Funktionale Sicherheit im Automobil

ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen

Bearbeitet von
Hans-Leo Ross

1. Auflage 2014. Buch. XIV, 280 S.
ISBN 978 3 446 43632 9
Format (B x L): 17,3 x 24,6 cm
Gewicht: 711 g

HANSER

Leseprobe

Hans-Leo Ross

Funktionale Sicherheit im Automobil

ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen

ISBN (Buch): 978-3-446-43632-9

ISBN (E-Book): 978-3-446-43840-8

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-43632-9

sowie im Buchhandel.

2 Warum Funktionssicherheit im Automobil?

Das Thema Funktionssicherheit spielte erst sehr spät im Vergleich zu anderen Branchen eine größere Rolle beim Automobilbau. Mehr Funktionalität, Komplexität von Produkt und Markt waren vom Kunden, den Hersteller und den Händlernetzen gefordert. Ein wesentlicher Grund war auf jeden Fall, dass die gesamte Fahrzeugtechnik doch in erster Linie von Maschinenbauern dominiert wurde. Hier waren natürlich auch die Sicherheitsmechanismen aus diesem Bereich entwickelt worden, ohne dass man sich dabei auf Elektronik und sogar Software verlassen hat. Das heißt, die Sicherheitsmechanismen beruhten in erster Linie auf robustem Design und hydraulischen oder pneumatischen Sicherheitsmechanismen. Mit zunehmender Automatisierung und Elektrifizierung von wesentlichen Fahrzeugfunktionen und dem Wunsch, diese Systeme für höhere Geschwindigkeiten und höhere Dynamik anwendbar zu machen, führte kein Weg mehr an der Elektrifizierung vorbei. Auch die Idee von Steer-by-wire und Brake-by-wire bis hin zum heutigen autonomen oder hochautomatisierten Fahren macht die Nutzung von software-basierenden Sicherheitsmechanismen unumgänglich. Sieht man einen heute üblichen Mittelklassewagen wie den Passat, so hat dieser circa 40 Steuergeräte, die weitgehend auch noch immer an einem CAN-Bus hängen. Man hat erkannt, dass es ohne einen Systemansatz keine komplexen Fahrzeugsysteme geben kann. Eine der wesentlichen Herausforderungen für die ISO 26262 war, dass es viele Methoden unterschiedlichster Ausprägung gab, jedoch keinen einheitlichen Systementwicklungsansatz. Es war die wesentliche Aufgabe bei der Entwicklung der ISO 26262, sich auf ein Grundverständnis zum Systemengineering zu einigen. Daher wird es nicht verwundern, dass in der „Introduction“ das Wort „System Engineering“ mehrfach auftaucht.

2.1 Risiko, Sicherheit und Funktionssicherheit im Automobil

Risiko wird allgemein als ein mögliches Ereignis mit einer negativen Auswirkung beschrieben. Der griechische Wortursprung wird auch für die Gefahr benutzt. Im Sinne der Produktsicherheit spricht man von dem Kreuzprodukt aus Eintrittswahrscheinlichkeit und Gefahr. Über den Begriff und die Definition des Risikos gibt es in der wirtschaftswissenschaftlichen Literatur und Diskussion verschiedene Auffassungen. Die Definitionen reichen von „Gefahr einer Fehlabweichung“ bis zur mathematischen Definition „Risiko = Wahrscheinlichkeit x Ausmaß“. Allgemeine Definition: Die Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens; dies bezieht sich auf Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen. Etymologisch kann man Risiko zum einen auf riza (griechisch = Wurzel, Basis) zurückverfolgen; siehe auch risc (arabisch = Schicksal). Auf der anderen Seite kann Risiko auf ris(i)co (italienisch) zurückverfolgt werden; „die Klippe, die es zu umschiffen gilt“. Sicherheit entstammt dem Lateinischen und könnte frei als ohne Sorge (se cura = ohne Sorge) übersetzt werden.

Sicherheit wird heute in verschiedenen Kontexten betrachtet: wirtschaftliche Sicherheit, Sicherheit der Umwelt, Zutritt- oder Zugriffssicherheit (hier wird im Englischen nicht das Wort „Safety“ sondern der Begriff „Security“ verwendet), aber auch im Bereich Arbeitssicherheit, Anlagen- und Maschinensicherheit und der Fahrzeugsicherheit. Der Begriff Sicherheit grenzt sich signifikant von dem Begriff der Funktionssicherheit ab.

