwicklung
- Produktion
- Betrieb
- Außerbetriebnahme

Neben den Anforderungen an die einzelnen Phasen des Produktlebenszyklus definiert die Norm auch Lebenszyklus übergreifende Anforderungen an das Management und die Organisation der Funktionalen Sicherheit. Außerdem werden weitere unterstützende Prozesse beschrieben. Hierzu gehören:

- Konfigurationsmanagement
- Anforderungsmanagement
- Qualifizierung von Tools, Hardware- und Softwarekomponenten
- Sicherheitsnachweis/Nachweis der Normkonformität

Das Konfigurationsmanagement ist gerade in der Automobilindustrie von besonderer Bedeutung, da häufig konfigurierbare Software eingesetzt wird, deren Verhalten möglicherweise erst nach Serienstart durch Kalibrierdaten bestimmt wird [Sau]. Außerdem wird im Zusammenhang mit der Qualifizierung von Softwarekomponenten und dem Sicherheitsnachweis beschrieben, wie die Schnittstellen zu den Zulieferern und die Zuweisung der Sicherheitsverantwortung bei verteilter Entwicklung teilweise über mehrere Zuliefererebenen hinweg organisiert werden kann.

Das Kernstück der Norm ist das Sicherheitslebenszyklusmodell. Die einzelnen Teile der Norm beziehen sich größtenteils auf jeweils eine Phase dieses Modells. Abbildung 1 zeigt das Sicherheitslebenszyklusmodell mit den einzelnen Phasen.

Zunächst wird das gesamte System in einzelne Betrachtungseinheiten (items) unterteilt. Diese können zum Beispiel einzelne System- oder Fahrzeugfunktionen umfassen. Nach Abschluss der Konzeptphase wird eine Gefährdungs- und Risikoanalyse (siehe Abschnitt 4.2) durchgeführt. In dieser Phase wird festgelegt, welche Funktionen welchen Sicherheitslevel erreichen müssen.

Nachdem das Funktionale Sicherheitskonzept (siehe Abschnitt 4.2) erstellt wurde, erfolgt die Produktentwicklung auf Systemebene. Diese Phase enthält außerdem die Produktentwicklung auf Hardware- und Softwareebene. Des Weiteren muss während der Systementwicklung bereits die Planung der Produktion und des Betriebs berücksichtigt werden. Nach der Beurteilung der Funktionalen Sicherheit (siehe Abschnitt 4.5) und der Produktfreigabe, erfolgt die eigentliche Produktion. Der letzte Abschnitt des Sicherheitslebenszyklus beinhaltet den Betrieb, die Instandhaltung und die Außerbetriebnahme des Fahrzeugs.

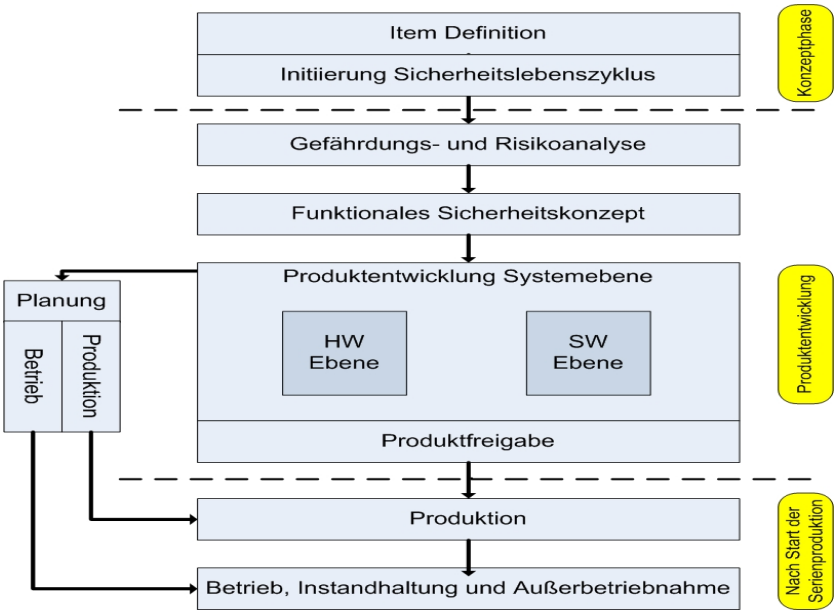

Abb. 1 Sicherheitslebenszyklus nach ISO 26262 [LPP10]

Im Gegensatz zur Grundnorm DIN EN 61508 definiert die ISO 26262 Norm für jede Phase bestimmte Arbeitsprodukte, meistens in Form von Dokumenten, die am Ende der jeweiligen Phase vorhanden sein müssen und so in den darauffolgenden Phasen genutzt werden können [LPP10].

