März 2013
1. Jahrg.
84364
Seite 1–56

InTeR

Zeitschrift zum Innovations- und Technikrecht

1

Deutscher Fachverlag GmbH · Frankfurt am Main

RAuN Dr. Ekkehard Helmig

ISO 26262 – Funktionale Sicherheit in Personenfahrzeugen: Zur Verantwortlichkeit der Funktionalen Sicherheitsmanager

Nach dem auf funktionale Fahrzeugsicherheit zielenden Konzept der Ende 2011 in Kraft getretenen Norm ISO 26262 zur funktionalen Sicherheit von Fahrzeugsystemen übernehmen „Functional Safety Manager" (FSM) für ihr Unternehmen und persönlich Verantwortlichkeiten für die Übereinstimmung eines funktionalen elektrischen und/oder elektronischen Sicherheitssystems wie Airbags, Fahrassistenzsysteme oder Fahrspurhaltesysteme mit den Forderungen der ISO 26262. Die Sicherheitsnorm wird in der Automobilindustrie als Stand der Technik und als Standard angesehen. Der vorliegende Beitrag bietet einen Überblick über die Norm und damit verbundenen Haftungsrisiken für FSM.

I.

Zur Einführung in die ISO 26262: Die Norm „Functional Safety – Road vehicles"[1] systematisiert prozessorientiert[2] die Kompetenzen eines Unternehmens für die Konzeption, die Entwicklung und die Produktion elektrischer und/oder elektronischer Systeme unter Beachtung gesetzlicher, in der Norm aber nicht spezifizierter Sicherheitsvorschriften. Sie vermittelt als technische Norm zugleich Vorgaben für rechtliche Verhaltensanforderungen an die Produzenten und ist damit ein Klassiker für die zunehmenden Synergien zwischen Recht und Technik. Technisch ausgedrückt: Technische Normen und rechtliche Vorschriften sind hybride Quellen für die technische und rechtliche Bewertung valider Sicherheitssysteme. Normen und Rechtsvorschriften können in diesem Zusammenhang nur interdisziplinär verstanden werden. Die Norm ist daher stets komplementärer Auslegungsmaßstab für die vertrags- und haftungsrechtliche Beurteilung technischer Produkte, weil der Gesetzgeber nur die Forderung nach sicheren Produkten stellt, sie aber nicht im Detail vorgibt und auch nicht vorgeben kann, wie die Sicherheit technisch zu gewährleisten ist.[3] Trotz der Herkunft der Normen aus privatrechtlichen Organisationen „herrscht aufgrund der praktischen Bedeutung und Verbreitung der Normen faktisch ein Befolgungszwang".[4]

II.

1. Auch wenn es eine absolute Sicherheit technischer Produkte nicht gibt,[5] verlangt der Bundesgerichtshof (BGH) in ständiger Rechtsprechung vom Hersteller eines technischen Produkts schon in der Konzeptions- und in der Konstruktionsphase all „diejenigen Maßnahmen zu treffen, die zur Vermeidung einer Gefahr objektiv erforderlich und nach objektiven Maßstäben zumutbar sind". Erforderlich „sind die Sicherheitsmaßnahmen, die nach dem im Zeitpunkt des Inverkehrbringens des Produkts vorhandenen neuesten Stand der Wissenschaft und Technik konstruktiv möglich sind".[6]

Der vom BGH in dieser Entscheidung geprägte „Begriff des technisch Möglichen"[7] bezieht sich auf die Umsetzung aller technischen und wirtschaftlich zumutbaren Möglichkeiten, ein Höchstmaß an Sicherheit zu gewährleisten und nicht darauf, alles, was möglich ist, unbesehen von Risiken auch in den Verkehr zu bringen. Die Anwendung von Technik muss sich an rechtlichen Maßstäben messen lassen.

2. In der Automobilindustrie wird versucht, diese Forderung unter Berufung auf „Branchenüblichkeit" zu relativieren. Daraus folgt, zunehmend das technisch Mögliche vornehmlich verkaufsfördernd anzupreisen, ohne dabei nach außen erkennbar die Priorität auf die Vermeidung nicht entfernt liegender Risiken zu richten, die der von der ISO 26262 geforderte Sicherheitskultur („safety culture"[8]) entspricht. Fahrzeuge mit komplexen elektrischen und elektronischen Systemen, entwickelt und hergestellt in einer vielschichtigen Wertschöpfungskette von Zulieferern unterschiedlicher Qualifikation wie Airbags oder Fahrassistenzsystemen sind, obwohl die Einzelsysteme der Sicherheit des Fahrzeugs dienen können, nicht zwangsläufig sicher. Sie sind den Risiken von Fehlfunktionen vor allem dann ausgesetzt, wenn sie etwa dem Trend zum „vernetzten Fahrzeug"[9] folgend über Internetverbindungen oder Infotainmentsysteme (z. B. iphone, ipad, MP3-Player), die nicht spezifisch für ein Fahrzeug entwickelt wurden, funktionswidrig angesprochen werden können. Fehlfunktionen durch nicht erkannte Einflüsse aus unverträglicher Software oder Hackerangriffen von Außen sind zunehmend an

1 Die umfangreiche (mehr als 370 Seiten) nur in englischer Sprache vorliegende Norm wurde von der International Organization for Standardization (ISO) unter wesentlicher Teilnahme führender Fahrzeughersteller und Systemlieferanten ausgearbeitet. Schon vor ihrem Inkrafttreten wurde sie von Fahrzeugherstellern als Vertragsbestandteil der Entwicklung und Herstellung sicherheitsrelevanter elektrischer und elektronischer Systeme zugrunde gelegt; vgl. dazu *Helmig,* Fahrzeugsicherheit versus Fahrerverunsicherung – Kritische Überlegungen zur KVV und zur ISO 26262, PHi 2010, 194 ff.; *Helmig,* Funktionale Sicherheit nach ISO 26262 und Produkthaftung für No-trouble-found-Fälle, PHi 2012, 32 ff.

2 Der Begriff „Prozess" wird in diesem Aufsatz technisch verstanden. Er richtet sich nach der Definition aus der DIN EN ISO 9000:2005: „Prozess: Satz von in Wechselbeziehung oder Wechselwirkung stehender Tätigkeiten, der Eingaben in Ergebnisse umwandelt."