Im Zusammenhang mit technischen Systemen oder Produkten wird Sicherheit als die Freiheit von unakzeptablen Risiken beschrieben. Als Schaden wird allgemein die Verletzung oder die Beeinträchtigung von Personen sowie Umweltschäden gesehen.

Folgende Gefährdungen werden unterschieden:

- chemische Reaktionen von Stoffen, Materialien etc. führen zu Brand, Explosion, Verletzung, gesundheitlicher Beeinträchtigung, Vergiftung, Umweltschäden etc.
- toxische Stoffe führen zu Vergiftung (auch Kohlenmonoxid), Verletzung (Folge durch z. B. Ausgasung von Batterie, Fehlreaktion des Fahrers, Werkstattpersonal), andere Schäden etc.
- hohe Ströme und insbesondere hohe Spannungen führen zu Schäden (insbesondere Personenschutz)
- Strahlungen (nuklear oder auch andere Strahlung (Folge z. B. Alpha-Teilchen in Halbleiter))

- thermisch (Schäden durch Überhitzung, Verbrennung, Brand, Schmoren, Rauch etc.)
- Kinetik (Verformung, Bewegung, beschleunigte Masse kann zu Verletzung führen)

Diese potenziellen Ursachen für Gefährdungen lassen sich nicht eindeutig abgrenzen, da chemische Reaktionen auch zu Vergiftungen, Überhitzung bis zum Brand und somit auch zu Rauchvergiftungen führen können.

Ähnliche Zusammenhänge sieht man bei zu hohen Strömen oder bei überhöhten Spannungen. Hohe Spannungen führen bei Berührung zu Verbrennungen von Personen, sie können aber auch die Ursache von Bränden sein. Die Überspannung wird oft als nicht-funktionales Risiko oder Gefahr gesehen. Daher wird in den meisten Standards solchen Gefahren durch Designvorgaben begegnet. Der Berührungsschutz an unserem Schutzkontaktstecker ist ein typisches Beispiel dazu.

Dies führt auch zu folgender Sicht und Abgrenzung zur Funktionalen Sicherheit.

Die Funktionssicherheit wird allgemein als eine korrekte technische Reaktion eines technischen Systems in einem definierten Umfeld, bei gegebener definierter Stimulation am Eingang des technischen Systems umschrieben. In der ISO 26262 wird Funktionssicherheit definiert als Freiheit von unakzeptablen Risiken basierend auf Gefahren, die durch Fehlfunktionen von E/E-Systemen verursacht werden. Hier werden in mechatronischen Systemen auch die Fehlfunktionen der mechanischen oder hydraulischen Systemkomponenten mit elektronischen Sicherheitsmechanismen zu beherrschen sein. Diese Abgrenzung wird später in Bezug auf den Scope der ISO 26262 diskutiert.

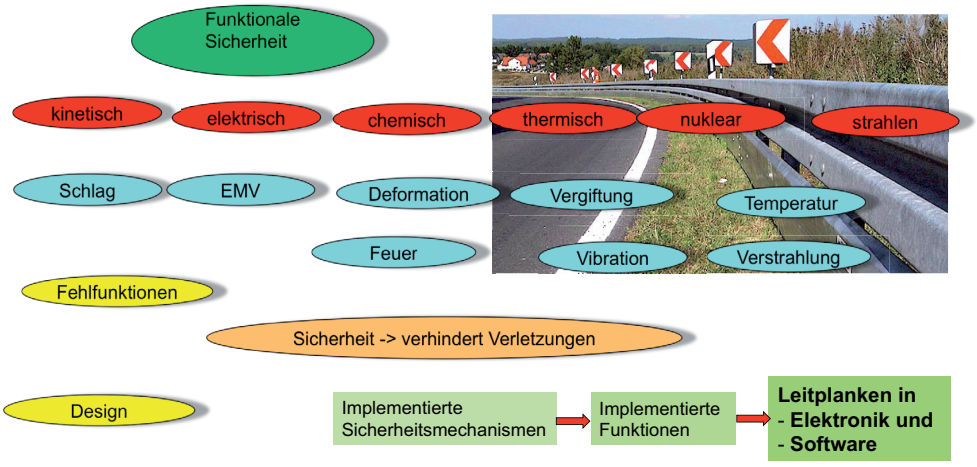

Bild 2.1 Funktionssicherheit und sicheres Design

Gerade beim Automobil hat man funktionale Absicherungen mit hydraulischen Systemen schon immer angewendet. Ein typisches Beispiel war hier das Zweikreisbremssystem oder die hydraulische Lenkung. Elektronische und softwarebasierende funktionale Sicherheitsmaßnahmen wurden erst im Wesentlichen mit ABS bei Bremssystemen vor 30 Jahren eingeführt. Vorher versuchte man allgemein durch hinreichend robuste System- und Komponentenauslegung (also durch das Design) die notwendige Sicherheit zu gewährleisten.

