ISO 26262: Beurteilung der Pkw-Sicherheit

Normiert auf die Straße

Peter Löw, Roland Pabst, Erwin Petry

In mehreren Beurteilungsrunden prüfen Fachleute, ob ein neues Fahrzeug den Ansprüchen der Norm ISO 26262 an die funktionale Sicherheit genügt. Dabei gehen sie nach einem klaren Plan vor. Die Freigabe des Autos für den Straßenverkehr regelt jedes Land selbst.

Das tatsächliche Erreichen von funktionaler Sicherheit nach der Norm ISO 26262 muss in jedem Fall für das in Verkehr gebrachte Produkt nachgewiesen werden. Dieser Nachweis erfolgt aber nicht durch eine einzige Beurteilung am Ende der Entwicklung. Das wäre ein viel zu großes Risiko für das Projekt. Sie ist vielmehr eine inkrementelle Tätigkeit mit Zwischen-Assessments und einem abschließenden Gutachten.

Es wird empfohlen, nach Abschluss einer Phase des Sicherheitslebenszyklus oder des Projekts ein Zwischen-Assessment durchzuführen, das sich vor allem mit dem soeben erstellten Hauptergebnis befasst und dieses beurteilt. Die einzelnen Assessments könnten sich beispielsweise beziehen auf: Gefährdungs- und Risikoanalyse, das funktionale Sicherheitskonzept, das Systemdesign, das Softwaredesign oder einige wenige Entwicklungsmuster des Produkts zum Abschluss der Hauptentwicklungszyklen. Außerdem bieten sich einzelne Analyseergebnisse zur Beurteilung an, zum Beispiel Kritikalitätsanalyse oder FMEDA (Failure Modes, Effects and Diagnostic Coverage Analysis). Ein solches Vorgehen ist dringend angeraten. Es vermeidet späte Überraschungen und sorgt rechtzeitig für Korrekturmaßnahmen und Disziplin im Projekt.

Die Beurteilung der funktionalen Sicherheit ist eine wichtige Tätigkeit, die geplant werden muss und nach einem Prozess gesteuert durchgeführt werden sollte. Die Abbildung zeigt eine Übersicht eines typischen Assessment-Prozesses, bestehend aus den Phasen Vorbereitung, Durchführung, Bericht und Korrektur.

Alle Schritte dokumentieren

Wie für einen Prozess üblich, sollte jeder einzelne Prozessschritt beschrieben sein und zwar zum Beispiel durch folgende Angaben:

- verantwortliche Rolle
- durchzuführende Aktivitäten
- Angaben zum Zeitpunkt, der Dauer und den Abhängigkeiten der Prozessschritte
- Start- und Endekriterien für den Prozessschritt
- Eingabeinformationen für den Schritt (Input) und Ergebnisse des Schritts (Output)
- vorgeschriebene und empfohlene Hilfsmittel

Im Folgenden gehen wir auf wesentliche Aspekte der einzelnen Prozessschritte ein. Eine Beurteilung beginnt mit einer Beauftragung dafür. Dafür ist der Funktionssicherheitsbeauftragte im Projekt zuständig. Ziel und Umfang der anstehenden Beurteilung sind festzulegen und mit dem Assessor ist eine Vereinbarung zu treffen. Ergebnis ist eine schriftliche Assess-

ment-Beauftragung. Von nun an liegt die Verantwortung für die detailliertere Planung und die Durchführung beim Assessor. In der Praxis wird die Rolle des Sicherheits-Assessors häufig durch eine Person einer externen Organisation besetzt. Zertifizierungs- und Prüforganisationen und Beratungsunternehmen bieten solche Dienstleistungen an. Die Hauptgründe für eine externe Vergabe sind Zweifel an der eigenen Unabhängigkeit und Beurteilungsfähigkeit sowie ein höherer Stellenwert eines solchen externen Gutachtens in den Augen der Kunden. Nach der Erfahrung der Autoren sollten sich gerade größere Unternehmen hier aber mehr zutrauen und im eigenen Unternehmensverbund für den Aufbau entsprechender Stellen sorgen. Dies zahlt sich langfristig aus.

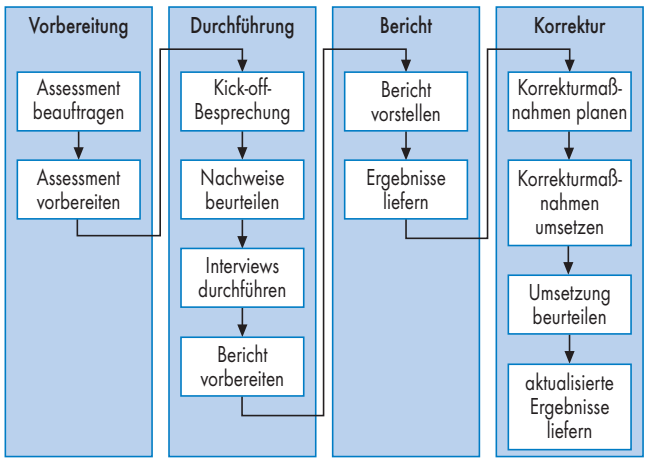
Der Assessor verschafft sich durch Vorgespräche einen tieferen Einblick in die Aufgabenstellung. Er stellt eventuell ein Assessment-Team zusammen, informiert sich über die Zuständigkeiten im Projekt und fordert bestimmte Unterlagen des Projekts vorab an. Typisch sind etwa folgende Unterlagen:

- Prozessdokumentation
- Organigramme
- Konfigurationsmanagementplan oder Inhaltsverzeichnis des Sicherheitsnachweises
- Gefährdungs- und Risikoanalyse
- Sicherheitsplan
- funktionales und technisches Sicherheitskonzept
- Design
- Ergebnisse von Sicherheitsanalysen
- Verifikations- und Validierungsplanung
- frühere Assessment-Berichte
- Auditberichte
- Argumentationen zur Betriebsbewährtheit
- Qualifikationsunterlagen zu Werkzeugen und Komponenten

In der nun folgenden eigentlichen Beurteilungsphase mit der Analyse der Nachweise, Interviews und der Vorbereitung des Berichts wird gemäß dem aufgestellten Plan meist iterativ vorgegangen. Es ist wichtig, dass der Assessor hier systematisch agiert. Als besonders nützlich haben sich zwei Hilfsmittel erwiesen: ein Werkzeug, das den Assessor durch die relevanten Anforderungen der anzuwendenden Sicherheitsnorm führt und eine Vorlage für den Bericht, in dem die Erkenntnisse kontinuierlich dokumentiert werden. Das Werkzeug enthält die Beurteilungskriterien, eine Sammlung von einleitend zu stellenden offenen Fragen, Hinweise zur möglichen Umsetzung der Anforderungen der Norm sowie Raum zur Dokumentation der Antworten und Nachweise, der Erkenntnisse und der Beurteilung. Es ist üblich, hierfür eine Excel-Datei zu verwenden, die entweder Bestandteil des Werkzeugkastens des externen Assessors ist oder von der Organisation als Bestandteil des Sicherheitsprozesses für interne Assessoren entwickelt wurde.

Es hängt von vielen Faktoren ab, wie die Befragung von Personen, das Sammeln der Nachweise, die Prüfung der Inhalte und das Erstellen des Berichts konkret ablaufen. Der Assessor muss sich auf die entsprechenden Umstände einstellen und angemessen vorgehen. Geht es zum Beispiel in einem Zwischen-Assessment um die Beurteilung einer ganz bestimmten Analyse, dann steht vielleicht nur genau ein Dokument im Zentrum der Beurteilung. Es ist vielleicht ausreichend, mit dem Autor zu sprechen und das ein oder andere Dokument mit Randbedingungen anzusehen.

Geht es dagegen um die Sicherheitsbeurteilung des Entwicklungsstands eines Musters, sollte man nicht nur Testkriterien und Testergebnisse ansehen. Man muss verstehen und beurteilen, wie in der Entwicklungsphase vorgegangen wurde. Hierbei ist der Assessor viel stärker auf die Befragung von verschiedenen Mitarbeitern angewiesen.



Ein typischer Prozess für ein Sicherheits-Assessment besteht aus den Phasen Vorbereitung, Durchführung, Bericht und Korrektur.

Ist abschließend das fertige Produkt zu beurteilen, steht der Safety Case im Vordergrund. Ist er sauber aufgebaut, lässt er sich systematisch prüfen. Bei einer solchen vollständigen Beurteilung empfehlen sich die abwechselnde Durchführung von Interviews und die Prüfung von Dokumenten.

Keine Bewertungsskala

Die Normen für die funktionale Sicherheit stellen in der Regel keine Skala zur Bewertung einzelner Anforderungen zur Verfügung. Sie geben lediglich für die Gesamtbeurteilung die *Annahme*, *bedingte Annahme* oder die *Ablehnung* vor. Die Autoren empfehlen, dass der Assessment-Prozess eine Regelung enthält, wie einzelne Normanforderungen charakterisiert und wie solche Einzelcharakterisierungen aggregiert werden. Folgendes Verfahren kann beispielsweise angewendet werden.