4.2 Gefährdungs- und Risikoanalyse

Bei der Gefährdungs- und Risikoanalyse wird festgelegt, wie sicher die einzelnen Elemente und Funktionen eines Systems sein müssen. Zur Charakterisierung der Sicherheitslevel wurde das Konzept der ASIL-Stufen eingeführt. Die Abkürzung ASIL steht für Automotive Safety Integrity Level. Die ASIL-Stufen gehen von A bis D wobei A die niedrigste und D die höchste Stufe ist. Je höher eine Funktion bezüglich des ASIL-Levels eingestuft wird, desto sicherer muss die Funktion sein. Ist zum Beispiel eine Funktion als ASIL-Level D eingestuft, dürfen nicht mehr als 100 Fehler bzw. Ausfälle innerhalb von 1 Milliarde Betriebsstunden auftreten [Roo].

Die Festlegung des jeweiligen ASIL-Levels für eine Funktion erfolgt anhand von drei Faktoren [LPP10] :

- **Severity S** (Schwere des möglichen Schadens)
- **Exposure E** (Häufigkeit der Fahrsituation)
- **Controllability C** (Beherrschbarkeit durch den Fahrer)

Die Schwere des möglichen Schadens **Severity S** wird in vier Kategorien S0 bis S3 eingeteilt (siehe Tabelle 1). Die Kategorie S0 steht für Unfälle ohne Verletzungen der Insassen, wie zum Beispiel das Anfahren an einen Zaun oder Begrenzungspfahl mit weniger als 15 km/h [LPP10]. S3 steht für die schlimmstmöglichen Verletzungen nämlich lebensgefährliche Verletzungen, bei denen das Überleben einer oder mehrerer Insassen unwahrscheinlich ist. Eine solche Situation wäre zum Beispiel ein Seitenaufprall eines anderen Fahrzeugs mit mehr als 35 km/h.

Severity	
S0	Keine Verletzungen
S1	Leichte und mittlere Verletzungen
S2	Schwere Verletzungen
S3	Lebensgefährliche Verletzungen

Tabelle 1 Severity S (Schwere des möglichen Schadens)

Die Häufigkeit von Fahrsituation **Exposure E** ist in fünf Stufen E0 bis E4 eingeteilt (siehe Tabelle 2). Die Kategorie E0 entspricht einer unvorstellbaren Situation und wird deshalb auch größtenteils bei der Festlegung der ASIL-Level außer Acht gelassen. Eine Situation, die bei jeder Fahrt auftreten kann, wird in die Exposure-Stufe E4 eingeteilt. Hierzu gehören Situationen wie das Schalten oder Beschleunigen des Fahrzeugs.

Exposure	
E0	Unvorstellbar
E1	Sehr niedrige Wahrscheinlichkeit
E2	Niedrige Wahrscheinlichkeit
E3	Mittlere Wahrscheinlichkeit
E4	Hohe Wahrscheinlichkeit

Tabelle 2 Exposure E (Häufigkeit der Fahrsituationen)

Für die Beherrschbarkeit einer Situation durch den Fahrer **Controllability C** werden ebenfalls vier Kategorien C0 bis C3 unterschieden (siehe Tabelle 3). C0 steht für Situationen, die im Allgemeinen beherrschbar sind. Auch diese Kategorie wird bei der Einstufung der ASIL-Level größtenteils außer Acht gelassen, da Situationen die für den Fahrer beherrschbar sind, meistens zu keinen Verletzungen führen. Schwierig oder nicht mehr beherrschbare Situationen werden mit C3 eingestuft. Beispiele hierfür ist ein totaler Ausfall der kompletten Bremskraft oder eine unmotivierte Lenkbewegung bei mittlerer bis hoher Geschwindigkeit [For].

Controllability	
C0	Im Allgemeinen beherrschbar
C1	Einfach beherrschbar
C2	Normalerweise beherrschbar
C3	Schwierig oder nicht beherrschbar

Tabelle 3 Controllability C (Beherrschbarkeit durch den Fahrer)

Mit der Festlegung dieser drei Faktoren kann dann anhand von Tabellen das resultierende ASIL-Level abgelesen werden. Abbildung 2 zeigt die Tabelle für Situationen bei denen die Schwere des möglichen Schadens mit S1 eingestuft wurde.

	C1	C2	C3
E1			
E2			
E3			ASIL A
E4		ASIL A	ASIL B

Abb. 2 Festlegung der ASIL-Level für S1

S1 steht für leichtere bis mittlere Verletzungen, wie sie zum Beispiel bei einem Frontalzusammenstoß zweier PKW mit weniger als 20 km/h auftreten können [LPP10]. Hierzu gehören unter anderem leichte Fleischwunden, unkomplizierte Rippen- oder Knochenbrüche und kurzzeitige Bewusstlosigkeit [For].

Allgemein ist zu beobachten, dass je höher die Schwere des potentiellen Schadens, je unkontrollierbarer die Situation und je höher die Wahrscheinlichkeit für das Auftreten der Situation ist, desto höher ist auch das resultierende ASIL-Level.