Folgende Definitionen zu Risiko, Gefahr und der Integrität wurden in der DIN EN 61508-1 (VDE 0803 Teil 1):2002-11 ergänzt:

A.5 Risiko und Sicherheitsintegrität

Es ist wichtig, dass die Unterscheidung zwischen Risiko und Sicherheitsintegrität vollständig erkannt wird.

Risiko ist ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten auftretenden gefahrbringenden Vorfalls. Es kann für unterschiedliche Situationen ausgewertet werden (EUC-Risiko, notwendiges Risiko, um das tolerierbare Risiko zu erreichen, tatsächliches Risiko (siehe Bild A.1)). Das tolerierbare Risiko wird auf gesellschaftlicher Basis bestimmt und berücksichtigt gesellschaftliche und politische Faktoren. Die Sicherheitsintegrität bezieht sich nur auf die sicherheitsbezogenen E/E/PE-Systeme, sicherheitsbezogene Systeme anderer Technologie und externe Einrichtungen zur Risikominderung. Die Sicherheitsintegrität ist ein Maß für die Wahrscheinlichkeit dieser Systeme/Einrichtungen, die notwendige Risikominderung in Bezug auf die festgelegten Sicherheitsfunktionen zufrieden stellend zu erreichen. Sobald das tolerierbare Risiko festgelegt und die notwendige Risikominderung bestimmt worden ist, können die Anforderungen zur Sicherheitsintegrität für die sicherheitsbezogenen Systeme zugeordnet werden (siehe 7.4, 7.5 und 7.6 der IEC 61508-1).

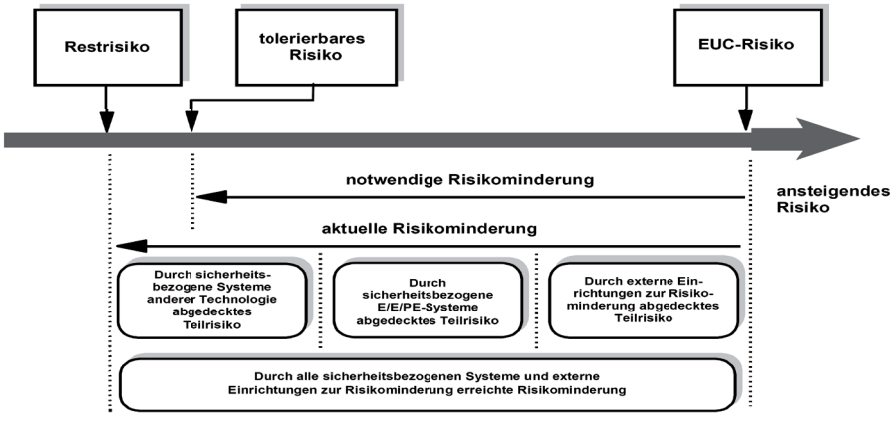

Bild 2.2 Risikominimierung gemäß IEC 61508 (Quelle: DIN EN 61508-1 (VDE 0803 Teil 1):2002-11)

Weiter zeigt die IEC 61508 folgende Darstellungen zu den Zusammenhängen:

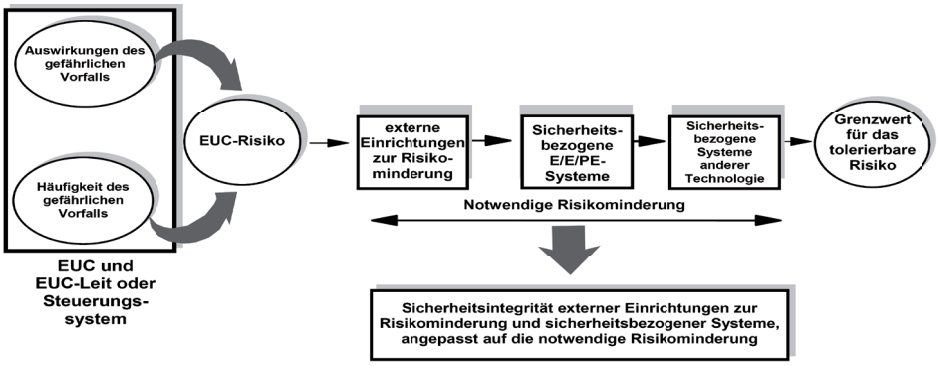

Bild 2.3 Risiko- und Sicherheitsintegrität gemäß IEC61508 (Quelle: DIN EN 61508-1 (VDE 0803 Teil 1):2002-11)

