1 Einleitung

Die ISO 26262 verändert zurzeit die Fahrzeugentwicklung in einer Form, wie man sich das vor 10 Jahren, als das Thema Funktionssicherheit in der Automobilindustrie stärker in den Vordergrund getreten ist, nie hätte vorstellen können. Als sich Anfang des 21. Jahrhunderts die ersten deutschen Arbeitskreise mit dem Thema beschäftigt hatten und bereits 2005 die ersten internationalen Gremien dazu gebildet wurden, wollte man als Antwort auf die Frage nach der Produktsicherheit eine schlanke Lösung. In den Jahren bis zur endgültigen Veröffentlichung der ISO 26262 sind zehn Bände mit etwa 1000 Anforderungen entstanden. In all diesen Jahren sind viel Wissen, Methodik und auch Lösungsansätze diskutiert worden, die nur in Fragmenten in die Norm als Anforderung, Hinweise (Notes) oder informative Kapitel eingeflossen sind. Derzeit gibt es in jedem Land weitere Normvorhaben, die sich teilweise nur mit der Übersetzung der ISO 26262, aber auch mit der Methodenentwicklung zur ISO 26262 beschäftigen. Die ISO 26262 wurde nicht als Richtlinie geschrieben, sondern sie stellt nur Anforderungen an Aktivitäten und Methoden, die bei den jeweiligen Sicherheitsaktivitäten berücksichtigt werden sollen. Dabei hat man weitgehend darauf verzichtet anzugeben, wie man etwas im Sinne der Norm umsetzen muss. Dies hängt in erster Linie damit zusammen, dass ein Sicherheitsstandard weitgehend den Stand der Technik widerspiegelt und somit solche Vorgaben oft nur für einen bestimmten Zeitausschnitt gültig sind. Welches Design als sicher bezeichnet werden kann oder welche Methode sich als geeignet zeigt, stellt sich oft nur als ein kleines Zeitfenster dar. Sicherheitsdesign und auch Methoden zur Sicherheit sollen sich kontinuierlich weiterentwickeln und nicht durch Normen zum Stillstand gezwungen werden. Das Bedürfnis nach einer Richtlinie ist sehr groß, aber auch dieses Buch, welches einen weiteren Einblick in die Hintergründe der Norm gewähren soll, hat nicht den Anspruch die korrekte Umsetzung der ISO 26262 wiederzugeben. Mit den Hinweisen zu den Methoden, die den Schwerpunkt dieses Buchs darstellen, kann allgemein keine einzige Anforderung der Norm erfüllt werden. Die Normerfüllung kann nur im Kontext der konkreten Produktentwicklung geschehen.

Oft werden in der ISO 26262 verschiedene Anforderungen und Hinweise für den Leser recht komplex beschrieben. Diese Formulierungen sind Kompromisse, die die

Experten, welche die Norm entwickelt haben, eingehen mussten. Daher sind alle Übersetzungen in diesem Buch bereits mögliche Interpretationen, die unter einem anderen oder zukünftigen Kontext komplett anders interpretiert oder übersetzt werden können. Allen Lesern kann man nur den Hinweis geben, sich bei der Auslegung und Anwendung der Normen in der Praxis an die Texte der ISO 26262 zu halten.

1.1 Begriffe und Übersetzungen aus der ISO 26262

Die ISO 26262 wurde nur in englischer Sprache verfasst, selbst die übliche Übersetzung ins Französische wurde wegen indifferenter Nutzung von Begriffen nicht umgesetzt. Somit gilt für die ISO 26262 als eine der wenigen Normen auch der englische Text in Frankreich als normativ. Nur Japan hat indes eine japanische Übersetzung veröffentlicht. Dies war auch notwendig, da der typische Entwickler in Japan doch Schwierigkeiten hat, die englische Sprache zu lesen oder zu interpretieren. Für die Worte Verifikation, Analyse, Untersuchung, Validation, Überprüfung gibt es nur ein japanisches Wort, daher müssen entsprechende Übersetzungshilfen her. Es wurde von den japanischen Übersetzern versichert, dass der Inhalt sich nicht verfälscht hätte. Aber selbst bei der Übersetzung ins Deutsche fällt es schwer, die richtigen Worte zu definieren. Begriffe wie Verifikation, Analyse und Validation werden hier gemäß ISO 26262 benutzt. Die folgenden Begriffe aus dem Glossar der ISO 26262 wurden in diesem Buch angepasst. Die in diesem Buch blau hinterlegten Kästen sind freie Übersetzungen der ISO 26262, die aber dem Verständnis des Autors entstammen. Ganz freie Interpretationen, Meinungen oder gar Empfehlungen des Autors sind in normaler Schrift wie der allgemeine Text des Buches geschrieben. Wörtliche Zitate sind kursiv geschrieben.

