1 Einleitung

Das Verhüten von Unfällen darf nicht als eine Vorschrift des Gesetzes aufgefasst werden, sondern als ein Gebot menschlicher Verpflichtung und wirtschaftlicher Vernunft.

(Werner von Siemens, 1880)

1.1 Wieso die automotive spezifische Sicherheitsnorm ISO 26262:2011?

NRMES

Einen wesentlichen Beitrag für die Einschätzung der Zukunft sicherer eingebetteter Systeme liefert die National Roadmap Embedded Systems (NRMES).

Die Kombination sicherer eingebetteter Systemkomponenten mit elektronischen und mechatronischen Systemen ist ein typisches Merkmal in der Technik, wie z. B. bei automobilen Sicherheitssystemen. Die NRMES stellt dar, dass eingebettete Systeme oftmals strikten sicherheitskritischen Anforderungen unterliegen, deren Verletzung verheerende Auswirkungen auf Mensch und Technik mit sich bringen kann.

Sicherheitsnachweis

So benötigen viele Systeme – z. B. in der Automobiltechnik, der Avionik oder der Medizintechnik – eine explizite Zulassung, die den Nachweis eines hinreichenden Sicherheitsniveaus erfordert. Für den Nachweis der Sicherheit eines Systems ist Korrektheit weder notwendige noch hinreichende Bedingung. Vielmehr folgt der Sicherheitsnachweis eigenen spezifischen Verfahren, die z. B. die Bestimmung und Bewertung von Risiken (Risikoakzeptanz) verlangen.

QS-Verfahren

In diesem Zusammenhang spielen Verfahren zur Qualitätssicherung (QS) wie Test, Analysetechniken und formale Beweisverfahren eine wichtige Rolle. Sie liefern einen Beitrag zur Zulassung, ersetzen sie jedoch nicht.

Bezug zur Software

In technischen Anwendungsbereichen geht von Softwarefehlern einerseits potenziell eine Gefährdung aus, andererseits ermöglicht Software aber auch die Unterstützung von Sicherheit, indem sie z. B. fort-

laufend Diagnosen des Systemzustands durchführt. Daher ist es unerlässlich, Software in die Sicherheitsanalyse und die Zertifizierung von eingebetteten Systemen einzubeziehen.

Branchen und funktionale Sicherheit

Eingebettete Systeme als bedeutende Innovationstreiber mit hoher querschnittlicher Wirkung bilden das Nervensystem moderner Steuer- und Informationssysteme. In ihnen ist inhärent die funktionale Sicherheit der jeweilig realisierten Produkte sicherzustellen. Dies gilt insbesondere in so wichtigen Gebieten wie Energietechnik, Medizin- und Gesundheitstechnik, Verkehrs- und Transportwesen (mit Automobil-, Schienen-, Luft- und Raumfahrttechnik), Industrieautomatisierung/ Robotik sowie der Informations- und Kommunikationstechnik mit ihren diversen Ausprägungen.

1.1.1 ISO 26262:2011, Edition 15.11.2011

Für die Automobiltechnik enthält der neue Standard ISO 26262:2011 (wir beziehen uns in diesem Fachbuch ausschließlich auf den Stand 15.11.2011 für die Teile 1 bis einschließlich 9 und den Stand 08.01.2012 für den Teil 10 des Standards) Richtlinien zur Entwicklung funktional sicherer Systeme.

Es gibt kaum noch Projekte in der Automobilindustrie, bei denen nicht Sicherheitsanforderungen nach einer ASIL-Klassifikation gefordert werden.

ASIL-Klassifikation

Der ASIL (Automotive Safety Integrity Level) wird nach bestimmten Parametern ermittelt und die Einstufung kann aus einer in der ISO 26262:2011 vorgegebenen Tabelle für jede Gefährdung in den Stufen QM oder ASIL-A bis ASIL-D abgelesen werden. Neuere Technologien wie Assistenzfunktionen und erweiterte Fahrzeugfunktionalitäten sowie die Entwicklung von Mehrwertfunktionen durch Integration bisher getrennter Funktionen führen dazu, dass eine zunehmende Anzahl softwareintensiver elektronischer Systeme als sicherheitsrelevant eingestuft wird und deshalb entsprechend dem Automotive-Sicherheitsstandard ISO 26262:2011 entwickelt werden muss.