Abbildung 2 zeigt, dass für die Stufe S1 bei der Schwere des potentiellen Schadens eine hohe Wahrscheinlichkeit für das Auftreten der Situation (E4) in Kombination mit einer normalerweise möglichen Beherrschbarkeit der Situation (C2) in einem ASIL-Level A resultiert. Als normalerweise beherrschbar (C2) werden die Situationen eingestuft, in denen durchschnittliche weniger als 10% der Fahrer nicht in der Lage sind die Situation zu kontrollieren [For]. Dies ist zum Beispiel der Fall, wenn auf einer unbeleuchteten Landstraße das Licht des Fahrzeugs ausfällt, da die meisten Fahrer (mehr als 90%) in der Lage waren, das Fahrzeug zu stoppen ohne von der Fahrbahn abzukommen.

ASIL-Level A ergibt sich außerdem, wenn zwar die Situation für den Fahrer schwierig oder nicht mehr beherrschbar ist (C3), aber dafür auch nur mit mittlerer Wahrscheinlichkeit (E3) auftritt. Zu den Situationen, die mit mittlerer Wahrscheinlichkeit auftreten, gehören zum Beispiel das Fahren auf nasser Fahrbahn oder das Betanken des Fahrzeugs.

	C1	C2	C3
E1			
E2			ASIL A
E3		ASIL A	ASIL B
E4	ASIL A	ASIL B	ASIL C

Abb. 3 Festlegung der ASIL-Level für S2

Bei größerer Schwere eines möglichen Schadens, werden auch die resultierenden ASIL-Level höher. Abbildung 3 zeigt die Einstufung der ASIL-Level für eine Schwere des möglichen Schadens auf Stufe S2. Diese steht für schwere Verletzungen der Insassen bei denen im Gegensatz zu S3 jedoch ein Überleben wahrscheinlich ist. Hierzu zählen Schädelbasisbrüche jedoch ohne Schädigung des Gehirns, mehrstündige Bewusstlosigkeit oder mehrfache Rippenbrüche [For].

Hier erfolgt eine Zuordnung eines ASIL-Levels A bereits für Situationen, die nur mit niedriger Wahrscheinlichkeit (E2) auftreten, dafür aber nur schwer bis gar nicht mehr beherrschbar sind (C3). Zu Exposure-Stufe E2 gehören Situationen, die mehrmals im Jahr auftreten, zum Beispiel Fahrten mit einem Anhänger oder Dachgepäckträger [LPP10].

Tritt die betrachtete Situation bei jeder Fahrt auf (E4) und ist sie schwer bis gar nicht mehr beherrschbar (C3), so wird ihr für die Severity-Stufe S2 ein ASIL-Level C zugeordnet. Tritt die betrachtete Situation zwar bei jeder Fahrt auf (E4), ist dafür aber einfach beherrschbar (C1), so wird ihr nur ein ASIL-Level A zugeordnet. Zu den einfach beherrschbaren Situationen zählen diese, in denen weniger als 1% der Fahrer nicht in der Lage sind die Situation zu kontrollieren [For]. Wenn zum Beispiel beim Anfahren des Fahrzeugs die Lenksäule blockiert ist es für die meisten Fahrer (mehr als 99%) möglich durch Bremsen des Fahrzeugs die Situation unter Kontrolle zu behalten, sodass keine Insassen verletzt werden [For].

Abbildung 4 zeigt die Tabelle zur Zuordnung der ASIL-Level für Situationen in denen die Schwere des möglichen Schadens die höchste Stufe (S3) erreicht hat. Bei Severity-Stufe S3 erleiden die Insassen lebensgefährliche Verletzungen, die ein Überleben unwahrscheinlich werden lassen. Hierzu gehören Verletzungen der Halswirbel und des Rückenmarks, Hirnblutungen, länger als 12 Stunden andauernde Bewusstlosigkeit und kritische offene Wunden an Brustkorb oder Bauchhöhle.

Für die höchste Stufe des möglichen Schadens (S3) wird bereits bei einer sehr niedrigen Wahrscheinlichkeit für das Auftreten der betrachteten Situation (E1) in Kombination mit einer schweren bis unmöglichen Beherrschbarkeit (C3) ein ASIL-Level A zugeordnet. Zu den Situationen, die mit sehr niedriger Wahrscheinlichkeit (E1) auftreten, gehören das Auslösen des Airbags, das Abschleppen eines Fahrzeugs und das Starten des Fahrzeugs mittels Starthilfe [For].

	C1	C2	C3
E1			ASIL A
E2		ASIL A	ASIL B
E3	ASIL A	ASIL B	ASIL C
E4	ASIL B	ASIL C	ASIL D

Abb. 4 Festlegung der ASIL-Level für S3

Nach Abschluss der Gefährdungs- und Risikoanalyse und Festlegung eines ASIL-Levels für jede Funktion des Systems, wird das **Funktionale Sicherheitskonzept** erstellt. Hierbei werden die konkreten Sicherheitsanforderungen aus den Sicherheitszielen abgeleitet und den jeweiligen Architekturelementen zugeordnet. Des Weiteren werden die Fehlertoleranzzeiten spezifiziert. Ein Fahrer-Warnkonzept, welches festlegt, wie der Fahrer über den aufgetreten Fehler bzw. Ausfall einer Funktion informiert werden soll, wird erstellt. Außerdem wird ein Konzept für den sicheren Betrieb im Fehlerfall angefertigt. Bereits in dieser Phase werden Kriterien für die spätere Sicherheitsvalidierung festgelegt.

