



FUNKTIONALE SICHERHEIT – UMGANG MIT UNABHÄNGIGKEIT,
RECHTLICHEN RAHMENBEDINGUNGEN UND HAFTUNGSFRAGEN

Rechtliche Folgen der ISO 26262

Nun ist es soweit – die ISO 26262 ist nach etwa acht Jahren nationaler und internationaler Vorarbeit durch die entsprechenden Normungsgremien veröffentlicht (Band 1-9). Dieser Beitrag gibt eine Übersicht über das rechtliche Umfeld sowie den Stand der Wissenschaft und Technik. Zudem befasst er sich mit Themen, die dem entwickelnden Ingenieur oft nicht nahe stehen, wie Unabhängigkeit bei Reviews und Assessments, die für die rechtliche Einordnung von persönlicher Haftung und der des Unternehmens ausschlaggebend sind.

Die ISO 26262 zur Funktionalen Sicherheit in Personenkraftwagen bestimmt in Zukunft maßgebend die elektrische und elektronische Architektur. Sie ist relevant für die Umsetzung der Forderungen der europäischen Verordnung 661/2009, nach denen die Fahrzeugsicherheit gemäß dem jeweils neusten Stand von Wissenschaft und Technik ausgelegt werden muss. Da die Norm ein Rahmenwerk zur Erreichung von Funktionaler Sicherheit bei der Verwendung komplexer elektrischer und elektronischer Systeme in Fahrzeugen ist, gehört sie selbst auch zum aktuell gültigen wissenschaftlichen und technischen Stand der Technik. Funktionale Sicherheit ist eine Eigenschaft dieser Systeme, die durch die Methoden der ISO 26262 bewertet werden kann. Die Bewertung selber reduziert Risiken, vermeidet sie aber nicht vollständig.

Die Norm fordert die Integration ihrer Anforderungen in die Prozesse eines Qualitätsmanagementsystems nach der ISO/TS 16949:2009. Die Umsetzung der Anforderungen

der Norm bestimmt wesentlich die zivilrechtliche und strafrechtliche Verantwortlichkeit der Hersteller sicherheitsrelevanter Systeme und insbesondere die der Fahrzeughersteller. Sie zwingt mit der Forderung zum Abschluss einer Leistungsschnittstellenvereinbarung (engl. Development Interface Agreement, DIA) zu einer vertraglichen Festlegung der Verantwortlichkeiten zwischen Fahrzeugherstellern und Zulieferern durch Festlegung und Dokumentation der Sicherheitsaktivitäten in der Konzeptphase, der Entwicklungsphase und der Produktionsphase. Die ISO 26262 gewinnt damit eine enorme rechtliche Relevanz für die vertrags- und haftungsrechtliche Beziehung der an der aufsteigenden Wertschöpfungskette der Automobilindustrie Beteiligten.

Haftungsgrundlagen – Produkt- und Produzentenhaftung

Zur Klarstellung der rechtlichen Relevanz der ISO 26262 sind die beiden Rechtskreise „Produkthaftung“ sowie „Produzentenhaftung“ zu betrachten.

Produkthaftung – folgend dem nationalen und europäischen Produkthaftungsgesetz – stellt die außervertragliche, gesetzliche, verschuldensunabhängige Haftung (deliktische Produkthaftung) für fehlerhafte (Teil-)Produkte dar. Umfasst sind alle Fälle, in denen für fehlerhafte Produkte zu haften ist. Zu berücksichtigen ist, dass auch ein spezifikationsgerechtes Produkt „fehlerhaft“ sein kann. „Die Ersatzpflicht des Herstellers ist nur dann ausgeschlossen, wenn der Fehler nach Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte.“ (§1 Abs. 2, Ziffer 5 PHG).

Produzentenhaftung – hier insbesondere in Bezug auf §823 BGB – beschreibt die außervertragliche, verschuldensabhängige Haftung. Voraussetzung für deren Anwendung sind Pflichtverletzung + Rechtsgutverletzung + Schaden + Verschulden. In Bezug auf die Pflichtverletzung + Verschulden ist im vorliegenden Beitrag insbesondere die Thematik des Waltens der erforderlichen Sorgfaltspflicht, z. B. in Bezug auf Stand der Wissenschaft und Technik relevant.

Die Rechtsfolgen aus der ISO 26262 ergeben sich nicht erst aus der Anwendung eines Produkts, das nach den Prozessen der Norm hergestellt wurde. Die Norm selber erhebt den Anspruch, gesetzliche und behördliche Anforderungen zu berücksichtigen. Der Anwender der Norm muss bereits in der Konzeptphase, in der Entwicklungsphase und in der Produktion rechtliche Anforderungen erfüllen. Das setzt voraus, dass er die Anforderungen kennt.

