ISO 26262

Die **ISO 26262** („*Road vehicles – Functional safety*“) ist eine ISO-Norm für sicherheitsrelevante elektrische/elektronische Systeme in Kraftfahrzeugen. Die ISO 26262 definiert ein Vorgehensmodell zusammen mit geforderten Aktivitäten und Arbeitsprodukten („work products“) sowie anzuwendenden Methoden in Entwicklung und Produktion.

Die Umsetzung der Norm soll die funktionale Sicherheit eines Systems mit elektrischen/elektronischen Komponenten im Kraftfahrzeug gewährleisten. Damit ist die Norm eine Anpassung der IEC 61508 an die spezifischen Gegebenheiten im Automobilbereich. Im Fokus der Norm liegen Fahrzeuge bis 3500 kg zulässiger Gesamtmasse,[1] nicht jedoch Prototypen oder spezielle Fahrzeuge wie beispielsweise Umbauten für Behinderte. Die Norm ist nicht anwendbar auf Systeme, die entwickelt wurden, bevor sie in Kraft gesetzt wurde. Die Anwendung der Norm ist freiwillig, aber in der Praxis verlangen immer mehr Automobilhersteller von ihren Zulieferern die Anwendung in neuen Projekten.

Nach einem längeren Vorlauf (Teile 1–9 im April 2011 als *Final Draft International Standard* (FDIS) veröffentlicht) wurde die Norm mit Ausnahme von Teil 10 am 14. November 2011 in Kraft gesetzt.[2] Die ISO 26262 wird von der ISO-Arbeitsgruppe „ISO TC22/SC3/WG16“ bearbeitet. Da die Erstellung von Teil 10 (informative Guideline) längere Zeit in Anspruch nahm, wurde er erst später, am 1. August 2012, veröffentlicht.

Eine deutschsprachige Version ist nicht geplant. Es kann davon ausgegangen werden, dass innerhalb von drei Jahren mit der ersten Überarbeitung der ISO 26262 begonnen wird, so dass mit der „Second Edition“ gegen 2017/2018 gerechnet werden kann.

1 Anwendungsbereich und Hintergrund

Mit der stetig wachsenden Komplexität elektronischer Komponenten in Fahrzeugen steigt auch die Möglichkeit von Fehlfunktionen. Ist eine sicherheitsrelevante Komponente von einer solchen Fehlfunktion betroffen, können im schlimmsten Fall Menschen zu Schaden kommen. Würde z. B. ein ESP-Steuergerät in einem Kraftfahrzeug bei zügiger Fahrt unberechtigt eine Vollbremsung auslösen, könnte dies zu einer Massenkarambolage führen. Um das Risiko von Gefahr bringenden Fehlfunktionen von sicherheitsrelevanten Elektronik-Systemen zu minimieren, sollten diese unter Berücksichtigung einschlägiger Normen entwickelt werden. In der Vergangenheit galt die Empfehlung, elektrische/elektronische Systeme, die eine sicherheitsrelevante Funktion in Automobilen ausführen und deren Ausfall ein maßgebliches Risiko für Mensch oder Umwelt bedeutet, auf Basis der IEC 61508 zu entwickeln. Diese Norm ist generisch auf sicherheitsrelevante Produkte, wie ein Sicherheitsschaltrelais für eine Notstromabschaltung, anwendbar. Da dieser Standard für moderne Automotive-Anwendungen nicht ausreichend bzw. nicht spezifisch genug ist, wurde eine neue Norm erstellt.

Zu den Anwendern dieses Standards gehören Automobilhersteller, Automobilzulieferer und Prüfinstitute. Möchte beispielsweise ein Automobilhersteller oder -zulieferer ein sicherheitsrelevantes System bzw. eine Komponente entwickeln, muss dies anhand einer Sicherheitsnorm wie der ISO 26262 erfolgen. Um die funktionale Sicherheit des Produkts zu gewährleisten, wird von der ISO 26262 ab einem entsprechenden Sicherheitslevel gefordert, dass eine von der Entwicklung organisatorisch unabhängige Stelle (z. B. ein externes Prüfinstitut, u. U. aber auch eine interne QM-Stelle) hinzugezogen wird. Eine Prüfung durch eine für ISO 26262 gemäß EN ISO/IEC 17025 akkreditierte Prüfstelle kann dann neben dem Sicherheitsnachweis auch dem Reduzieren der Risiken im Bereich der Produkthaftung im juristischen Sinn dienen.

Die ISO 26262 ist nach einhelligem Verständnis der deutschen Experten zur funktionalen Sicherheit als Beitrag zum Stand der Wissenschaft und Technik in Bezug auf die funktionale Sicherheit von Straßenfahrzeugen anzusehen (Konsens bei der letzten Fachtagung zur funktionalen Sicherheit).