Abbildung 5 zeigt ein Beispiel für das Ergebnis einer Gefährdungs- und Risikoanalyse in Kombination mit einem Funktionalen Sicherheitskonzept.

In diesem Beispiel wird die Gefährdungs- und Risikoanalyse für die Funktion der Servolenkung also Lenkkraftunterstützung durchgeführt. Als mögliche Fehlerfälle wurden die drei links stehenden Situationen identifiziert: unmotivierte Lenkbewegung, halbierte Lenkkraftunterstützung und Ausfall der Lenkkraftunterstützung. Des Weiteren wurden drei Fahrszenarien jeweils abhängig von der Geschwindigkeit festgelegt. Für jede der drei Gefährdungsarten wurden dann für jedes der drei Fahrszenarien die Exposure-, Controllability- und Severity-Stufen bestimmt. Anhand dieser Faktoren können dann die ASIL-Level den entsprechenden Tabellen entnommen werden.

Da immer eine Kombination aller drei Fahrszenarien auftreten kann, ist das resultierende ASIL-Level für alle drei Fahrszenarien zusammen das jeweils höchste der drei einzelnen Fahrszenarien. Für die Gefährdung „Halbierte Lenkkraftunterstützung“ in Kombination mit dem Fahrszenario „Langsame Fahrt“ war keine Zuordnung eines ASIL-Level notwendig, sondern qualitätssichernde Maßnahmen (QM) sind als ausreichend eingestuft worden.

G&R Servolenkung							
	Fahrszenarien / Gefährdungen	Langsame Fahrt (<= 20km/h)		Stadtfahrt (ca. 40-60 km/h)		Landstraße (ca. 80-100 km/h)		Resultierendes ASIL
1	Unmotivierte Lenkbewegung	E	E4	E	E4	E	E4	ASIL D
		C	C2	C	C2	C	C3	
		S	S1	S	S2	S	S3	
		ASIL	A	ASIL	C	ASIL	D	
2	Halbierte Lenkkraftunterstützung	E	E4	E	E4	E	E4	ASIL B
		C	C1	C	C1	C	C1	
		S	S1	S	S2	S	S3	
		ASIL	QM	ASIL	A	ASIL	B	
3	Ausfall der Lenkkraftunterstützung	E	E4	E	E4	E	E4	ASIL B
		C	C2	C	C1	C	C1	
		S	S1	S	S2	S	S3	
		ASIL	A	ASIL	A	ASIL	B	

	Sicherheitsanforderung	Sicherer Zustand	Sicherheitszeit
1	Unmotivierte Lenkbewegungen sind mit Sicherheit zu verhindern. Ansteuerung Fehlerlampe. Eintrag Fehlerspeicher.	Betrieb der Lenkkraftverstärkung deaktivieren. Mechanische Lenkbarkeit bleibt bestehen.	20-30 ms
2	Lenkkraftunterstützung überwachen und ggf. nachregeln. Ansteuerung Fehlerlampe. Eintrag Fehlerspeicher.	Betrieb der Lenkkraftverstärkung aufrechterhalten. Betrieb in einem "verdächtigen Zustand".	20-30 ms
3	Lenkkraftunterstützung überwachen und ggf. nachregeln. Ansteuerung Fehlerlampe. Eintrag Fehlerspeicher.	Betrieb der Lenkkraftverstärkung aufrechterhalten. Betrieb in einem "verdächtigen Zustand".	20-30 ms

Abb. 5 Beispiel Gefährdungs- und Risikoanalyse [LPP10]

Der untere Bereich von Abbildung 5 zeigt einen Teil des Funktionalen Sicherheitskonzeptes. Den jeweiligen Gefährdungen werden die entsprechenden Sicherheitsanforderungen zugeordnet. Außerdem wird beschrieben, wie ein möglichst „Sicherer Zustand“ nach Auftreten eines Fehlers bzw. Ausfalls erreicht werden kann. Zum Beispiel soll, nachdem eine unmotivierte Lenkbewegung durch einen Fehler im Lenkkraftverstärkungssystem aufgetreten ist, dieses deaktiviert werden, um weitere Fehler solcher Art zu verhindern. Des Weiteren wird eine Sicherheitszeit festgelegt, die besagt, wie viel Zeit verstreichen darf, bis das System auf den aufgetreten Fehler entsprechend reagieren und einen „Sicheren Zustand“ erreichen kann.