In der ISO 26262 wurde der Bezug zwischen Risiko, Gefahr und Sicherheitsintegrität anders definiert. Der Begriff der Sicherheitsintegrität wird in der ISO 26262 nicht direkt verwendet. Besonders der Begriff EUC (Equipment under Control) wurde nicht verwendet. EUC würde man mit dem „Gerät oder System welches sicherheitstechnisch beherrscht werden soll“ beschreiben. Die ISO 26262 lässt unter bestimmten Randbedingungen auch zu, dass die gewünschte Fahrzeugfunktion selbst sicherheitstechnisch ausprägt werden kann. In dem Fall, enthält das System keine Sicherheit durch das EUC selbst. Formal muss ja gemäß IEC 61508 das EUC und die Sicherheitsfunktionen einen Fehler zur gleichen Zeit verursachen, damit eine gefahrbringende Fehlerfolge entsteht. Wäre zum Beispiel ein hydraulisches Bremsensystem das EUC, welches in seiner Funktionen durch ein EE-System überwacht wird, dann könnten Fehler des hydraulischen Bremsensystems durch das EE-System abgewendet werden. In der Automobiltechnik nimmt dann meist von den mechanischen oder Systemen in anderer Technologie Kredit als „sichere“ Rückfallebene.

Wie bereits oben beschrieben, definiert die ISO 26262 die Funktionale Sicherheit als Freiheit von unakzeptablen Risiken basierend auf Gefahren, die durch Fehlfunktionen von E/E-Systemen verursacht werden. Jedoch werden auch Interaktionen von Systemen mit E/E-Funktionen eingeschlossen, somit wären mechatronische Systeme eingeschlossen. Ob rein mechanische Systeme in heutigen Automobilen wirklich keine Interaktion mit E/E zeigen, ist wohl zweifelhaft. Weiter schließt der Scope der ISO 26262 (einleitendes Kapitel, welches den Umfang der Norm beschreibt) wieder Gefährdungen wie elektrischer Schlag, Feuer, Rauch, Hitze, Strahlung, Vergiftung, Entflammung, (chemische) Reaktion, Korrosion, Freiwerden von Energie oder vergleichbare Gefahren aus, solange sie nicht durch Fehlfunktionen von elektrischen

Komponenten verursacht sind. Hier wird man wohl schnell die Batterie sehen, aber auch die giftigen Elektrolyte in Kondensatoren. Weiter kann man diskutieren, ob eine Motorwicklung eine elektrische Spule ist oder eine mechanische Komponente. Allgemein wird es schwer, bei nicht-funktionalen Gefahren tatsächlich den ASIL zu bestimmen. Grundsätzlich wurden bisher solche Komponenten hinreichend robust ausgelegt, so dass eine Gefährdung vermieden werden konnte. Im Rahmen der Gefahren- und Risikoanalyse ist es sehr schwer einer Design- oder Auslegungsschwäche einen ASIL zuzuordnen.

Der Scope der ISO 26262 schließt auch die funktionale Performance aus. Das heißt Funktionen, die bei korrekter Funktion bereits eine Gefährdung darstellen, werden allgemein durch die Gebrauchssicherheit vorab schon ausgeschlossen.

Die ISO 26262, Teil 3, Anhang B9 beschreibt die Zusammenhänge zwischen Risiko und Schaden wie folgt:

Ein Risiko (R = Risk) kann grundsätzlich als Kombination der Häufigkeit (f = frequency), mit der ein gefährlicher Vorfall auftritt, und dem möglichen Ausmaß des Schadens (S = Severity) beschrieben werden:

$R = f \cdot S$

Die Auftretenshäufigkeit (f) wird wiederum durch mehrere Parameter beeinflusst:

Da ist zum einen die Wahrscheinlichkeit, mit der das später realisierte System selbst ein gefährliches Ereignis bewirkt. Dieser Parameter ist gekennzeichnet durch unerkannte zufällige Fehler der Systemkomponenten und durch gefährliche systematische Fehler, die im System verblieben sind. Da eine Entwicklung gemäß dieser Norm solche Fehler vermeiden soll, ergibt sich dieser Parameter als Mindestforderung an das fertige System (Probability of dangerous failure). Er bleibt bei der Risikobestimmung deshalb zunächst außer Betracht.