3 Die Regeln der Wirtschaftskommission für Europa der Vereinten Nationen (Economic Commission for Europe – UNECE) aufgrund des Übereinkommen(s) über die Annahme einheitlicher technischer Vorschriften für Radfahrzeuge, Ausrüstungsgegenstände und Teile, die in Radfahrzeuge(n) eingebaut und/oder verwendet werden können, und die Bedingungen für die gegenseitige Anerkennung von Genehmigungen, die nach diesen Vorschriften erteilt wurden vom 20.3.1958, geändert am 16.10.1995 sind zunächst nur Empfehlungen an die 47 Mitgliedsstaaten und die 27 EU-Länder, die in jeweils nationales Recht übernommen wurden (derzeit etwa 126 Regeln). Sie sind meist bauteilbezogen. Sie widerspiegeln – von Problemen ihrer gesetzgeberischen Legitimation ganz abgesehen – keine allgemeingültigen Sicherheitsanforderungen.

4 *Ensthaler/Müller/Synnatzschke,* Technologie- und technikorientiertes Unternehmensrecht, BB 2008, 2638, 2641.

5 Die ISO 26262 (10-5.3.1) stellt dies ausdrücklich klar: „Given that absolute safety is an unobtainable goal, safety cases can demonstrate that the system is free of unreasonable risk." Der Begriff „unreasonable risk" wird in der Norm (1.136) definiert als: „Risk judged to be unacceptable in a certain context according to valid societal moral concepts."

6 BGH, 16.6.2009 – VI ZR 107/08, VersR 2009, 1125 – Airbag, Rn. 15 und 16.

7 BGH, 16.6.2009 – VI ZR 107/08, VersR 2009, 1125 – Airbag, Rn. 20 a. E., m. w. N.

8 ISO 26262-1:2011-1.107; ISO 26262-2:2011–Annex B.

9 ADAC Motorwelt, Heft 8, August 2012, S. 20.

der Tagesordnung.[10] In den USA wird offen über diese „new vulnerability", die „neue Verletzlichkeit", mit bereits dagegen eingeleiteten Maßnahmen der amerikanischen Straßenaufsichtsbehörden National Highway Traffic Safety Administration (NHTSA) diskutiert.[11] Dieser Branchenüblichkeit, die nicht selten hinter dem zur Gefahrenvermeidung Möglichen zurückbleibt, schiebt die Rechtsprechung des BGH einen klaren Riegel vor. Technik, die dem Ingenieur einleuchtend ist, muss es nicht auch für den Verbraucher sein.[12]

III.

Die Systematik der ISO 26262 kann an dieser Stelle nur kurz beschreiben werden:

1. Die der funktionalen Sicherheit für Fahrzeugsysteme gewidmeten ISO 26262 erfasst[13] den ganzen Lebenszyklus („safety lifecycle")[14] elektrischer und elektronischer Sicherheitssysteme für Fahrzeuge und soll damit dem Ziel der Gefahrenvermeidung dienen. Der Sicherheitslebenszyklus erfasst alle Sicherheitsaktivitäten während der Konzeptphase, der Entwicklungsphase, der Produktion, des Betriebs, des Services und der Entsorgung.[15] Allerdings erhebt die Norm als Rahmenwerk auch den Anspruch, Vorlage für sicherheitsrelevante Systeme sein zu können, die auf anderen Technologien beruhen.

Mit dem Trend der wachsenden technologischen Komplexität, Softwareanwendungen und Implementierung mechatronischer Bauteile, so die Einführung der Norm, steigen die Risiken aufgrund von systematischen Ausfällen („systematic failures"[16]) und von Zufallsausfällen („random hardware failures"[17]) der Hardware. Zielsetzung der Norm ist die Beherrschung der Komplexität und die Reduzierung von Restrisiken („residual risks") einschließlich der Gefährdungspotenziale („hazards"[18]) für Leib und Leben („harms"[19]) daraus für die Gewährleistung der funktionalen Sicherheit eines Systems. Denn, so die Norm, die Sicherheit des Fahrzeugs hängt von dem Verhalten der Kontrollsysteme selbst ab[20] und nicht vom Fahrzeug: Der Airbag erfüllt nur seine Funktion für die Fahrzeugsicherheit („functional safety"), wenn er nur im Falle eines Zusammenstoßes auslöst. Ein solcher Fall liegt der zitierten Airbag-Entscheidung des BGH zugrunde. Derzeit allerdings häufen sich die Rückrufe wegen fehlerhaft auslösender Airbags.[21]

Die ISO 26262 formuliert ein Konzept von Sicherheitszielen („concept of safety goals")[22] und ein Sicherheitskonzept („functional safety concept"[23]) für ein bestimmtes Sicherheitsziel in einer hierarchischen Rangfolge: (i) Eine Gefährdungsanalyse und eine Risikobewertung identifizieren Gefährdungspotenziale, deren Risiko reduziert werden soll; (ii) für jedes in Betracht gezogene Gefährdungsereignis wird ein Sicherheitsziel formuliert; (iii) jedem Sicherheitsziel wird ein Integritätslevel zugeordnet (Automotive Safety Integrity Level – ASIL[24]); (iv) ein Konzept für die funktionale Sicherheit beschreibt die Funktionalität des Systems zur Erreichung des Sicherheitsziels; (v) das technische Sicherheitskonzept beschreibt, wie die Funktionalität aus dem Konzept für die funktionale Sicherheit in Hardware und Software implementiert wird; (vi) Sicherheitsanforderungen an die Software und an die Hardware beschreiben die besonderen Sicherheitsanforderungen, die als Bestandteile des Software- und des Hardwaredesigns eingefügt werden, gemessen an der Sicherheitsfunktionalität im ganzen Fahrzeug.