Bewertung (Assessment) der Funktionalen Sicherheit

1.4 (Assessment)

Untersuchung einer Eigenschaft eines Fahrzeugsystems (1.69) oder Elementes (1.32)

Hinweis: Einen gewissen Grad der Unabhängigkeit (1.61) einer gewissen Partei oder Parteien, die ein Assessment durchführen, sollte für jedes Assessment gewährleistet sein.

Allgemein wird das Word „Assessment“ mit Beurteilung übersetzt. Die Untersuchung (examination) wird als Basis für eine Beurteilung (Assessment) gesehen. Wenn es um die Aktivität „Functional Safety Assesment“ gemäß der ISO 26262 geht, so wird der Begriff „Assessment der Funktionalen Sicherheit“ benutzt.

1.6 ASIL (Automotive Safety Integrity Level)

ASIL bezeichnet eines von insgesamt vier Levels zur Vermeidung von nicht tolerierbaren Restrisiken. Der ASIL verweist auf Sicherheitsmaßnahmen und notwendige Anforderungen aus der ISO 26262 für das Fahrzeugsystem (Item, 1.69) oder einzelne Elemente (1.32). Dabei steht ASIL D für das höchste und ASIL A für das niedrigste Sicherheitslevel.

Im Rahmen dieses Buches wird nur der Begriff „ASIL“ verwendet.

Die ISO 26262 gibt bereits in Teil 10 eine Beschreibung der Elemente eines Fahrzeugsystems, wobei ein Element ein System, ein Subsystem (logisches oder technisches Element und damit auch eine Funktionsgruppe), eine Komponente, ein HW-Bauelement oder eine SW-Unit sein kann.

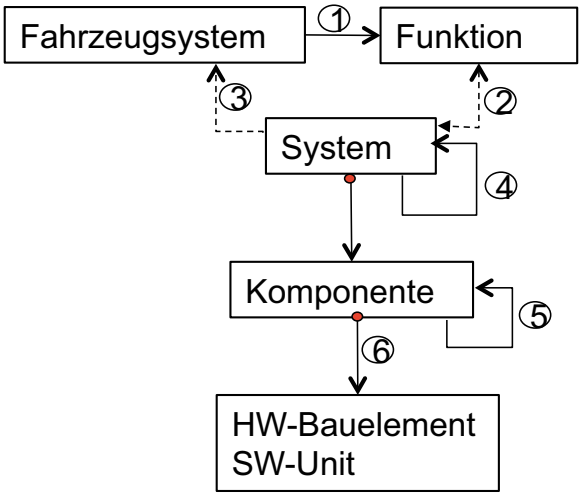

Bild 1.1 Elemente eines Fahrzeugsystems (Quelle: ISO 26262, Teil 10, Bild 3)

Teil 1 der ISO 26262 wird unter 1.69 Fahrzeugsystem (Item) wie folgt beschrieben:

1.69 (Fahrzeugsystem, item)

System (1.129) oder Feld von Systemen, welche eine Funktion auf Fahrzeugebene realisiert, auf welches die ISO 26262 angewendet werden soll.

Item wird als Fahrzeugsystem übersetzt, wenn es sich im das konkrete „Item“ aus der ISO 26262 handelt. Historisch gesehen, sollte der Begriff „Betrachtungseinheit“ für „Item“ verwendet werden, durch die Definition des Begriffes liegt der Begriff Fahrzeugsystem näher. Ist dies wichtig, wird in Klammern der Begriff „Item“ ergänzt. Der Begriff „Feld von Systemen“ wird im Kapitel 4 kritisch hinterfragt, bei einer systematischen hierarchischen Gliederung sollte es sich um Systeme und zugeordnete Subsysteme handeln.

Das Bild 3 (hier Bild 1.1) aus dem Teil 10 kann wie folgt aus dieser Definition abgeleitet werden:

1. System (1.129) oder mehrere Systeme, die eine (oder mehrere) Funktion(en) auf Fahrzeugebene realisieren, auf die die ISO 26262 angewendet werden.
2. Ein System kann eine oder mehrere Funktionen realisieren, es kann aber auch eine Funktion auf mehreren Systemen realisiert werden.
3. Ein Fahrzeugsystem besteht aus einem oder mehreren Systemen, wobei ein System aus mindestens einem Sensor, einer Verarbeitung und einem Aktuator besteht. Die ISO 26262 zieht in einer Note den Schluss, dass ein System mindestens drei Elemente haben sollte, jedoch wäre es denkbar, dass zum Beispiel ein Aktuator in die Verarbeitungseinheit integriert wäre.
4. Ein System kann in beliebige Subsysteme gegliedert werden, wobei laut ISO 26262 die Systeme nicht hierarchisch gegliedert sein müssen. Handelt sich es um Systeme, die gemeinsam Funktionen mit höherem ASIL realisieren sollen, wird man wegen der Mehrfachfehlerbeherrschung eine eindeutige hierarchische Gliederung der Systeme definieren müssen.
5. Ein System (oder Subsystem) besteht aus einer oder mehreren Komponenten.
6. Die Komponenten bestehen aus (elektrischen) HW-Bauelementen (HW-Parts) oder aus SW-Units.