Rechtliche Einordnung der ISO 26262

Was ist unter der Begrifflichkeit „Stand der Wissenschaft und Technik“ zu verstehen? Ist er mit der Einhaltung der einschlägigen veröffentlichten Normen (insbes. DIN/ISO/IEC) gleichzusetzen? Nein, nicht automatisch. Normen können überholt sein und daher nicht mehr den aktuellen Stand der Technik wiedergeben. Hersteller müssen alle ihnen zugänglichen technischen und wissenschaftlichen Erkenntnisse ausnutzen, auch wenn die bekannten Normen lediglich geringere Sicherheitsstandards erlauben. Allerdings bilden Normen einen Mindeststandard, sodass ein Produkt nach außen zunächst dem durchschnittlichen Benutzer den Eindruck erweckt, dass es seinen Sicherheitserwartungen entspricht.

Der Stand der Wissenschaft und Technik wird insgesamt durch allgemein verfügbare (nicht zwingend neue) technische Erkenntnisse und Lösungen geprägt – ungeachtet dessen, ob bereits branchenüblich und wo auf der Welt veröffentlicht. Es obliegt der Sorgfaltspflicht eines entwickelnden Unternehmens, den jeweils aktuellen Stand der Wissenschaft und Technik bei der Entwicklung anzuwenden. Wichtige, in Bezug auf die Anwendung der ISO 26262 zu berücksichtigende Faktoren sind:

- Ist ein E/E-Teilsystem/eine Komponente mit einer sicherheitsrelevanten Funktionalität ausgestattet, so sind mindestens u. a. die aktuell verfügbaren Standards (oder veröffentlichte Normenentwürfe) zur Funktionalen Sicherheit anzuwenden oder auf alternative Weise das minimal gleichwertige Sicherheitsniveau zu erreichen.
- Der Zulieferer eines Teilsystems ist bei Nicht-Vorliegen von sicherheitstechnischen Vorgaben durch seinen Kunden keinesfalls von der Sorgfaltspflicht befreit. D. h., der Zulieferer ist zur Anwendung des Möglichen zur Absicherung sicherheitsrelevanter Funktionen bzw. deren im zugelieferten Teil beinhalteten Teilfunktionen verpflichtet.

Nun stellt sich die Frage, wie viel Aufwand betrieben werden muss, um den anzuwendenden Stand der Wissenschaft und Technik für die konkrete Applikation festzustellen. Allgemein gilt:

- Das Gefahrenpotenzial entscheidet über den erforderlichen Aufwand.
- Ein Vergleich mit marktgängigen Referenzprodukten ist erforderlich.
- Ein Abgleich mit bekannten Informationen zur potenziellen Absicherung ist durchzuführen.
- Bei technischem Neuland und hohem Risiko ist eigene Forschung und ggf. die Entwicklung eines eigenen und neuen Stand der Wissenschaft und Technik (z. B. auf dem Gebiet der E-Mobilität) unumgänglich.

In Bezug auf die in diesem Beitrag betrachtete ISO 26262 gilt unter Berücksichtigung des juristischen Umfelds:

- Die ISO 26262 wird in der Regel bereits jetzt in den Vertragswerken der Fahrzeughersteller und Tier-1-Zulieferern angewendet. Die Umsetzung ist daher für alle sich aktuell in der Entwicklung



Frequenzmeister: 20 Herzschläge/Sek. 50 Flügelschläge/Sek.

Was Frequenzen angeht, setzt der Kolibri in der Natur Standards – im Bereich Schwingungsanalyse setzt diese unser Messsystem **PikesPEAK**.

- Untersuchung rotierender Systeme
- Exakte DrehSchwingungsanalyse
- Hochpräzise Winkelbestimmung
- Identifizierung von Resonanzen und Gleichlaufschwankungen

Dieses Messsystem meistert Ihre Herausforderungen!

- Leistungsstark durch Multiprozessor
- Abstrate analoger Signale bis 500 kHz
- Drehzahlerfassung mit einer Auflösung von < 0,1 ns
- Dynamische Messbereichsanpassung bei 16 Bit Auflösung
- Analoge und digitale Signale kombinierbar
- Modular aufgebaut und mobil einsetzbar

Extreme messen und analysieren



AFT Atlas Fahrzeugtechnik GmbH
Gewerbestraße 14 · D-58791 Werdohl
Tel. 02392 809-312

www.pikespeak.de

SCHAEFFLER GRUPPE
AUTOMOTIVE

befindenden Produkten zumindest im definierten Anwendungsbereich notwendig. Auf dem Nutzfahrzeugsektor kann additiv (bei entsprechender Argumentation auch alternativ) die generische Grundnorm IEC 61508 angewendet werden.