Alle Prozesse und Maßnahmen innerhalb und zwischen den Stufen dieser Rangfolge unterliegen einer laufenden dokumentierten Erfüllungsüberprüfung in aufsteigender Wertigkeit („Confirmation Measures"[25]): Das „confirmation review"[26] prüft die Übereinstimmung von bestimmten Arbeitsergebnissen („work products") innerhalb eines definierten Konzept-, Entwicklungs- oder Produktionsprozesses auf der Ebene eines Zulieferers oder in der Wertschöpfungskette zwischen den Zulieferern oder final beim Fahrzeughersteller.[27] Das „functional safety audit" bewertet die Implementierung von Prozessen, die für alle funktionalen Sicherheitsaktivitäten gefordert sind. Das „functional safety assessment" bewertet die funktionale Sicherheit, die von dem System auf Systemebene erreicht wird.[28]

2. Was nach einer perfekten, lückenlosen und sich selbst überwachenden Prozessstrenge aussieht, deren Ergebnis die Festlegung des ASIL ist, kann zu Missverständnissen Anlass geben und birgt deshalb Haftungsrisiken: Funktionale Sicherheit eines Systems im Verständnis der ISO 26262 ist keine Produkteigenschaft des Systems in dem Sinne, dass es im Fahrzeug auch funktioniert. Es ist nur grundsätzlich und konzeptionell geeignet, Sicherheitsfunktionen auch im Fahrzeug zu erfüllen, wenn es nach den Prozessen der

10 Das „Center for Automotive Embedded Systems Security" (CAESS) hat in einer umfassenden Studie „Comprehensive Experimental Analyses of Automotive Attack Surface" die Anfälligkeit elektronischer Systeme empirisch nachgewiesen, http://www.autosec.org/publications.html. Handelsblatt-online vom 26.7.2012 „Hacker greifen nach dem Steuer".

11 Automotive News 20.9.2011, S. 11: „War with computer hackers hits the road".

12 Die Automotive News kommentierte in der Ausgabe vom 6.8.2012: „Technology in automobiles is a great thing. But what is intuitive to the electronics engineers might not be intuitive to the customer".

13 ISO 26262-1:2011-1.97.

14 Der Lebenszyklus eines Systems erfasst nach der ISO 26262 die Konzeptphase, die Entwicklungsphase, die Produktionsphase, die Wartung und die Entsorgung eines Sicherheitssystems.

15 ISO 26262-2:2011-5.2.1.

16 ISO 26262-1:2011-1.130.

17 ISO 26262-1:2011-1.92.

18 ISO 26262-1:2011-1.57.

19 ISO 26262-1:2011-1.56; ISO 26262-1:2011-1.59.

20 ISO 26262-10:2011-4.1 lit. b).

21 http://www.auto-motor-und-sport.de/news/honda-airbag-rueckruf-1735547.html; http://www.auto-motor-und-sport.de/news/toyota-us-rueckruf-gelaendewagen-wegen-airbag-problemen-3675501.html; http://www.auto-motor-und-sport.de/news/ford-us-rueckruf-1-2-mio-pickups-mit-airbag-problem-3657395.html; http://www.autobild.de/artikel/rueckruf-honda-japan-usa-kanada-1124962.html; Allein Chrysler musste im November 2012 fast 745.000 Fahrzeuge wegen defekter Airbags zurückrufen: http://www-odi.nhtsa.dot.gov/recalls/latestRecalls.cfm: „Chrysler is recalling certain model year 2002 and 2003 Jeep Liberty vehicles manufactured January 9, 2001, through March 28, 2003, and 2002 through 2004 Jeep Grand Cherokee vehicles manufactured February 13, 2001, through May 23, 2003. A component in the air bag control module may fail causing the front airbags, side curtain airbags, and/or seatbelt pretensioners to deploy inadvertently while the vehicle is being operated."

22 Sicherheitsziele sind die höchsten Sicherheitsanforderungen an ein Sicherheitssystem (ISO 26262:-10:2012-6.5.1). Sie werden schon in der Konzeptphase festgelegt.

23 ISO 26262-3:2011-7.4.8 und 8.

24 ISO 26262-3:2011-7; ISO 26262-8:2011-4.3. Die Norm definiert fünf ASIL: Den QM-ASIL als niedrigste Stufe, ASIL A, ASIL B, ASIL C und ASIL D als den höchsten sicherheitsrelevanten Level.

25 ISO 26262-1:2011-1.17 und ISO 26262-2:2011-6.

26 ISO 26262-1:2011-1.18.

27 Die Feststellung, ob ein Zwischen- oder Endprodukt den vereinbarten Spezifikationen entspricht, wird im Rahmen von Prozessen der „Verifizierung" (ISO 9000:2005-3.8.4) getroffen. Die Feststellung, ob ein Zwischen- oder Endprodukt den Anforderungen in der nächst höheren Wertschöpfungskette entspricht, wird in den Prozessen der „Validierung" (ISO 9000:2005-3.8.5) getroffen.

28 ISO 26262-2:2011-6.2; ISO 26262-10:2012-5.2.2.

Norm konzipiert, entwickelt und hergestellt wurde. Die Umgebungsbedingungen aus dem Fahrzeug (z. B. Vibrationen, Temperatur, Feuchtigkeit, elektro-magnetische Einflüsse etc.) oder der Verkehrslage finden in der Norm ausdrücklich keine Berücksichtigung.[29] Funktionale Sicherheit ist daher nur eine eng definierte Systemeigenschaft, die durch die Methoden und Instrumente der funktionalen Sicherheitsbewertung (z. B. Kompatibilität unterschiedlicher Software im System[30]) nach den Maßstäben der Norm beurteilt werden kann: Der Airbag soll beim Aufprall auslösen. Dass er diese Anforderung wirklich erfüllt, nach der Norm also seine „performance" demonstriert, ist nicht Gegenstand der Norm.[31] Es gibt also wegen dieser Selbstbeschränkung der Norm keine Gleichung: Funktionale Sicherheit = Sicherheit des Fahrzeugs.