4.3 Entwicklung auf Systemebene

In Abbildung 6 ist die Phase des Sicherheitslebenszyklus dargestellt, die die Entwicklung auf Systemebene beschreibt. Sie ist dabei selbst wieder in verschiedene Abschnitte untergliedert.

In der Phase „Einleitung der Produktentwicklung auf Systemebene“ wird zunächst die Gesamtplanung um die Validierungs-, Integrations- und Testplanung ergänzt [LPP10]. Unter Umständen kann in diesem Schritt das Gesamtsystem nochmal in Subsysteme unterteilt werden.

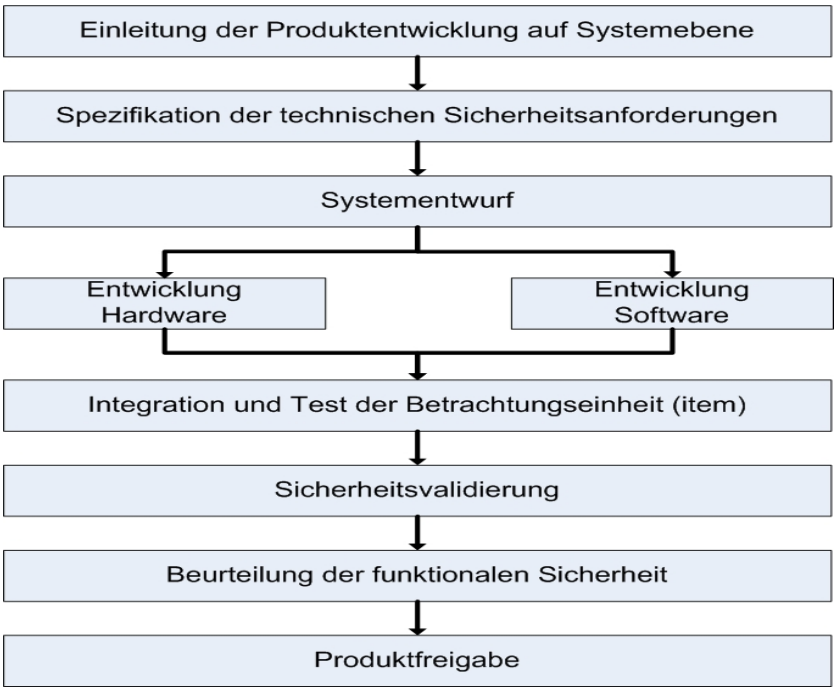

Abb. 6 Entwicklung auf Systemebene nach ISO 26262 [LPP10]

Anschließend werden die technischen Anforderungen aus den funktionalen Sicherheitsanforderungen hergeleitet [LPP10]. Dabei richten sich diese Anforderungen vor allem an die Mechanismen zur Entdeckung und Beherrschung von Fehlern im System selbst und in interagierenden Systemen untereinander [LPP10]. Außerdem sollten Anforderungen an die Prozesssicherheit und Fehlerbeherrschungszeit definiert werden.

Bei der Entwicklung des Systementwurfs sollte darauf geachtet werden, dass dieser möglichst verifizierbar ist. Des Weiteren wird in der ISO 26262 Norm die Wiederverwendung von bewährten Architekturen und Methoden ausdrücklich empfohlen [LPP10].

Nachdem Systementwurf erfolgt die Entwicklung von Hardware und Software. Letztere wird in Abschnitt 4.4 näher erläutert.

Im Anschluss an diese Phase werden die zu Beginn des Sicherheitslebenszyklus definierten *items* zu einem Gesamtsystem integriert und getestet. Anschließend erfolgt die Sicherheitsvalidierung und die Beurteilung der Funktionalen Sicherheit bis schließlich das Produkt freigegeben werden kann. Sicherheitsvalidierung und Beurteilung der Funktionalen Sicherheit sind Thema von Abschnitt 4.5.

4.4 Softwareentwicklung

Die ISO 26262 Norm schlägt für die Strukturierung der Softwareentwicklung das in Abbildung 7 dargestellte Phasenmodell vor. Es ist angelehnt an das in der Automobilbranche weit verbreitete V-Modell.

Die zeitliche Abfolge der einzelnen Schritte ist in dieser Grafik durch die roten Pfeile dargestellt. Die Elemente „Systementwurf“ und „Integration und Test der