Steigende Komplexität

Damit steigt einerseits die Zahl der sicherheitsrelevanten elektronischen Komponenten und Systeme, andererseits werden aber auch die Vernetzung, Interaktion und Komplexität sowie die Sicherheitsanforderungen untereinander immer komplexer. Zusätzlich zu den hohen Sicherheitsanforderungen der einzelnen Systeme wächst auch deren Komplexität bei der heute üblichen verteilten Durchführung der Entwicklungsprojekte. Die Einsatztauglichkeit derartig entwickelter Produkte erfordert einwandfrei funktionierende Hardware und Software in Bezug auf die zu erfüllenden Sicherheitsfunktionen. Neue Zukunfts-

technologien, wie z.B. Hybridantriebe und E-Fahrzeuge, beinhalten beträchtliches Entwicklungspotenzial.

1.1.2 Fachausschuss für Kraftfahrzeuge

Der Fachausschuss für Kraftfahrzeuge (FAKRA) bildete Ende 2003 eine Arbeitsgruppe mit dem Ziel, den generischen Standard IEC 61508 für die Automotive-Industrie zu interpretieren, um die Spezialisierung auf die Serienproduktion in der Automobilbranche abbilden zu können.

Durch die daraus resultierenden Management- und technischen Aktivitäten im Bereich der funktionalen Sicherheit (FuSi) sollen elektronisch basierte Elemente so sicher entwickelt werden, wie es nach dem Stand der Technik möglich ist.

1.1.3 Stand der Technik

Dazu wurde der Stand der Technik bezüglich aller Aspekte, die für die Sicherheit von Bedeutung sind, in der ISO 26262:2011 beschrieben.

Die branchenweite Definition, Einführung und Etablierung dieses überarbeiteten Standards sind abgeschlossen und der Standard wurde in 2011 ratifiziert.

Nachweisführung

Wird ein Fahrzeug auf allen Ebenen – auch bei allen Zulieferern – gemäß ISO 26262:2011 entwickelt und hergestellt, kann der Automobilhersteller den notwendigen Nachweis liefern, den Erfordernissen bei der Herstellung sicherheitskritischer, elektronischer Einrichtungen entsprochen zu haben. Einige sicherheitsrelevante Funktionen wie z.B. die vollständig elektronisch betätigte Parkbremse, die elektronische Lenksäulenverriegelung, veränderbare Dämpfercharakteristiken bei Fahrzeugen mit Luftfederung, das neue Aktiv-Lenksystem von BMW oder das Dynamic Steering von AUDI, das durch gezieltes Gegenlenken zur Fahrstabilität beiträgt, wurden bereits in Anlehnung an die IEC 61508 bzw. den Normenentwurf der ISO/DIS 26262:2009 entwickelt sowie einem unabhängigen Assessment unterzogen. Diese Entwicklungen erfüllen die höchsten Sicherheitsanforderungen gemäß dem Stand der Technik.

1.1.4 ISO 26262:2011 – eine anwendbare Norm

Die steigende Zahl von Rückruf- und Serviceaktionen in den letzten Jahren bekräftigen die Entscheidung für die Anwendung dieses aktuellen Sicherheitsstandards für funktionale Sicherheit von Straßenfahrzeugen < 3,5 t und die darin geforderte Einführung eines funktionalen Sicherheitsmanagements (FSM) bei allen beteiligten Firmen vor Projektstart.

Produktvertrauen und Sicherheit

Eine im Jahr 2010 veröffentlichte Statistik des Kraftfahrt-Bundesamtes (KBA) bezifferte mit 185 Rückrufaktionen einen Rekord. Im Jahr 2000 mussten die Hersteller im Vergleich nur 72-mal Fahrzeuge zurückrufen. Wie das Beispiel einer Gaspedal-Rückrufaktion eines asiatischen OEM zeigt, kann das Vertrauen des Konsumenten in eine Fahrzeugmarke im Extremfall zu Absatzeinbußen und zum Imageschaden führen.