ISO 26262 = Fahrzeugsicherheit?

Die ISO 26262 ist keine in sich geschlossene Systemnorm zur Sicherstellung der Funktionalen Sicherheit von in Fahrzeugen verwendeten E/E-Systemen und der Fahrzeuge selber. Man kann nicht die Gleichung formulieren: „Erfüllung der Forderungen der ISO 26262 = Fahrzeugsicherheit“. Allein die Forderungen nach „freedom of interference“ und das noch nicht geklärte Problem der Ablenkung („distracting“) des Fahrers durch zu viele Assistenzsysteme oder das Problem des Ausfalls nur eines Teilsystems mit einer Kettenwirkung auf nachgeschaltete Teilsysteme und die sich daraus ergebende Einschränkung der Handlungsfreiheit des Fahrers sind derzeit völlig offen.

Die ISO 26262 ist ein Rahmenwerk im Sinne eines Leitfadens (Prozesse und Methoden), innerhalb dessen auf anderen Technologien beruhende sicherheitsrelevante Systeme betrachtet werden können. Sie enthält:

- den automobilen Sicherheitslebenszyklus einschließlich der Produktion,
- die risikoorientierte Annäherung, um Sicherheitsstufen (Safety Integrity Level) zu bestimmen,

- Anforderungen an die prozessbezogene Verifizierung, die Validierung und die Bestätigung von Maßnahmen, um das Erreichen der Sicherheitsstufe zu bestätigen und gegebenenfalls einen hinreichenden und annehmbaren Grad der Sicherheit zu erreichen,
- Anforderungen an die Festlegung einer Schnittstelle zur Gewährleistung einer lückenlosen und Norm konformen Zusammenarbeit von OEM und Zulieferern und deren Nachweis.

Erforderliches Umfeld zur ISO 26262

Die Sicherheitsanforderungen der ISO 26262 beziehen sich nur auf E/E-Systeme im Fahrzeug. In der Gefahren- und Risikoanalyse (G&R) werden zwar alle Fehler und Störungen in Bezug auf die Funktionalität berücksichtigt. Die Norm stellt aber keine Anforderungen an andere Technologien (Mechanik, Hydraulik und Pneumatik) und berücksichtigt keine Einflüsse von E/E-Systemen von außen, wie etwa Hackerangriffe über mobile Datenkommunikationsschnittstellen wie GPS, LTE, UMTS, GPRS und GSM und weiter über das Infotainment auf das Bordnetz. Auch Störfaktoren wie Vibration, Betriebsumgebung im Fahrzeug, Temperatur, Umwelteinflüsse, Fahrerfähigkeit, etc. werden nicht im zu entwickelnden E/E-Sicherheitskonzept weiterführend abgedeckt. Sie trifft keine Aussage zur Qualität (Fehlerfreiheit) der für die Systeme verwendeten Bauteile (Sensoren, Halbleiter-Bauelemente, Platinen, Mikroschalter etc.). Sie setzt dafür ein zertifiziertes und wirksames QM-System etwa nach ISO/TS 16949:2009 voraus.

ISO/TS 16949 ist ein Qualitätsmanagementsystem, das Bedingungen für die Herstellung fehlerfreier Produkte schafft. Sie sichert aber nicht die Qualität der Produkte selbst.

Die Aktivitäten nach der ISO 26262 sind integraler Bestandteil des übergeordneten prozessorientierten Ansatzes des Qualitätsmanagementsystems nach der ISO/TS 16949:2009, insbesondere Kapitel 7 (Produktrealisierung). Die Prozesse der ISO/TS 16949 müssen die Aktivitäten der ISO 26262 implementieren. Die ISO 26262 erweitert den Fokus der ISO/TS 16949 von der Verantwortlichkeit der Zulieferer in der Wertschöpfungskette (ISO/TS 16949-02: „Wechselwirkung“) im Sinne der Fehlervermeidung und Fehlerbeherrschung [ISO/TS 16949 – Anmerkung zu 7.2.1] um die Verantwortlichkeit des für Sicherheit des Gesamtfahrzeugs zuständigen OEMs für die Validierung des Gesamtsystems.