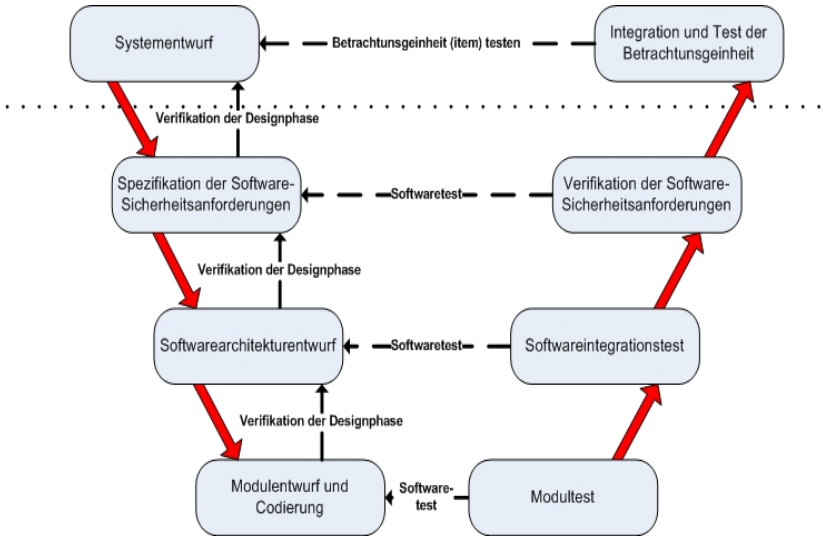

Abb. 7 Phasenmodell für die Softwareentwicklung nach ISO 26262 [LPP10]

Betrachtungseinheit“ gehören nicht zur Phase der Softwareentwicklung und sind daher durch die gestrichelte Linie abgetrennt. Sie sind dennoch in der Grafik dargestellt, um die Einbettung der einzelnen Schritte der Softwareentwicklung in die Entwicklung auf Systemebene besser nachvollziehen zu können.

Die reine Softwareentwicklung beginnt mit der Spezifikation der Softwaresicherheitsanforderungen. Anschließend wird auf Basis dieser Anforderungen der Softwarearchitekturentwurf erstellt. Danach werden die einzelnen Module entworfen und codiert. Während jedem dieser Schritte erfolgt eine Verifikation des Designs, was ggf. bei Unstimmigkeiten im Design zur Folge hat, dass ein vorheriger Schritt wiederholt werden muss.

Nach der Codierung werden die entsprechenden Tests der Software durchgeführt, wobei mit der kleinsten zu testenden Einheit, dem Modultest, begonnen wird. Anschließend erfolgen der Softwareintegrationstest und die Verifikation der Softwaresicherheitsanforderungen. Wird bei einer dieser Überprüfungen ein Fehler detektiert, muss dieser in der jeweils in der Grafik gegenüberliegenden Entwicklungsphase korrigiert werden. Von dort aus werden dann die restlichen Phasen der Softwareentwicklung durchlaufen.

Zu den einzelnen Schritten im Phasenmodell fordert die Norm je nach ASIL-Level einer Komponente die Einhaltung bestimmter Regeln bzw. Verfolgung bestimmter Muster beim Entwurf, der Codierung und dem Testen. So wird zum Beispiel die Initialisierung von Variablen für alle ASIL-Level gefordert, um ein Fehlverhalten aufgrund unbeabsichtigter Werte im Speicher zu verhindern [LPP10]. Des Weiteren wird eine Modularisierung und eine strukturierte Programmierung empfohlen. Ab ASIL-Level B ist außerdem eine defensive Programmierung ratsam [LPP10]. Bei der defensiven Programmierung überprüft ein Programm selbst möglichst viele Voraussetzungen, bevor es seinen eigentlichen Zweck erfüllt, um so auf möglichst alle unterschiedliche Situationen adäquat reagieren zu können.

Für die Dokumentation der Softwarearchitektur werden für ASIL-Level A und B informelle Notationen als ausreichend angesehen. Ab ASIL-Level C ist allerdings mindestens eine semiformale Notation notwendig [LPP10].

Auch für das Testen der Software sind je nach ASIL-Level bestimmte Vorgaben zu beachten. So gilt für die Modultests, dass ab ASIL-Level A mindestens eine Anweisungsüberdeckung erreicht werden muss. Zweigüberdeckung ist ab ASIL-Level B notwendig und für ASIL-Level D wird eine MC/DC-Metrik (Modified Condition/Decision Coverage, Modifizierte Bedingung/Entscheidungsüberdeckung) empfohlen [LPP10]. Für die Gesamtsoftwaretests wird Funktions- und Aufrufüberdeckung ab ASIL-Level C als sinnvoll angesehen. Für vollständige Funktionsüberdeckung muss jede Funktion mindestens einmal aufgerufen werden. Aufrufüberdeckung sagt aus, ob jeder Funktionsaufruf eines Programms einmal ausgeführt wurde.

4.5 Beurteilung der Funktionalen Sicherheit

Die Beurteilung der Funktionalen Sicherheit erfolgt in sogenannten Sicherheitsassessments. Überprüft werden dabei [LPP10]:

- die durchgeführten Tätigkeiten
- die erstellten Arbeitsprodukte
- die benutzten Werkzeuge
- die Erreichung der Ziele und Anforderungen der Norm

Die Überprüfung der erstellten Arbeitsprodukte wird auch als Review bezeichnet. Bestenfalls sollten diese Überprüfungen nicht erst ganz am Ende des Entwicklungsprozesses durchgeführt werden, sondern in möglichst allen Phasen [LPP10].