2 Inhalt

Die ISO 26262 besteht aus zehn Teilen, die folgende Inhalte abdecken:

1. Vokabular
2. Management der funktionalen Sicherheit
3. Konzeptphase
4. Produktentwicklung: Systemebene
5. Produktentwicklung: Hardwareebene
6. Produktentwicklung: Softwareebene

7. Produktion, Betrieb und Außerbetriebnahme
8. Unterstützende Prozesse
9. ASIL- und sicherheitsorientierte Analysen
10. Guideline (nur informativ)

Teil 1 erklärt die Begriffe und Abkürzungen, die in der Normenreihe verwendet werden.

Teil 2 beinhaltet die geforderten Managementtätigkeiten während der unterschiedlichen Phasen des Sicherheitslebenszyklus eines Systems, welches E/E-Subsysteme (Elektrik/Elektronik-Subsysteme) beinhaltet. Des Weiteren werden die organisatorischen Voraussetzungen genannt, die erfüllt sein müssen, damit das zu entwickelnde System gemäß dem geforderten ASIL (*automotive safety integrity level*) entwickelt werden kann.

Teil 3 enthält Anforderungen bezüglich der Durchführung einer Gefährdungsanalyse und Risikoabschätzung (*hazard analysis and risk assessment*). Dazu müssen zunächst die potentiellen Gefährdungen (*hazards*) des Systems identifiziert werden. Dies geschieht durch Betrachtung der Fehlfunktionen des untersuchten Systems in spezifischen Fahrsituationen. Anschließend wird jede Gefährdung mit einer Sicherheitsanforderungsstufe von A bis D klassifiziert bzw. als nicht sicherheitsrelevant eingeordnet (*quality management – QM*). Anders als zum Beispiel in der IEC 61508 geschieht die Risikoanalyse in der ISO 26262 mittels einer festgelegten, qualitativen Methodik. Dazu muss für jede identifizierte Gefährdung einzeln die Schwere der Auswirkung (*severity – S*), die Häufigkeit der Fahrsituation (*exposure – E*) und die Beherrschbarkeit der Fehlfunktion in der jeweiligen Fahrsituation z. B. durch den Fahrer (*controllability – C*) abgeschätzt werden. Aus einer vorgegebenen Tabelle lässt sich dann für jede Gefährdung die Einstufung QM oder ASIL A bis D ablesen.

Mit steigendem ASIL steigen auch die Anforderungen an die Sicherheit, die in den nachfolgenden Teilen spezifiziert sind. An Gefährdungen der Klasse QM sind keine Anforderungen gestellt, die über das übliche Qualitätsmanagement des Systemherstellers hinausgehen, und ihre Beherrschung kann deshalb durch eine erfolgreiche Umsetzung einer Qualitätsmanagementnorm, wie zum Beispiel der ISO 9001 oder der ISO/TS 16949 nachgewiesen werden.

Die Teile 4, 5 und 6 behandeln die Entwicklungsprozesse auf Systemebene, Hardwareebene und Softwareebene in Anlehnung an geschachtelte V-Modelle und definieren für die einzelnen Abschnitte Vorgehensweisen und Arbeitsergebnisse. Für die umzusetzenden Anforderungen werden Methoden aufgelistet, die je nach ASIL als *optional*, *recommended* (empfohlen) oder *highly recommended* (dringend empfohlen) eingestuft werden. Es können jedoch auch andere, nicht genannte Methoden verwendet werden, wenn deren Wirksamkeit zur Erfüllung der jeweiligen Anforderung begründet werden kann.

Teil 7 beinhaltet das prinzipielle Vorgehen beim Erstellen eines Produktions- und Installationsplans für sicherheitsrelevante Systeme, um die Anforderungen an die funktionale Sicherheit beim Produktions- und Installationsprozess sicherzustellen, sowie die Anforderungen, die den Betrieb, die Wartung, die Reparatur und die Stilllegung unter der Einhaltung aller Sicherheitsaspekte gewährleisten sollen.

Teil 8 beinhaltet sowohl die Beschreibung und Zuordnung von Verantwortlichkeiten innerhalb einer verteilten Entwicklungsumgebung, als auch der richtigen Spezifikation der Anforderungen an den gesamten Sicherheitslebenszyklus. Des Weiteren werden das Konfigurations- und Änderungsmanagement sowie das richtige Durchführen von Verifikationen und Dokumentationen erläutert. Dieser Teil der Norm beinhaltet ebenfalls jeweils einen Abschnitt zur Reduzierung von Risiken, die von Softwarewerkzeugen und Software- sowie Hardwarekomponenten herrühren. Darunter fallen beispielsweise Risiken, die durch Fehler im verwendeten Compiler entstehen.