Confirmation measures	Degree of Independence applies to ASIL			
	A	B	C	D
Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14) Independence with regard to the author of the argument	10	11	12	13
Confirmation review of the completeness of the safety case (see 6.5.3) Independence with regard to the authors of the safety case	10	11	12	13
Functional safety audit in accordance with 6.4.8 Independence with regard to the developers of the item and project management	–	10	11	13
Functional safety assessment in accordance with 6.4.9 Independence with regard to the developers of the item and project management	–	10	12	13

- a The notations are defined as follows:
- : no requirement and no recommendation for or against regarding this confirmation measure;
 - 10: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;
 - 11: the confirmation measure shall be performed, by a different person;
 - 12: the confirmation measure shall be performed, by a person from a different team i.e. not reporting to the same direct superior;
 - 13: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

Unabhängigkeit bei Assessments und Audits

Betrachtet der Anwender die ISO 26262 isoliert von der restlichen Normenwelt, so erscheint die erforderliche Unabhängigkeit des Reviewers, Assessors und Auditors klar geregelt (Tabelle 1). Doch wie belastbar ist diese Einstufung in Hinblick auf Stand der Wissenschaft und Technik? Im Regelfall gilt: „Wo kein Kläger,

Tabelle 1: Auszug aus ISO 26262-2 Table 1.

da kein Richter“. Dies bedeutet, dass bei ordnungsgemäßer Funktionsweise des betroffenen Produktes etwa mit einem Sicherheitsintegritätslevel ASIL D die Überprüfung der Funktionalen Sicherheit von einer Person aus einer anderen Abteilung oder Organisation ohne eine Forderung und Dokumentation von Unabhängigkeit und Kompetenz der selbigen zu genügen scheint.

Doch bei Betrachtung eines möglichen Produkthaftungsfall (Annahme: Personenschaden) treten diverse zusätzliche Anforderungen zutage:

1. Im Produkthaftungsfall wird im Rahmen der Beweisbringung die Unabhängigkeit und Kompetenz der assessierenden bzw. auditierenden Stelle begutachtet.

Wirkliche Unabhängigkeit ist nur gegeben, wenn keine wirtschaftliche oder arbeitsrechtliche Abhängigkeit der analysierenden Stelle vom herstellenden Unternehmen gegeben ist. Dies ist bei haus-

internen Prüfstellen unstrittig anzuzweifeln. Zu viele Faktoren können eine Rolle spielen: Wettbewerbsdruck, Kosteninteresse, unzulänglicher Informationsaustausch vor einer Verifizierung und Validierung, Zeitdruck vor SOP etc. Im Schadensfall kommt es immer auf die Wertung bei der ex-post-Betrachtung an. Jeder Richter und jeder Staatsanwalt wird nach Argumenten suchen, wie und warum ein nachträglich erkanntes Problem hätte schon früher festgestellt und vermieden werden können.

Schutz gegen Auffinden solcher Argumente bietet nur die Feststellung der geplanten und umgesetzten Unabhängigkeit in der Prüfung, die genaue Dokumentation der Entscheidungsparameter für eine Akzeptanz eines „residual risks“, die Integrität der Risikoabwägung und die genaue Risikobeschreibung für den Fahrzeugbenutzer aus der antizipierenden Perspektive des Risikos und der Wahrscheinlichkeit der Risikobeherrschung.

2. Wird zusätzlich noch die Kompetenz der prüfenden Stelle untersucht – und hiervon ist bei einem Gerichtsfall auszugehen –, so kommt der weitere schwerwiegende Aspekt der rechtlichen Anerkennung der Stelle hinzu.

Wie wird in der Regel international (auch in anderen Technologien wie Luft- und Raumfahrt, Automatisierungstechnik, Kerntechnik und Eisenbahn) der Kompetenz- und Unabhängigkeitsgrad einer konformitätsbewertenden Stelle entsprechend dem Stand der Wissenschaft und Technik neutral nachgewiesen? Durch Akkreditierungen. Akkreditierung ist gemäß ISO/IEC 17011 die Bestätigung durch eine dritte Stelle, die formal darlegt, dass eine Konformitätsbewertungsstelle die Kompetenz besitzt, bestimmte Konformitätsaufgaben wahrzunehmen. Für Deutschland gilt: Seit dem 01.01.2010 ist ausschließlich die Deutsche Akkreditierungsstelle GmbH DAkkS für alle Akkreditierungen in Deutschland zuständig. Die DAkkS befindet sich aktuell im Gesellschafterbesitz zu 1/3 des Bundes, zu 1/3 bei fünf Bundesländern und zu 1/3 des Bundesverbands der Deutschen Industrie (BDI).