Das Sicherheitsassessment wird von einem sogenannten Assessor durchgeführt. Dieser sollte nicht nur den Assessmentprozess beherrschen, sondern sich auch mit dem entwickelten System, den dafür notwendigen technischen Voraussetzungen und mit funktionaler Sicherheit allgemein, gut auskennen.

Eine weitere wichtige Anforderung an den Assessor ist, dass dieser möglichst unabhängig ist. Die ISO 26262 Norm definiert insbesondere für die Durchführung von Reviews fünf Stufen I0 bis I4, die jeweils die Notwendigkeit einer Maßnahme und die nötige Unabhängigkeit der durchführenden Person beschreiben. Die niedrigste Stufe I0 gibt an, dass eine Maßnahme durchgeführt werden sollte [LPP10]. Wird eine Maßnahme mit I1 eingestuft, muss sie durchgeführt werden [LPP10]. Ab I2 muss die Maßnahme durchgeführt werden von einer Person aus einem anderen Team, welches nicht den selben Vorgesetzten hat wie das entwickelnde Team [LPP10]. Bei der Einstufung einer Maßnahme in I3 muss diese von einer Person aus einer anderen Abteilung/Organisation durchgeführt werden, die wirtschaftlich unabhängig ist von der entwickelnden Abteilung/Organisation [LPP10].

Die Reviews der Gefährdungs- und Risikoanalysen werden für die Notwendigkeit ihrer Durchführung bzw. der Unabhängigkeit der durchführenden Person unabhängig vom ASIL-Level immer in I3 eingestuft. Für alle Reviews zu Bestandteilen des Systems, die mit ASIL-Level D eingestuft wurden, gelten ebenfalls die strengen Vorschriften der Kategorie I3.

4.6 Umsetzung der Norm mithilfe Modellgetriebener Softwareentwicklung

Die Umsetzung der ISO 26262 Norm mithilfe Modellgetriebener Softwareentwicklung, welche immer stärker in der Automobilindustrie genutzt wird, bietet einige Vorteile.

Es können Code und Testfälle direkt aus dem Modell generiert werden. Dies vereinfacht und verbessert das systematische Testen. Des Weiteren können Inspektion des Designs und des Codes durch Modellverifikationen ersetzt werden. Allgemein macht ein modularer Aufbau die Software überschaubarer und somit leichter verifizierbar [HIRK]. Die Modelle sind gerade für unabhängige Personen, zum Beispiel Reviewer, leichter verständlich [KSF].

Allerdings sind alle diese Vorteile nicht so ohne weiteres immer vollständig ausnutzbar, da auch bei Modellgetriebener Softwareentwicklung häufig an einigen Stellen der Code von Hand nachbearbeitet werden muss. Dadurch kann dann nicht die Inspektion des Codes allein durch Modellverifikation ersetzt werden. Außerdem ist der aus Modellen generierte Code häufig nicht sehr effektiv, was gerade für zeitkritische Anwendungen in elektronischen Systemen im Fahrzeug problematisch sein kann.

5 Probleme/Schwierigkeiten bei der Umsetzung

Ein prinzipielles Problem bei der Umsetzung der Norm ist, dass der in der Softwareentwicklung für die Wiederverwendbarkeit notwendige modulare Aufbau im Konflikt mit der systemweiten Eigenschaft Sicherheit steht [KSF]. Bei der Kombination verschiedener Softwareelemente muss deren Rückwirkungsfreiheit bewiesen werden. Dies bedeutet, dass nicht-sicherheitskritische Elemente die sicherheitskritischen nicht beeinflussen dürfen. Hierfür darf die nicht-sicherheitskritische Software den Speicher der sicherheitskritischen nicht berühren und außerdem nicht mehr Laufzeit benötigen als für sie vorgesehen wurde [WFK]. Auch sicherheitskritische Elemente untereinander müssen rückwirkungsfrei sein. Kann die nötige Unabhängigkeit mehrerer Elemente nicht nachgewiesen werden, hat ein aus mehreren Unterelementen kombiniertes Element das höchste ASIL-Level seiner Unterelemente [SKb].

Eine weitere Schwierigkeit besteht bei der Interpretation der ASIL-Stufen. Gerade bei der Gefährdungs- und Risikoanalyse können viele Einschätzungen strittig sein. Sie hängen häufig stark von dem jeweiligen Umfeld der Entwicklung ab. So wird zum Beispiel das Auftreten der Fahrsituation „Anfahren am Berg“ je nach regionalen Gegebenheiten mal mit niedriger und mal mit hoher Wahrscheinlichkeit eingeschätzt.

Des Weiteren steigt der Entwicklungsaufwand nach der Entscheidung für die Umsetzung der Norm um ca. 3% bis 10% in den ersten Jahren [Sau]. Dies ist vor allem auf den zusätzlichen Dokumentations-, Analyse-, Review- und Auditierungsaufwand zurückzuführen.