Die Begriffe wie Modul, SW-Datei etc. werden in der ISO 26262 nicht definiert. Bei integrierten Halbleitern wird man auch über Sub-Parts sprechen, damit sind logische Funktionselemente gemeint, die bestimmte Funktionen und Sicherheitsmechanismen innerhalb eines integrierten Halbleiters realisieren.

1.2 Fehlerbegriffe der ISO 26262

Die Norm gibt die Begriffe wie folgt in ihrem Band 1 vor:

1.36 (Fehler, error)

Abweichung zwischen einem ausgeführten, beobachteten oder gemessenen Wert oder einer Bedingung (Zustand) und dem wahren, spezifizierten oder theoretisch korrekten Wert oder der Bedingung (Zustand).

Hinweis 1: Ein Fehler (error) kann durch eine unvorhersehbare Betriebsbedingung oder durch eine Abweichung (fault, 1.42) im System (1.129), Subsystem oder in Komponenten (1.15) auftreten.

Hinweis 2: Eine Abweichung (fault) kann selbst als ein Fehler innerhalb des betrachteten Elementes interpretiert werden und schließlich als Ursache zu einem Ausfall (failure) führen.

1.39 (Ausfall, failure)

Die Fähigkeit, dass ein Element (1.32) eine geforderte Funktion erfüllen kann, ist nicht mehr gegeben.

Hinweis: Fehlerhafte Spezifikationen sind Quellen für Ausfälle.

1.42 (Abweichung, fault)

Nicht normaler Zustand (Bedingung), welcher Ursache für ein Fehlverhalten eines Elementes (1.32) oder Fahrzeugsystems (1.69) sein kann.

Hinweis 1: Permanente, intermittierende oder transiente Abweichungen (1.134) (insbesondere „Soft-Errors“) werden betrachtet.

Hinweis 2: Eine intermittierende Abweichung tritt zeitweise immer wieder (sporadisch) auf. Diese Abweichungen können auftreten, wenn technische Komponenten (1.15) das Ende ihrer Lebensdauer erreicht haben (Spezifikation) oder auch durch Störungen (prellen) an einem Schalter entstehen. Einige systematische Abweichungen (1.131) (zum Beispiel zeitliche Grenzlagen) können zu intermittierenden Abweichungen führen.

Bei der Übersetzung wurden Annahmen getroffen, die hier erläutert werden.

„Fault“, „failure“ und „error“ werden oft wie folgt übersetzt:

Fault: Abweichung, Anomalie, Mangel, Defekt, Nicht-Konformität

Error: Irrtum, Störung oder Fehler

Failure: Versagen oder Ausfall.

Die Zusammenhänge dieser drei Begriffe und auch deren Modell der Fehlerpropagation wird im Kapitel 4.4.2 beschrieben. Hier muss nur angemerkt werden, dass der Begriff „Fehler“ im Deutschen allgemeiner gefasst ist und damit in diesem Buch in erster Linie als Sammelbegriff für alle drei Begriffe benutzt wird. Wird Fehler rein nur als „error“ betrachtet, dann wird dies im Kontext erklärt.

In der Sicherheitsbetrachtung werden auch folgende Aspekte unterschieden:

- Einfachfehler (oder Einzelfehler) und
- Mehrfachfehler.

Wenn ein einziger Fehler oder eine Abweichung von einem beobachtbaren Verhalten oder Eigenschaft alleine zu einem Versagen eines Systems führt, so bezeichnet man dies als Einfachfehler. Führen nur mehrere Fehler oder Abweichungen zu unbeabsichtigtem geänderten beobachtbaren Verhalten oder zu geänderten Eigenschaften, so bezeichnet man diese Fehler als Mehrfachfehler. Bei Doppelfehlern müssen zwei Fehler zu einem solchen Versagen führen. Im Rahmen der ISO 26262 wird diese Bezeichnung nicht auf ein Systemverhalten bezogen, sondern auf ein Sicherheitsziel. Zum Beispiel verletzen Einfachfehler, die im spezifizierten Zustandsraum auftreten, immer unmittelbar ein Sicherheitsziel, sonst sind es keine Einfachfehler.