3. Die Beurteilungen, ob ein Gefährdungsereignis („hazardous event"[32]) im oder durch den Fahrzeugbetrieb besteht, seiner Folgenschwere („severity"[33]), seiner Eintrittswahrscheinlichkeit („probability of exposure")[34] und die Kontrollierbarkeit („controllability"[35]) der Gefährdungsereignisses durch den Fahrer und/oder andere gefährdete Personen (z. B. Fußgänger) beruht auf selektierten Annahmen und Wertungen. Die selektierten Annahmen sind im Sinne der Forderungen des BGH notwendig subjektiv und willkürlich. Sie können in Bezug auf das jeweilige Sicherheitsziel für den Schutz des Fahrers richtig oder falsch oder unvollständig sein, die daraus gezogene Wertung für daraus abgeleitete Sicherheitsmaßnahmen muss entsprechend ungewiss sein. Die Norm geht zum Beispiel von einem „repräsentativen Fahrer" aus, von dem angenommen wird, dass der nicht müde ist, über eine durchschnittliche Fahrpraxis in einer nicht gerade verkehrsarmen Gegend verfügt, die Verkehrsregeln beherrscht und Rücksicht auf andere Verkehrsteilnehmer nimmt.

a) Die vom Systemtechniker definierten Annahmen des möglichen Verhaltens des Fahrers in einem ebenfalls systemspezifisch, aber willkürlich, angenommenen Gefährdungsereignis gehen bereits in der Konzeptphase des Sicherheitssystems in die Annahmen für die grundlegende Gefährdungsanalyse und Risikobewertung („hazard analysis and risk assessment") ein,[36] die durchgeführt wird, um das Risiko zu identifizieren und die Sicherheitsziele für dieses spezifische Risiko zu definieren. Reaktionsweisen von äußeren Verkehrsumständen oder von Ausfällen oder Fehlfunktionen von Sicherheitssystemen (durch einen Reifenschaden fällt der Reifendrucksensor aus mit unmittelbarer Auswirkung auf andere Motorsteuerungsfunktionen) lassen sich nur bedingt vorhersehen. Entsprechend ungenau sind unvermeidlich die Wertungen daraus und die darauf gestützten Entscheidungen über die finale Auslegung eines Sicherheitssystems. Studien zeigen, dass das Fahrerverhalten und die Einstellungen von Fahrern zu Sicherheitssystemen völlig unterschiedlich sind und sichere Prognosen erst nach weiteren Erfahrungswerten mit sich etablierenden Sicherheitssystemen möglich sind.[37] Die Norm sieht keine Systematik oder Prozessorientierung an den Forderungen der Rechtsprechung vor, die Ansprüche nach dem neuesten Stand der Wissenschaft etwa der auf den Fahrer bezogenen Verhaltens- und Unfallforschung auf den neuesten Stand der Technik anzuwenden, obwohl nur dadurch ein konsistentes Sicherheitskonzept gestaltet werden kann.

b) Unvermeidliche Fehler der Annahmen und der daraus getroffenen Wertungen für die Systemrealisierung über den gesamten Sicherheitslebenszyklus lassen sich in dem „confirmation review", dem „functional safety audit" oder dem „functional assessment" nicht vollständig eliminieren, weil sich die Annahmen etwa über das angenommene Verhalten des Fahrers in diesen Prüfungsprozessen weder bestätigen noch widerlegen lassen. Es verbleibt notwendig ein Restrisiko („residual risk"), in das zusätzliche unvermeidliche Fehler von Software und Hardware eingehen. Ein Unternehmen, das sich für seine Produkte auf die Einhaltung der technischen Vorgaben der ISO 26262 beruft, kann damit nicht sagen, dass es auch ein absolut sicheres Produkt in den Markt gibt. Es muss deshalb auf das Restrisiko aufmerksam machen. Die Risikobeschreibung muss so umfassend sein, dass der Fahrer das Risiko erkennt, versteht, damit umgehen und entscheiden kann, wie er es für sich und andere Verkehrsteilnehmer vermeiden kann.[38]

IV.

Diese Systemfehler lassen sich auch nicht durch die kategorische Forderung der ISO 26262 nach einem „Competence Management"[39] vermeiden: „Die Organisation muss sicherstellen, dass Personen, die in die Durchführung des Sicherheitslebenszyklus einbezogen sind, über hinreichende Fertigkeiten, Kompetenzen und Qualifikationen entsprechend ihren Verantwortlichkeiten verfügen" und auch die Autorität haben, sich durchzusetzen.[40] Verantwortliche Personen sind der Projektmanager,[41] der Safety Manager,[42] der Verantwortliche für das „functional safety audit",[43] der Verantwortliche für die funktionale Sicherheitsbewertung,[44] sowie der Verantwortliche für die Aufrechterhaltung der funktionalen Sicherheit des Systems nach der Pro-

29 ISO 26262-2:2011-1.
30 "Freedom of interference".
31 ISO 26262-2:2011-6.4.5.6.
32 ISO 26262-1:2011-1.59.
33 ISO 26262-1:2011-1.120.
34 ISO 26262-3:2011-7.
35 Controllability ist nach der ISO 26262-1:2011-1.20 die Fähigkeit, bestimmte Gefährdungen oder Schäden durch rechtzeitige Reaktion der betroffenen Person zu vermeiden. Sie beruht auf einer Einschätzung der Wahrscheinlichkeit, dass der Fahrer oder andere Verkehrsteilnehmer in der Lage sind, die Verletzungsgefahr zu vermeiden (ISO 26262-10:2012-6.3). Die Annahme in Hinblick auf die Kontrollierbarkeit in der Gefahrenanalyse und der Risikobewertung werden in der Sicherheitsvalidierung bewertet (ISO 26262-4:2011-9).
36 Für die Beurteilung eines Sicherheitssystems nach dem „neuesten Stand von Wissenschaft und Technik" im Sinne der Airbag-Entscheidung ergeben sich daraus neue Überlegungen: Für die Beurteilung schon in der Konzeptionsphase, ob ein Produkt dem neuesten Stand von Wissenschaft und Technik entspricht, kommt es nicht allein auf die technischen Aspekte an. Wenn die Sicherheit eines Produkts oder der Umgang mit ihm wesentlich von menschlichen Faktoren wie das antizipierte Fahrerverhalten abhängt, ist dem Maßstab „neuester Stand von Wissenschaft und Technik" nur genügt, wenn interdisziplinär etwa auch die Fahrerpsychologie und Erkenntnisse aus der Unfallforschung eingehen. Sehr informativ: *Qureshi,* A Review of Accident Modelling Approaches for Complex Socio-Technical Systems, Australian Computer Society, 2007, abrufbar unter: http://www.crpit.com/confpapers/CRPITV86Qureshi.pdf.
37 http://iihs.org/news/rss/pr070312.html: „Crash avoidance features reduce crahes..", News Release des Highway Loss Data Institute.
38 BGH, 16.6.2009 – VI ZR 107/08, VersR 2009, 1125 – Airbag; vgl. auch § 6 Abs. 1 Produktsicherheitsgesetz (ProdSG).
39 ISO 26262-2:2011-5.4.3.1 (Overall Safety Management).
40 ISO 26262-2:2011-5.4.2.1.
41 ISO 26262-2:2011 -6.4.2.2.
42 ISO 26262-2:2011-6.4.2.4; nach 6.4.3.1 ist der Safety Manager verantwortlich für die Planung und Koordination der funktionalen Sicherheitsaktivitäten in der Entwicklungsphase des Sicherheitslebenszyklus.
43 ISO 26262-2:2011-6.4.8.2.
44 ISO 26262-2:2011-6.4.9.3.