Eine Gefahr sehen Experten außerdem in der Überinterpretation der Norm [Sau]. Dies hätte zur Folge, dass der Nachweis der Sicherheit einen höheren Stellenwert als die eigentliche Aufgabe, nämlich die Entwicklung des Systems selbst, einnimmt.

6 Fazit

Durch die Entwicklung der ISO 26262 Norm wurde ein einheitlicher Standard für den Stand von Technik und Wissenschaft geschaffen. Sie lässt für die Automobilindustrie

weniger Interpretationsfragen als die Grundnorm DIN EN 61508 offen, was prinzipiell zu begrüßen ist.

Allerdings bleibt die Akzeptanz der Norm weiterhin fraglich. Vor allem befürchten die Juristen der US-amerikanischen Automobilhersteller, dass auch die Umsetzung der Norm ihnen bei amerikanischen Gerichtsverfahren keinen Vorteil verschaffen wird [LPP10].

Die immer noch angespannte wirtschaftliche Lage vieler Automobilhersteller lässt die Vorteile einer Umsetzung strittig erscheinen. Gerade der am Anfang steigende Entwicklungsaufwand von 3% bis 10% ist unter Umständen nicht von jedem Unternehmen tragbar.

Auch bleibt unklar, wie lange die Norm wirklich als ein gutes Maß für den aktuellen Stand von Wissenschaft und Technik angesehen werden kann, bevor sie selbst wieder veraltet ist.

Literatur

[For] Prof. T. Form. Sicherheit. http://www.ifr.ing.tu-bs.de/lehre/downloads/skripte/Form_alt/form_alt_Folien_FE2_Teil12.pdf, Zugriffsdatum: 24.08.11.

[GS] Karl Greb and Anthony Seely. Design of Microcontrollers for Safety Critical Operation. http://www.ti.com/ww/en/mcu/tms570/downloads/Design_of_Microcontrollers_for_Safety.pdf, Zugriffsdatum: 24.08.2011.

[HG] Chris Hills and Günter Glöe. Preparing for ISO 26262. http://www.phaedsys.org/principals/riskcats/riskdata/PhaedSys%20-%20CATS%20article%20AE%20Aug-Sept%2009.pdf, Zugriffsdatum: 24.08.2011.

[HIRK] Ibrahim Habli, Ireri Ibarra, Roger Rivett, and Tim Kelly. Model-Based Assurance for Justifying Automotive Functional Safety. http://www-users.cs.york.ac.uk/~ihabli/Papers/2010Habli_SAE.pdf, Zugriffsdatum: 24.08.11.

[HMNS] Dipl.-Ing. Josef Horstkötter, Dr. Pierre Metz, Dipl. Inf. (FH) Anastasia Ntima, and Dr. Wolfgang Seim. Funktionale Sicherheit und ISO 26262 - Entmystifiziert. http://www.synspace.com/index2.php?option=com_docman&task=doc_view&gid=60&Itemid=138, Zugriffsdatum: 24.08.2011.

[KSF] Olaf Kath, Rudolf Schreiner, and John Favaro. Safety, Security, and Software Reuse: A Model-Based Approach. http://www.favaro.net/john/RESAFE2009/results/RESAFE2009%20Intecs%20ikv%20object%20security.pdf Zugriffsdatum: 24.08.11.

[LPP10] Peter Löw, Roland Pabst, and Erwin Petry. *Funktionale Sicherheit in der Praxis*. dpunkt Verlag, 2010.

[Roo] Elena Root. Aspekte des Sicherheitsbegriffs in automotiven Anwendungen. http://www.uni-koblenz-landau.de/koblenz/fb4/institute/IST/AGZoebel/Lehre/ss09/Seminar09/root, Zugriffsdatum: 24.08.11, Universität Koblenz.

[Sau] Jürgen Sauler. Interview: Alle Fakten zur neuen Sicherheits-Norm für die Autoindustrie ISO 26262. http://www.elektronikpraxis.vogel.de/index.cfm?pid=906&pk=248663&p=4, Zugriffsdatum: 24.08.11.

[SKa] Jürgen Sauler and Stefan Kriso. ISO 26262 - Die zukünftige Norm zur funktionalen Sicherheit von Straßenfahrzeugen. http://www.elektronikpraxis.vogel.de/index.cfm?pid=904&pk=242243&p=2, Zugriffsdatum: 24.08.2011.

[SKb] Jürgen Sauler and Stefan Kriso. Norm zur funtionalen Sicherheit von Straßenfahrzeugen. http://www.automobil-industrie.vogel.de/elektronik/articles/242475, Zugriffsdatum: 24.08.11.

[WFK] Dr. Thomas Wenzel, Martin Fassl, and Joachim Kalmbach. Entwicklung von Steuergeräte-Basis-Software nach ISO/DIS 26262. http://www.elektroniknet.de/automotive/technik-know-how/sicherheitselektronik/article/31185/2/Entwicklung_von_Steuergeraete-Basis-Software_nach_ISODIS_26262/, Zugriffsdatum: 24.08.11.