Zum anderen ist die Dauer und Häufigkeit zu berücksichtigen, in der sich Personen in einer Situation befinden, in der die o. g. Gefahren gegeben sind (E = Exposure).

Nicht zuletzt, ist die Abwendbarkeit von Schäden durch rechtzeitige Reaktionen von beteiligten Personen (C = Controllability) mitentscheidend für den Eintritt eines Unfalls.

$f = E \cdot C$

Das (Kreuz-)Produkt E*C stellt einen Wert für die Auftretenswahrscheinlichkeit oder -häufung der äußeren Umstände dar, unter denen ein Fehler ein entsprechendes Potenzial für das angegebene Schadensausmaß besitzt.

Die ISO 26262 beschreibt eine normative Methode, nach der eine systematische Ableitung des potentiellen Risikos, das von der zu untersuchenden Betrachtungseinheit

(Item, Fahrzeugsystem) ausgehen könnte, auf Basis einer Gefahren- und Risikoanalyse durchgeführt werden kann. In anderen Sicherheitsstandards wird die Gefahren- oder Risikoanalyse nicht normative vorgegeben. Die Methoden werden nur beispielhaft beschrieben oder es werden Anforderungen an die Methoden formuliert.

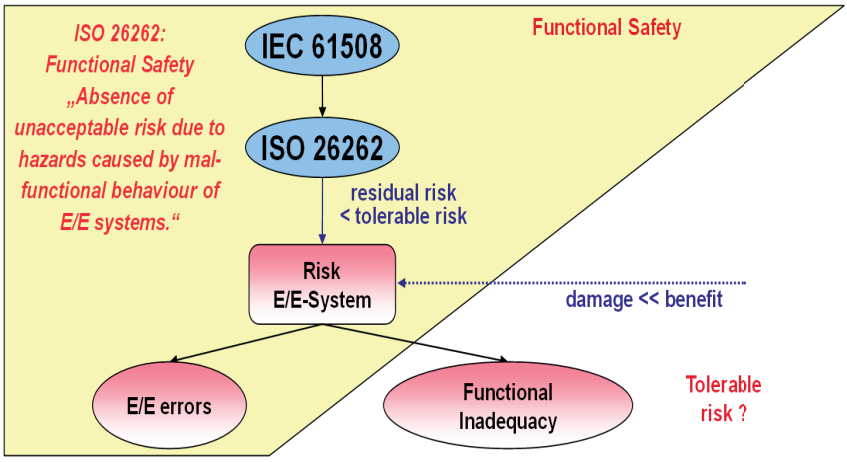

Bild 2.4 Abgrenzung zu Gefahren, basierend auf korrekt funktionierenden Systemen (Quelle: nicht realisiertes Forschungsprojekt)

Insbesondere wenn eine Funktion nicht geeignet ist beziehungsweise für bestimmte sicherheitsrelevante Funktionen falsch beschrieben ist, wird mit den in der ISO 26262 beschriebenen Aktivitäten und Methoden die notwendige Risikominimierung nicht erzielt werden können. Dies ist eine besondere Herausforderung, da die ISO 26262 weder das EUC (System, Maschine oder Gerät welches sicherheitstechnisch beherrscht werden soll) noch den Unterschied zwischen Sicherheitsfunktionen auf Anforderung (low demand) oder kontinuierlicher (high demand) Absicherung betrachtet. Woher leitet man ab, ob eine Reaktion des Fahrzeugsystems oder eine Messung (oder Ermittlung von Gefahrensituationen oder Objekten etc.) hinreichend, tolerierbar oder sicherheitstechnisch angemessen ist?

2.2 Qualitätsmanagementsystem

Prof. Dr. rer. nat. Dr. oec. h. c. Dr.-Ing. E. h. Walter Masing gilt als der Vater der Qualitätsmanagementsysteme, auf jeden Fall hier in Deutschland. Sein Standardwerk „Masing Handbuch Qualitätsmanagement“ hat die Normierung und die Interpretation