SIM SIMPLE SIMTOOLS

- for development and test engineers
- building distributed embedded systems
- based on FlexRay and CAN communication standards
- integrated with MATLAB/Simulink
- using EB software and hardware platforms



SIMTOOLS

Tel +43 (0) 5 9010 29330 info@simtools.at www.simtools.at

Zur Konformitätsbetrachtung von Produkten ist für Prüfstellen der ISO/IEC 17025 (optional ISO/IEC 17020 für Inspektionsstellen) der entsprechende internationale Standard gültig – das gilt auch für die Funktionale Sicherheit. Sie stellt die erforderliche Basis für die Akzeptanz von Prüfberichten/Zertifikatsberichten im Falle von Rechtsstreitigkeiten dar (Alternative im deutschen Rechtsraum: Öffentlich bestellte und vereidigte Sachverständige). Diese haben einen höheren Grad an Objektivität, auch wenn jedes Gutachten, das nicht vom Gericht bestellt wurde, „Parteigutachten“ bleibt. Zusatzanforderung ist: „Kein Stallgeruch“, also die Prüfstelle ist kein Teil eines gemeinsamen Unternehmensverbands.

Es wird davon ausgegangen, dass im Falle eines Gerichtsverfahrens bei Nichtberücksichtigung dieser Rahmenbedingungen sowohl in Hinblick auf Produkt- als auch Produzentenhaftung eine Entlastung des entwickelnden Unternehmens oder Entwicklers und eine Beweislastumkehr nicht gegeben ist. D. h., Nachweise wirtschaftlich oder arbeitsrechtlich abhängiger Organisationseinheiten oder nicht für Funktionale Sicherheit akkreditierter Dritter werden demzufolge gerichtlich nicht zum Zwecke der Beweiserbringung des Einhaltens des Standes der Wissenschaft und Technik akzeptiert. In Bezug auf die Sorgfaltspflicht ist es als Stand der Wissenschaft und Technik anzusehen, dass der Teil der Produktabstimmung „Assessment“ zur Funktionalen Sicherheit von hierfür gemäß ISO/IEC 17025 bzw. ISO/IEC 17020 akkreditierten, sich nicht im eigenen Konzernverbund befindlichen Prüfstellen durchgeführt wird.

Schlussbetrachtung – heutiger Stand

Bei Abgleich der gesetzlichen Rahmenparameter und des Stands der Wissenschaft und Technik auch in der Normungsgebung mit der derzeitigen Praxis in der europäischen Automobilindustrie ist zu konstatieren, dass sich auf dem Gebiet der Funktionalen Sicherheit in den letzten Jahren viel getan hat, es allerdings in der Regel noch einiger Anstrengungen bedarf, den aktuellen Stand der Wissen-

schaft und Technik auf dem Gebiet der Absicherung umzusetzen. Die Sensibilität für die rechtlichen Rahmenbedingungen und die Wahrnehmung der Sinnhaftigkeit der Absicherung gemäß Stand der Wissenschaft und Technik schreitet aber kontinuierlich voran – national wie international. (oe)



Martin Schmidt ist Leiter Global Competence Center Funktionale Sicherheit bei SGS-TÜV GmbH – ein Unternehmen der SGS-Gruppe und des TÜV Saarland e.V.; Co-Initiator der Normungsarbeiten zur ISO 26262.



Marcus Rau ist Leiter Training Funktionale Sicherheit bei SGS-TÜV GmbH; SGS-TÜV Vertreter im deutschen Normungsgremium zur ISO 26262 - ISO TC22/SC3/WG16.



Dr. Bernhard Bauer ist kommissarischer Leiter des Fachgebietes Elektronik & IT der TÜV NORD Mobilität GmbH & Co. KG.



Dr. Ekkehard Helmig ist selbständiger Rechtsanwalt und Notar, fokussiert auf Produkthaftung, technische Regelwerke Automotive und ihre rechtliche Umsetzung.

@ SGS-TÜV GmbH
www.sgs-tuev-saar.com

HANSEr eMOBILITY

HANSEr

HANSEr eMobility

Nutzen Sie 2012 die beiden Themen-Specials für Ihre Marketingkommunikation!

HANSEr eMobility 1 erscheint am 03.05.2012

HANSEr eMobility 2 erscheint am 08.10.2012 – mit Kompetenzposter

Jeweils mit den Themen: Leistungselektronik, Hybrid-/E-Fahrzeug-Komponenten, Energiemanagement, Energiespeicher, Ladekomponenten, CarIT/Connected Cars, Entwicklungs-Tools und Mess- und Prüftechnik

Weitere Informationen unter:

scharlsend@hanser.de oder Tel. +49 8144 9969512



Sonderheft eMobility

Kompetenzposter