Produkthaftung

Seit der Veröffentlichung der ISO 26262:2011 steht der Automobilbranche eine anwendbare Norm zur funktionalen Sicherheit zur Verfügung, die unter Beteiligung der Automobilindustrie entstand und deren speziellen Belange berücksichtigt. Es gibt derzeit keine Richtlinie und kein Gesetz, das OEMs, Supplier oder Second Tiers zur Anwendung der ISO 26262:2011 verpflichtet. Allerdings definiert eine Norm wie diese immer den Mindeststand der Technik, d.h., im Falle einer Produkthaftung muss nachgewiesen werden, dass der Stand der Technik erreicht wurde. Ohne Anwendung der ISO 26262:2011 wird es im Produkthaftungsfall für die beteiligten Firmen schwierig werden, den Nachweis zu führen, dass der Stand der Technik bzw. Stand der Wissenschaft und Technik eingehalten wurde. Selbst bei deren Umsetzung ist man bei einem Produkthaftungsfall nicht auf der sicheren Seite, weil eben nur dieser Mindeststand der Technik durch eine Norm wie die ISO 26262:2011 repräsentiert wird.

Stand von Wissenschaft und Technik

Der OEM (in unserem Beispiel die Fa. Drivesmart AG) und der Supplier (in unserem Beispiel die Fa. safehicle GmbH) haben also nach wie vor die Verpflichtung, sich nach der Weiterentwicklung des Stands von Wissenschaft und Technik zu erkundigen und sich danach zu richten.

1.1.5 Beweislastumkehr

Werden die Anforderungen einer Norm wie der ISO 26262:2011 bei einer gemeinsamen Entwicklung des elektronischen Lenksystems nicht erfüllt und es kommt in einem Produkthaftungsfall zu dem Vorwurf, der Schaden sei entstanden, weil das Produkt nicht dem Stand von Wissenschaft und Technik entsprochen habe, so ist man gezwungen, das Gegenteil zu beweisen – **Beweislastumkehr**. Dies kann sich beliebig schwierig bis unmöglich gestalten.

1.2 Stufenweise zum ASIL-konformen Produkt

Die ISO 26262:2011 stellt erhebliche Anforderungen an die Verantwortlichkeiten, Entwicklungsprozesse, Dokumentation und Techniken bei der Entwicklung sicherheitsrelevanter Systeme.

Um professionelle Lösungen im sicherheitsrelevanten Bereich zeitnah zu entwickeln, ist fundiertes Know-how durch berufliche Qualifikation und Projekterfahrung notwendig.

Nachweispflicht

Hier unterscheidet sich die Norm nicht wirklich von den Anforderungen an Projekte aus dem nicht sicherheitskritischen Bereich, aber sie verlangt eindeutige Nachweise für diese Qualifikationen.

Notwendigkeit von Prozessen

Es bedarf integrierter, normkonformer und phasenorientierter Prozesse mit methodischen Ansätzen für alle Phasen der Entwicklung, Produktion und Außerbetriebnahme. Also Prozesse, die wirklich über den gesamten Sicherheitslebenszyklus eines Produkts definiert, eingeführt, etabliert, steuerbar, kontrollierbar und verfolgbar sind. Zusätzlich werden die verwendeten Prozesse durch moderne Werkzeuge unterstützt. Definierte und nachvollziehbare Meilensteine und Freigaben sind unabdingbar.

1.2.1 Klare Zuordnung von Verantwortung

Wichtigster Aspekt, um ein Projekt nach den Anforderungen dieser ISO-Norm erfolgreich zu bewältigen, sind die Zustimmung und Verpflichtung der Entscheidungsträger und die klare Zuordnung von Verantwortung.

Die Norm behandelt diese Anforderungen ausführlich und verlangt eine Kultur des sicherheitsbewussten Denkens und Vorgehens im Unternehmen. Abbildung 1–1 zeigt aufeinander aufbauende Schritte, die im Sicherheitslebenszyklus unerlässlich sind.