duktionsfreigabe.[45] Sie sind kollektiv die Adressaten für jede in einer Entstehungsphase getroffene Sicherheitsmaßnahme und jede festgestellte Sicherheitsanomalie. Sie müssen mit Gültigkeit für die gesamte Organisation dafür redundante Kommunikationsprozesse festlegen, die insbesondere der Forderung nach der Orientierung am neuesten Stand von Wissenschaft und Technik dokumentiert nachkommen.[46] Zwischen ihnen besteht nach der Norm Gleichwertigkeit. Von ihnen kann trotz gradueller Unterschiede in allen Entscheidungsfindungsprozessen insgesamt von „Functional Safety Managern" (FSM) gesprochen werden.[47] Sie müssen vor allem unabhängig sein. Die Forderung nach Unabhängigkeit setzt bestimmte Organisationsformen in einem Unternehmen voraus.

Die Unabhängigkeit ist von dem Unternehmen zu gewährleisten, das den FSM einsetzt, gleich, ob er angestellt, freier Mitarbeiter oder externer Berater ist. Diese Unabhängigkeit muss in der Unternehmensorganisation verankert, dokumentiert und im Rahmen der Managementbewertung messbar sein.[48] Die ISO 26262 verlangt deshalb zwingend: „Die Organisationen, die in der Umsetzung des Sicherheitslebenszyklus einbezogen sind, müssen ein wirksames Qualitätsmanagementsystem haben, das einem Qualitätsmanagementstandard wie dem der ISO/TS 16949, ISO 9000:2008 oder gleichwertig entspricht."[49] Die ISO/TS 16949:2009 ist ebenfalls ein in der globalen Automobilindustrie allgemein geltender Standard für die Anforderungen an ein Qualitätsmanagementsystem (QMS). Sie beruht auf der internationalen Norm ISO 9001:2008 mit Ergänzungen von Besonderheiten der Automobilindustrie.[50] Die ISO/TS 16949 ist in der Regel Vertragsbestandteil in allen Stufen der automobilen Wertschöpfungskette. Sie bestimmt wesentliche Anforderungen an die Unternehmensorganisation, die Managementverantwortung, Bereitstellung personeller und sachlicher Ressourcen sowie alle wesentlichen Prozesse für die Produktrealisierung.

Die ISO 26262 und ihre Prozesse können nur in einem wirksamen QMS nach der ISO/TS 16949 verstanden und umgesetzt werden. Die ISO 26262 kennt keine Prozesse, die sich etwa mit der Prüfung der Qualität von Komponenten und Bauteilen der Sicherheitssysteme befassen. Diese Forderungen liegen außerhalb der Anwendung der ISO 26262. Das muss im QMS geleistet werden, das dahingehend weitere Anforderungen an den gesamten Kommunikationsprozess mit dem Kunden, der Ermittlung der Anforderungen an das Produkt sowie die Sicherstellung der Fehlerfreiheit aller Zukaufteile und Leistungen stellt.[51] Bei der Zerlegung eines ASIL nach unterschiedlichen Sicherheitsbewertungen ist die Gewährleistung der Fehlerfreiheit der Komponenten ausschließlich im QMS angelegt.[52] Die Existenz des QMS wird deshalb von der ISO 26262 zwingend vorausgesetzt. Die Manager des QMS sind deshalb immer auch die Entscheidungsträger nach der ISO 26262.

1. Die Norm definiert den Begriff der geforderten „Unabhängigkeit" des Safety Managers nicht. Der „Final Draft" (FDIS) bestimmte noch für die „Confirmation Measures":[53] „The confirmation measures and the associated reviewer independence requirements are applied within the system safety process of an item in accordance with the highest ASIL level in the safety goals of the item under review. In order to ensure that these evaluations are conducted in an objective manner, confirmation measures can have additional criteria for the level of independence of the reviewer, auditors, or assessors." Diese wichtige Festlegung ist in der endgültigen Fassung von Abschnitt 10 der ISO 26262 (2012) nicht mehr enthalten. Geblieben ist allerdings die Festlegung der Norm, dass der Unabhängigkeit eine umso höhere Bedeutung zukommt, je höher der ASIL-Level ist.

Aus Teil 2 der Norm („Management of functional safety") lässt sich das Grundverständnis für die Unabhängigkeit eines FSM vereinfacht dahin ableiten, dass der ein Arbeitsergebnis einschließlich den zugrundeliegenden Annahmen und Wertungen als mit dem Sicherheitsziel entsprechend bestätigende FSM an der Erarbeitung oder Herleitung des Ergebnisses nicht beteiligt gewesen sein darf, um eine möglichst objektive Beurteilung zu gewährleisten. Für die Gefährdungsanalyse und die Risikobewertung etwa wird die Unabhängigkeit von Entwicklern des Systems, vom Projektmanagement und von den Autoren der Arbeitsergebnisse vorgeschrieben. Die gleiche Unabhängigkeit wird für das „confirmation review" der Systemintegration und den Testplan dafür, den Validierungsplan und die Sicherheitsanalyse verlangt.[54]