Teil 9 beinhaltet die Regeln der ASIL-Dekomposition und der Kritikalitätsanalyse. Weiterhin enthält Teil 9 einen Abschnitt, der die Durchführung von Analysen abhängiger Ausfälle erläutert, um Common Cause Fehler oder kaskadierende Fehler zu identifizieren, sowie einen Abschnitt, der die unterschiedlichen Analyseverfahren zum Erkennen von sicherheitskritischen Fehlern und Ausfällen innerhalb eines E/E-Systems aufzeigt.

Teil 10 beinhaltet Anwendungsbeispiele, Erläuterungen und weiterführende Information zu einigen Bereichen des Standards.

3 Schlüsselbegriffe der Norm

Die folgenden Begriffe sind meist keine exklusive Schöpfung der ISO 26262, sie kennzeichnen allerdings den Fokus dieser Norm. Entsprechend der einzigen Sprachversion der Norm werden diese Begriffe in englischer Sprache und der üblichen deutschen Verwendung angegeben:

- *System* im Sinne der Norm kann das Fahrzeug als Ganzes oder auch eine Komponente sein. Da Fahrzeuge aus vielen Komponenten von Fremdfirmen (Zulieferern) bestehen, hat jeder dieser Zulieferer ein System (in der Norm auch als *Component* bezeichnet) als Teil des Gesamtsystems, das entwickelt werden muss.

  Ein System[3] besteht wenigstens aus einem Sensor, Logik (Steuerung, Regler) und einem Aktor.

- *ASIL*: Der bereits erwähnte ASIL wird in den verschiedenen Teilen der Norm genutzt, um Maßnahmen zu empfehlen. Vor allem in Teil 5 (Hardware)

und Teil 6 (Software) finden sich zahlreiche Tabellen mit Methoden und Empfehlungen, die vom ASIL abhängig sind.

Beispielsweise wird eine deduktive Analyse wie die FTA (Fault Tree Analysis, Fehlerbaumanalyse) erst ab ASIL C und D besonders empfohlen.[4]

Die Einstufung ist das Ergebnis einer Gefahren- und Risikoanalyse und bewegt sich zwischen QM (keine Anwendung der von der Norm empfohlenen Maßnahmen notwendig) bis zu den höchsten Anforderungen mit ASIL D

- *Safe State*, *Sicherer Zustand*: Wenn ein System durch seine Eigendiagnose eine Funktionsstörung erkennt, soll es in einen Zustand wechseln, in dem keine Gefahr mehr vom System ausgeht. Dieser sichere Zustand ist von der Art des Gesamtsystems abhängig. Bei einer Motorsteuerung eines Pkw könnte dies der Zustand „Motor aus“ sein, bei der Motorsteuerung eines Kleinflugzeuges (nicht im Fokus der ISO, nur als Beispiel) wäre es „Vollgas“.
- *Fault Tolerant Time Interval*, *Fehlertoleranzzeit*: Wenn ein Fehler vom System durch Eigendiagnose erkannt wird, muss der sichere Zustand erreicht werden, bevor ein System gefährlich ausfallen kann.

  Beispiel: Wenn eine Getriebesteuerung 50 ms braucht um die Kupplung zu öffnen, den Gang zu wechseln und die Kupplung wieder zu schließen, dann könnte der Fehler „*Ungewolltes Einlegen eines Ganges aus dem Leerlauf/Stillstand ohne Fahrereingriff*“ frühestens nach 50 ms auftreten, weil das Fahrzeug erst mit dem Schließen der Kupplung anfahren könnte. Der Mikroprozessor der Steuerung muss also mindestens einmal alle 50 ms prüfen und erkennen, ob die Leistungsendstufe für den Motor der Kupplungssteuerung sich durch einen Fehler verselbständigt haben könnte und in der Lage wäre, von alleine einen Gang einzulegen.
- *Freedom of Interference*, *Rückwirkungsfreiheit*: Hierbei geht es darum, dass in einem System nicht immer auf Komponenten zurückgegriffen werden kann, die nach der Norm entwickelt wurden. Solche Komponenten sind beispielsweise COTS-Produkte wie Mikrocontroller, Speicherbausteine, Betriebssysteme (z. B. nach Autosar-Standard) oder Treiber für spezielle Komponenten. Im Gegensatz dazu müssen Komponenten, die an Sicherheitsfunktionen beteiligt sind, besonders gegen die anderen Komponenten abgesichert werden. Ein Softwaremodul, welches eine sicherheitsrelevante Berechnung ausführt und den Wert speichert, muss beim Rückruf der gespeicherten Daten sicherstellen, dass diese zwischenzeitlich nicht verändert wurden, beispielsweise indem es die Daten in mehreren Kopien ablegt oder bei jedem Lesen/Schreiben Prüfsummen vergleicht/erstellt.
- *Hardware Architectural Metrics*, *Hardwaremetriken*: Bei den Metriken geht es darum, dass das System (gegebenenfalls jedes elektronische Bauteil im System) auf seine Ausfallmöglichkeiten hin untersucht wird. Dabei ist zu bewerten, wie häufig ein zufälliger Ausfall eines Bauteils das ganze System in einen unsicheren Zustand bringen könnte. Aus dieser Analyse soll dann abgeleitet werden, an welchen Stellen die Ausfallsicherheit des Systems verbessert werden kann und ob ein gewisses Niveau erreicht wird.