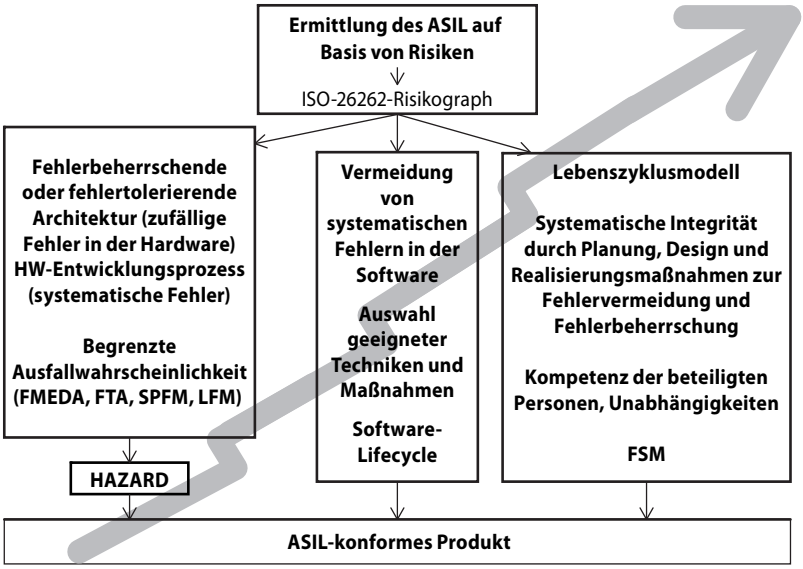

Abb. 1–1
Grundsäulen der ISO 26262:2011

Im Verlauf dieses Fachbuches stellen wir Ihnen die Planungsaktivitäten sowie abhängige Arbeitsprodukte samt Methoden und Verfahren vor.

G&R

Im Rahmen der Gefährdungs- und Risikoanalyse (G&R) werden die Gefährdungsszenarien erarbeitet und auf Basis der erkannten Risiken der ASIL ermittelt.

Hierauf gehen wir in Kapitel 8 »Gefährdungs- und Risikoanalyse« detailliert ein.

Zielsetzung

Ziel ist immer, dass zufällige Fehler, systematische Fehler und Common-Cause-Fehler nicht zu einer Fehlfunktion des sicherheitsrelevanten Systems führen und dass als Ergebnis dadurch die Verletzung oder der Tod von Menschen verhindert wird.

Item-Definition und Sicherheitslebenszyklus

Mit der Item-Definition erfolgt die Feststellung, ob es sich um eine Neuentwicklung oder um eine Modifikation handelt, und daraus resultierend muss der gesamte Sicherheitslebenszyklus oder ein geteilter Sicherheitslebenszyklus angewendet werden.

1.2.2 Prozessmodell und Reifegrade von Prozessen

V-Modell

Ein mögliches phasenorientiertes Prozessmodell für die Entwicklungsphasen ist das V-Modell 97 bzw. das V-Modell XT.

Die phasenorientierte und qualitätsgesicherte Projektbearbeitung ist eine zwingende Voraussetzung zur Entwicklung sicherheitsrelevanter eingebetteter Systeme.

Prozessreife

Der Reifegrad der angewandten und gelebten Entwicklungsprozesse kann beispielsweise durch Assessments nach Automotive SPICE bzw. nach CMMI bestimmt werden, um aus den daraus abgeleiteten Optimierungsmaßnahmen die Voraussetzungen für Safety-Compliant-Prozesse zu unterstützen. Allerdings reichen die Maßnahmen aus solchen Reifegrad-Assessments nicht aus, da nicht alle Teile der ISO 26262:2011 durch die geprüften Prozesse adressiert werden. Wir gehen in diesem Buch nicht weiter auf Assessments und Prozesse nach diesen Reifegradmodellen ein, da es hierzu bereits ausreichende und vielseitige Literatur gibt, die wir in Anhang F gerne empfehlen.

Genannte Fachbegriffe erläutern wir Ihnen im Verlauf des Buches bzw. sie sind im Glossar enthalten.

Das nächste Kapitel gibt einen Überblick zum Umfang, zum angesprochenen Leserkreis und zur effektiven Nutzung dieses Fachbuches und führt Sie in die Projektstory ein.