2. Diese normative Forderung der Unabhängigkeit hat gesetzlich und vertraglich Rechtsqualität in Bezug auf die Anforderungen an die Organisation des Unternehmens wie an den FSM persönlich. Sie ist nicht allein darauf gerichtet, technisch korrekte Ergebnisse aufgrund einer objektiven Bewertung zu generieren oder zu bestätigen. Sie ist vor allem dazu bestimmt, innerhalb der an der Entwicklung und Herstellung eines Sicherheitssystems Beteiligten, Zulieferer und Fahrzeughersteller, verlässliche Aussagen zu der Erreichung der gesetzlichen und vereinbarten Sicherheitsziele zu vermitteln. Auf die Integrität der auf Unabhängigkeit beruhenden Aussagen und Entscheidungen muss sich der Adressat verlassen können, weil er vor allem bei der Beteiligung mehrerer Zulieferer innerhalb einer produktbezogenen Wertschöpfungskette die Richtigkeit nur noch begrenzt im Rahmen von ihm durchzuführender Verifizierungen oder Validierungen überprüfen kann. Deshalb personalisiert die ISO 26262 deutlich, indem sie verlangt, die ver-

45 ISO 26262-2:2011-7.4.2.1.
46 ISO 26262-2:2011-5.4.2.3.
47 ISO 26262-1:2011-1.109: Nach der Normdefinition ist der „Safety Manager" in der „Rolle" einer Person bestimmt, die für das Management (ISO 26262-2:2011) der funktionalen Sicherheit während der Systementwicklung verantwortlich ist.
48 ISO/TS 16949:2009-5.6.
49 ISO 26262-2:2011-5.4.4.1. Die ISO/TS 16949:2009 ist eine in der globalen Automobilindustrie verbindliche Technische Spezifikation, die auf der internationalen Norm ISO 9001:2008 für Qualitätsmanagementsysteme beruht und diese mit besonderen Anforderungen aus der Automobilindustrie ergänzt. Der Begriff „Organisation" steht in beiden Regelwerken für Unternehmen oder Einheiten, die für die Wirksamkeit von Managementsystemen verantwortlich sind, um funktionale Sicherheit oder Produktqualität sicherzustellen. Der Begriff „Management" hat allerdings eine unterschiedliche Bedeutung: Während in der ISO/TS 16949 unter Management die Unternehmensführung über Hierarchien verstanden wird, verwendet die ISO 26262 den Begriff generisch für die Organisation der normspezifischen Prozesse innerhalb des Sicherheitslebenszyklus.
50 Herausgegeben von der IATF (International Automotive Task Force) stellt sie die Anforderungen an „Qualitätsmanagementsysteme, Besondere Anforderungen bei Anwendung von ISO 9001:2008 für die Serien- und Ersatzteil-Produktion in der Automobilindustrie". Sie wird weiter ergänzt durch so genannten „Customer Specific Requirements" (CSR) einzelner globaler Fahrzeughersteller.
51 ISO/TS 16949-7.4.
52 ISO 26262-10:2012-11.3.6.2, Tabelle 4.
53 ISO/DIS 26262-10-5.1.3.2 „Level of independence for performing the confirmation measures".
54 ISO 26262-2:2011-6.4.7.1, Tabelle 1. Die gleichen Anforderungen gelten für das „functional safety audit" (ISO 26262-2:2011-6.4.8) und das „functional safety assessment" (ISO 26262-2:2011-6.4.9).

traglichen Beziehungen zwischen Zulieferern und zum Fahrzeughersteller verantwortlichen Personen zu benennen.[55]

3. Die auf der Unabhängigkeit basierenden Feststellungen und Entscheidungsgrundlagen des FSM sind vornehmlich dem Unternehmen zuzurechnen. Sie repräsentieren, jedenfalls dem Anspruch der Norm nach, den gesamten projektbezogenen Wissensstand des Unternehmens am Maßstab des neuesten Standes von Wissenschaft und Technik. In der Bestätigung der Übereinstimmung mit den Forderungen der ISO 26262, also des Erreichens der vorgesehenen oder vereinbarten Sicherheitsziele durch die festgelegten Sicherheitsmaßnahmen über alle Prozesse definiert das Unternehmen dieses Wissen und gibt vor, darüber zu verfügen. Das Wissen muss als verfügbare Ressource seiner Leistungskompetenz im Rahmen eines in das Technologiemanagement eingeordneten Wissensmanagements dokumentiert sein.[56]

Der FSM ist immer Teil des Wissensmanagements, weil sich bei ihm die Wissenskompetenz des Unternehmens mit unmittelbarer Außenwirkung kumuliert, er es repräsentiert, und er die Wissenskompetenz alleinverbindlich nach außen kommuniziert: Das gilt für die Feststellung der Erfüllung vertraglicher Verpflichtung ebenso wie für das Wecken von Sicherheitserwartungen für den Gebrauch des Sicherheitssystems. „Wissen" ist dabei mehrschichtig zu verstehen: Es erfasst alle kompetenzrelevanten Informationen, die in einem Unternehmen für die Konzeption, die Entwicklung und die Herstellung eines Sicherheitssystems vorhanden sind. Es erfasst aber auch die „Sprache" der elektronischen Systeme und ihre Interaktion untereinander. Die Kommunikation in und unter elektronischen Bauteilen beruht auf gesteuerten Datenflüssen, die „auf der Ebene der Semantik" die Fähigkeit erlangen, „Sachverhalte oder Objekte abzubilden", also Abläufe für die gewollten Funktionalitäten eines Sicherheitssystems darzustellen oder zu bewirken.[57] Die systemgenerierten Informationen aus Datensätzen, „bei der die Informationsbeschaffung bzw. -übermittlung durch den Menschen allenfalls veranlasst, aber nicht mehr willentlich gesteuert wird", stellt besondere Anforderungen an das Wissensmanagement.[58] Diese Informationen beinhaltet notwendige Defizite insbesondere aus der bereits erwähnten willkürlichen Selektion von Annahmen und Risikobewertungen nicht vollständig beherrschbarer Fehlermöglichkeiten und -wahrscheinlichkeiten elektronischer Komponenten. Prüf- und Testsoftware unterliegen notwendig den gleichen begrenzten Fähigkeiten.