  Die Norm schlägt zwei Wege vor, diese Ausfallwahrscheinlichkeiten zu berechnen. Wichtigste Hilfsmittel sind dabei Fehlermodelle, die die Ausfallarten von Bauteilgattungen (wie Transistoren, Kondensatoren, Widerstände) beschreiben und Ausfallraten aus anderen Normenwerken (z. B. Siemensnorm SN 29500, siehe auch Failure in Time). Die Zusammenfassung erfolgt in einer FMEDA[5] oder einer FTA.
- *Proven-in-Use*, *Betriebsbewährtheit*: Wenn Komponenten eines Systems wiederverwendet werden sollen oder einige Zeit vor Inkrafttreten der Norm erfolgreich und fehlerfrei von Kunden verwendet wurden, kann man mit dieser Erfahrung den Entwicklungsaufwand bei Wiederverwendung reduzieren. Je nach Bedeutung können von der Norm geforderte Nachweise oder Maßnahmen entfallen. Voraussetzung ist eine Produktbeobachtung und die Analyse der Ausfälle, die in der Hand des Kunden aufgetreten sind.[6] Komponenten können Hardwarekomponenten und Softwaremodule sein, aber auch Teile der früher erarbeiteten Dokumentation, die selbst nur dem Nachweis einer sicheren Entwicklung dient.

4 Einzelnachweise

[1] Siehe ISO 26262-1:2011(E), Abschnitt „Scope“.

[2] www.iso.org.

[3] ISO 26262-1:2011 1.129 System.

[4] Beispielsweise in ISO 26262-4:2011 Abschnitt „7.4.3 Measures for the avoidance of systematic failures“ Tab. 1.

[5] Die Norm verwendet den Begriff FMEDA nicht, aber in ISO 26262-5:2011 Annex E finden sich Beispielrechnungen.

[6] ISO 26262-8:2011 Clause 14 „Proven in use argument“.

5 Literatur

- Marco Heinz Schlummer, "*Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie*", Dissertation an der Bergischen Universität Wuppertal, 2012
- Martin Hillenbrand, "*Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik / Elektronik Architekturen von Fahrzeugen*", Dissertation am Karlsruher Institut für Technologie, 2012, ISBN 978-3-86644-803-2
- Johannes Matheis, "*Abstraktionsebenenübergreifende Darstellung von Elektrik/Elektronik-Architekturen in Kraftfahrzeugen zur Ableitung von Sicherheitszielen nach ISO 26262*", Dissertation am Karlsruher Institut für Technologie, 2009, ISBN 978-3-8322-8968-3, Link zum Abstract
- Beispiel für eine Gefahren- und Risikoanalyse von Frederik Walderyd "*Hazard identification and safety goals on power electronics in hybrid vehicles* (PDF; 1,4 MB)" (engl.), Master Thesis an der Chalmers University of Technology, Göteborg 2010

6 Weblinks

- Überblicksartikel zur ISO 26262 auf elektronikpraxis.de

7 Text- und Bildquellen, Autoren und Lizenzen

7.1 Text

- **ISO 26262** *Quelle:* https://de.wikipedia.org/wiki/ISO_26262?oldid=151688015 *Autoren:* Aka, Matthäus Wander, Koppi2, Ralf Pfeifer, Käptn Weltall, Hydro, Jü, Hannes Kuhnert, Invisigoth67, BJ Axel, Tom md, Wosch21149, Omega prime, Andi Baer, Aleks-ger, Alexbot, S.Kriso, Poco a poco, Rr2000, Speedynet, Tetrapack-muc, MorbZ-Bot, KaiBorgeest, Bgeldrich, 46er, EmausBot, Jens Lüdemann, FuSi Experte, WikitanvirBot und Anonyme: 25

7.2 Bilder

7.3 Inhaltslizenz