4. Die Gewährleistung der Unabhängigkeit des FSM ist in der gesamten Wertschöpfungskette Vertragspflicht (§ 280 BGB), meines Erachtens nicht nur in der jeweiligen bilateralen Vertragsbeziehung zwischen einem Zulieferer und seinem Kunden in der nächst höheren Stufe der Wertschöpfungskette oder zwischen dem Systemhersteller (TIER 1) und dem Fahrzeughersteller, sondern mit Schutzwirkung für die gesamte Wertschöpfungskette, in der alle Beteiligten von einander abhängig und auf einander angewiesen sind. Das folgt aus der Produktverantwortung nach dem Produktsicherheitsgesetz. Die ISO 26262 verlangt dafür als Teil des „safety plans" ein „Development Interface Agreement (DIA)",[59] in dem die Leistungen der Zulieferer untereinander und ihre Vereinbarkeit mit der Forderung des letztverantwortlichen Fahrzeugherstellers für das im Fahrzeug integrierte System vertraglich festgelegt werden müssen.[60]

5. Die Unabhängigkeit der FSM als Entscheidungsträger muss vor allem effektiv sein. Sie müssen nach der ISO 26262 die ihrer Verantwortung entsprechende Autorität für die Kontrolle und Durchführung des ganzen Sicherheitsplans[61] haben.[62] Diese Normforderung ist ambivalent: Die Unternehmensführung muss die Autorität sicherstellen und dafür eigenständige Kontrollmechanismen im Rahmen des Risikomanagementsystems des ganzen Unternehmens (§ 91 Abs. 2 AktG) vorhalten, deren Wirksamkeit allerdings wiederum von der fachlichen Kompetenz des FSM und seiner Autorität, die Kompetenz auch gegen Widerstände durchzusetzen, abhängig ist. Eine Entlastung der Unternehmensführung durch die Bestellung des FSM von der primären Haftung wird man deshalb nicht ohne Weiteres annehmen können.

6. Für den FSM entstehen aus der Ausstattung mit der in der Norm geforderten Autorität und aus ihrer Wahrnehmung zwangsläufig Zielkonflikte auf unterschiedlichen Ebenen, die hier nur angerissen werden können. Die Anstellung eines FSM verursacht dem Unternehmen zunächst Kosten, deren Effizienz nicht unmittelbar messbar ist. Als Arbeitnehmer kann der FSM in einen Kompetenzkonflikt mit seinem Vorgesetzten oder, da er bereichsübergreifend entscheidet, mit anderen Abteilungen des Unternehmens geraten. Die Arbeitnehmerstellung relativiert faktisch das strenge Gebot der Unabhängigkeit nach der ISO 26262. Die Maßnahmen und Entscheidungen des FSM müssen nicht immer kompatibel mit den Interessen des Unternehmens sein, etwa wenn er Ergebnisse verwirft, wenn er sich einem Zeitdruck nicht beugt oder wenn er auf seiner Entscheidung trotz Überschreitung eines vorgegebenen Kostenrahmens beharrt.

7. Zusätzlich ist der FSM Risiken ausgesetzt, weil er persönlich für die Befundungen zur Sicherheit des Systems und Fehleinschätzungen über den Sicherheitslebenszyklus[63] einzustehen hat.[64] Er kann nicht alle Vorleistungen, die er in Summe zu beurteilen hat, im Detail nachprüfen, sondern muss sich auf die Verlässlichkeit der ihm präsentierten Arbeitsergebnisse anderer verlassen können. Er hat es auch nicht in der Hand, wie das von ihm gelieferte Sicherheitsargument in der Vertragsgestaltung mit anderen Zulieferern oder dem Fahrzeughersteller oder vom Fahrzeughersteller gegenüber dem Endverbraucher verwendet wird. Unkorrekte, nicht vollständige oder übertriebene Aussagen zu der vom FSM bestätigten Sicherheit des Systems und ihr Zusammenhang mit anderen Systemen oder

55 ISO 26262-8:2011-5.4.2.2 lit. e).
56 Sehr ausführlich zum und zutreffend zum Technologiemanagement *Müller/Wege,* in: Ensthaler/Gesmann-Nuissl/Müller, Technikrecht – Rechtliche Grundlagen des Technologiemanagements, 2012, S. 353 ff.
57 *Müller/Wege,* in: Ensthaler/Gesmann-Nuissl/Müller, Technikrecht – Rechtliche Grundlagen des Technologiemanagements", 2012, S. 355 f.
58 *Ensthaler/Müller/Synnatzschke,* Technologie- und technikorientiertes Unternehmensrecht, BB 2008, 2638, 2643.
59 Muster in: ISO 26262-8:2011, Annex B; ISO 26262-2:2011-6.4.3.5 lit. f).
60 ISO 26262-8:2011-5.
61 ISO 26262-2:2011-6.4.3.2 und 6.4.3.5.
62 Die ISO/TS 16949-5.5.1.1. kennt im Grundsatz diese Autorität, wenn sie vorschreibt „Personal, das für die Produktkonformität verantwortlich ist, muss die Befugnis haben, die Produktion anzuhalten, um Qualitätsprobleme zu lösen."
63 ISO 26262-2:2011-7.4.2.3.
64 Guter Überblick zur Haftung von Arbeitnehmern in Qualitätsverantwortung mit dem Schwerpunkt der Entwicklungstätigkeit bei *Dihlmann/Karcher/Schmidt/Gildeggen,* Die persönliche Haftung des Entwicklungsingenieurs für Produktfehler, PHi 2012, 148 ff.

dem ganzen Fahrzeug können, ohne dass er Einfluss darauf hätte, den Fehlerbegriff des § 3 ProdHaftG erfüllen, weil erweckte Sicherheitserwartungen enttäuscht werden.

Der FSM trägt auch die Folgen für Fehlentscheidungen seines Unternehmens, etwa dann, wenn erkannte Risiken trotz eines hohen Gefahrenmoments heruntergespielt werden und ihnen ein niedriger ASIL zugewiesen wird, obwohl ein hoher ASIL erforderlich wäre: Es gibt bekannte und immer wieder auftretende Fehler in der Motorsteuerung von Fahrzeugen: Die Motorsteuerung fällt bei einer bestimmten hohen Geschwindigkeit aus und geht in den Notlaufmodus über. Befindet sich das Fahrzeug auf der linken Fahrspur der Autobahn und muss wegen fehlender Motorleistung auf den Standstreifen durch dicht auffahrende Lastwagen manövrieren, ist die Unfallgefahr extrem hoch. Trotzdem wird dieser Fehler, dessen Ursache angeblich unbekannt ist, nur mit ASIL A, nicht mit ASIL D belegt. Informationen sind im Betriebshandbuch nicht vorhanden. Ein unabhängiger FSM und sein Unternehmen werden sich in einem Produkthaftungsfall die Frage stellen lassen müssen, wie diese Bagatellisierung zu vertreten ist, vor allem dann, wenn die Ursache (angeblich) nicht bekannt ist, das Fahrzeug trotzdem in den Verkehr gebracht wird.[65]

Dann stellt sich für den FSM neben denen, die sich gegen das Unternehmen richten, immer die persönliche Haftungsfrage. Die Rolle des FSM ist die einem Compliance Officer in Weitem vergleichbar. Ihm kann also je nach Fallgestaltung strafrechtlich eine Garantenstellung zukommen, wie sie der BGH für den Compliance Officer angenommen hat.[66]

Der FSM bedarf deshalb des besonderen Schutzes: Arbeitsrechtlich muss in Ergänzung seines Arbeitsvertrages ein Benachteiligungsverbot für alle Maßnahmen des FSM aufgenommen sein. Ferner muss er vom Unternehmen von allen Folgen seines Handelns freigestellt werden, Fälle der groben Fahrlässigkeit oder des Vorsatzes ausgeschlossen.

Gerät der Unternehmer in die Insolvenz, nützen dem FSM diese arbeitsvertraglichen Schutzmaßnahmen nichts. Er kann von Dritten in Anspruch genommen werden. Deshalb gebietet sich, dass der FSM ausdrücklich als mitversicherte Person in die Betriebs- und Produkthaftpflichtversicherung des Unternehmens aufgenommen wird. Die derzeit gängigen Klauseln in Versicherungspolicen stellen das nicht sicher. Der FSM muss unabhängig vom Unternehmen von dem Kostenrisiko der zivilrechtlichen und strafrechtlichen Rechtsverteidigung durch den Abschluss entsprechend werthaltiger Rechtsschutzversicherungen freigestellt werden, die auch Bestand haben, wenn der FSM aus dem Unternehmen ausgeschieden ist.

8. Das Problem ist in der Praxis angekommen und wird intensiv diskutiert, ohne dass bislang eine klare Linie für einen Lösungsansatz zu erkennen ist. Peter Grabs und Pierre Metz haben im Rahmen der 4. Euro-Forum-Konferenz zur ISO 26262 im September 2012 in ihrem Beitrag „A critical view on „Independence" in ISO 26262" auf die Problemlage aus den unklaren Formulierungen der Norm, aus der Unsicherheit im Umgang mit der Norm im Ganzen und aus den daraus folgenden Risken hingewiesen. Die unzulängliche Definition der Unabhängigkeit in der ISO 26262 beschreiben sie – wenn auch nicht abschließend – zutreffend mit den Stichworten: „creates confusion", „does not prevent economical bias", does not prevent „selective hiring", „neither addresses nor guarantees competence", „can lead to arbitrary organizational changes" und „does not reflect psychology".

Grabs und Metz schlagen einen „objektivierten" Ansatz vor und meinen, Unabhängigkeit sei als Methode und nicht als Ziel zu verstehen („Independende merely is a method but not a goal"). Dieser prozessorientierte Ansatz im Sinne der ISO/TS 16949:2009 ist richtig, ändert aber nichts an dem subjektiven Gehalt des unbestimmten Rechtsbegriffs der Unabhängigkeit des verantwortlichen FSM.[67]

In Hinblick auf diese Individualisierung der Haftungslage des Unternehmenshandelns auf den FSM ist der rechtslastige Begriff der Unabhängigkeit ein Fremdkörper in der Norm. Die strikte systembezogene prozessorientierte Norm kann zur auch rechtlichen Abgrenzung der Unabhängigkeit keinen eigenen Prozess zur Verfügung stellen, weil zu viele Implikationen aus dem Unternehmens-, Arbeits- und Versicherungsrecht vorausgesetzt werden. Bei der für 2014 anstehenden Revision der Norm dürfte sich die Streichung der Forderung nach Unabhängigkeit des FSM empfehlen. Für die Zwecke der Norm reicht es aus, es bei den Forderungen aus der ISO/TS 16949, Abschnitt 6 (Personelle Ressourcen), und der Festlegung der Funktionen des FSM bei den audits, den reviews und den assessments zu belassen.

V.

Technische Normen wie die ISO 26262 für die Funktionale Sicherheit in Personenfahrzeugen haben eine unmittelbare Rechtsrelevanz als Auslegungsgrundlagen rechtlicher Pflichten innerhalb einer Branche wie der Automobilindustrie.

Was technisch möglich ist, ist rechtlich nur dann zulässig, wenn die Umsetzung des technisch Möglichen den gesetzlichen Sicherheitsvorstellungen entspricht, die immer Bestandteil der in Normen festgelegten Sicherheitsziele sind.

Die ISO 26262 ist eine verhaltensnormierende Prozessnorm für die funktionale Sicherheit von Sicherheitssystemen. Sie gewährleistet nicht die Sicherheit des Fahrzeugs, sondern macht es in Bezug auf antizipierte Gefahrenlagen beherrschbar unter der Voraussetzung angenommener Bedingungen mit entsprechender Eintrittwahrscheinlichkeit.

Die ISO 26262 ist keine für sich allein stehende Norm. Sie ist nur innerhalb eines wirksamen Qualitätsmanagementsystems effektiv und effizient.

Die Entscheidungsträger, also die Functional Safety Manager, der ISO 26262 sind stets Manager im Qualitätsmanagementsystem und tragen wie die Qualitätsmanager eine hohe persönliche Verantwortung. Das Gebot der ISO 26262 für ihre Unabhängigkeit gebietet arbeitsrechtliche und unternehmerische Schutzmaßnahmen.

---

65 Der Autor hat die Erfahrungen selber bisher drei Mal machen müssen. In den chats im Internet wird das Thema diskutiert. Die Ausleseprotokolle geben keinen Hinweis auf die Ausfallursachen. Der Fahrer bleibt das Versuchskaninchen technischen – angeblichen – Unwissens des Fahrzeugherstellers.

66 BGH, 17.7.2009 – 5 StR 394/08, NJW 2009, 3173 ff.

67 Tagungsdokumentation zur 4. EUROFORM Konferenz „ISO 26262" vom 12.-14.9.2012; *Helmig,* Funktionale Sicherheit nach ISO 26262 und Produkthaftung für No-trouble-found-Fälle, PHi 2012, 32 ff.