Einzelne Anforderungen werden charakterisiert als „erfüllt“ (grün = Acceptance), „bedingt erfüllt“ (gelb = Qualified Acceptance) oder „nicht erfüllt“ (rot = Rejection). Für jede *bedingt erfüllte* oder *nicht erfüllte* Anforderung wird ein Argument (eine Erkenntnis) zur Begründung und Erläuterung formuliert. Im Fall mindestens einer *bedingt erfüllten* Anforderung und keiner *nicht erfüllten* Anforderung wird für den Beurteilungsgegenstand eine *bedingte Annahme* ausgesprochen. Können die beanstandeten Punkte noch korrigiert werden, lässt sich später die funktionale Sicherheit bescheinigen. Im Fall mindestens einer nicht erfüllten Anforderung wird die funktionale Sicherheit nicht bescheinigt und insgesamt ablehnend beurteilt. *Nicht erfüllt* sollte vergeben werden, wenn die funktionale Sicherheit gefährdet ist. Dies heißt im Umkehrschluss, dass eine *bedingte Annahme* voraussetzt, dass die funktionale Sicherheit (in ihrem Kern) nicht gefährdet ist und die Beanstandungen eher im Rahmen von Beurteilungsspielräumen liegen oder nur indirekt eine Gefahr darstellen.

Häufig wird im Fall einer Ablehnung keine punktuelle Nachuntersuchung stattfinden, sondern das ganze Sicher-

heits-Assessment wiederholt. Vereinbart man dies als automatische Konsequenz, sollten einzelne Anforderungen nur als *nicht erfüllt* charakterisiert werden, wenn ihre Nichterfüllung so fundamental ist und solch weitreichende Auswirkungen hat, dass dies die komplette Wiederholung des Sicherheits-Assessments rechtfertigt.

Es stellt sich in diesem Zusammenhang die Frage, was eine einzelne Anforderung der Norm ist, die atomar bewertet wird. Wir empfehlen, nicht jeden einzelnen Satz der Norm zu nehmen, sondern eine kleine Menge thematisch zusammengehörender Forderungen atomar zu bewerten.

Gesamtschau ist entscheidend

Beispiel: Die Sicherheitsnormen enthalten eine Reihe von Forderungen zu der Art und Weise, wie jede einzelne Software-Sicherheitsanforderung spezifiziert sein muss: zum Beispiel verständlich, unzweideutig, atomar, testbar, mit ASIL (siehe Artikel „In Serie“ auf Seite 115), rückverfolgbar, eindeutig identifizierbar. Es wäre zu kompliziert, diese einzelnen Eigenschaften von Anforderungen getrennt zu bewerten. Es ist vielmehr sinnvoll, diese Eigenschaften in ihrer Gesamtheit zu bewerten und im Fall von Auffälligkeiten konkret zu formulieren, worin das Problem besteht. Mit dieser Vorgehensweise lässt sich angemessen würdigen und bewerten, was Sinn und Zweck all der detailliert aufgeschriebenen Forderungen ist. Es ist Aufgabe des Assessors, die Norm im Kontext des konkreten Umfelds zu interpretieren. Es ist nicht seine Aufgabe, sich sklavisch an die Formulierungen der Norm zu halten. Er ist es, der die Norm als Ganzes verstanden haben muss und den Zusammenhang zwischen den einzelnen Klauseln der Norm bei seiner Bewertung im Blick behält.

Führt ein Assessment-Team die Beurteilung durch, kommt es immer an der ein oder anderen Stelle zu unterschiedlichen Bewertungen und Formulierungen der Ergebnisse durch die Mitglieder. Wie damit umgehen? Natürlich wird man die entsprechenden Punkte diskutieren und versuchen, ein Ergebnis zu erzielen, mit dem alle Teammitglieder leben können. Ist dies aber nicht möglich, hat der Sicherheits-Assessor oder Teamleiter das letzte Wort. Er steht mit seinem Namen für das Gesamtergebnis gerade und muss letztlich jeden Satz und jede Beurteilung vertreten können. Im Gegensatz dazu ist es bei Prozess-Assessments gegen Reifegradmodelle üblich, einen Konsens zu erzwingen. Das heißt aber, dass es einzelne Stellen im Bericht geben kann, die zum Beispiel als „nicht bewertet“ oder „Minderheitsvotum“ gekennzeichnet sind, weil eine Einigung darüber nicht möglich war. Ließe man solche Kennzeichnungen bei der Beurteilung der funktionalen Sicherheit zu, ergäben sich Lücken und Unklarheiten in der Beurteilung, was zumindest bei einer abschließenden Beurteilung am Projektende nicht sein darf.

Die Norm fordert als Voraussetzung für die Freigabe eine erfolgreiche Beurteilung der funktionalen Sicherheit der Betrachtungseinheit und das Vorliegen des Sicherheitsnachweises. Zur eigentlichen Freigabe auf Fahrzeugebene nennt die Norm drei Forderungen:

- Es muss einen Produktfreigabebericht geben, mit Name, Unterschrift, Datum, Version und Konfiguration des Produkts, sowie Referenzen auf zugehörige Unterlagen.
- Software und Hardware, die freigegeben werden, müssen in einer Baseline enthalten sein, die unter Konfigurationskontrolle stehen muss.
- Zum Zeitpunkt der Produktfreigabe bekannte Sicherheitsbedenken oder Abweichungen müssen in einem institutionalisierten Prozess dokumentiert sein.

Die Freigabe auf Fahrzeugebene erfolgt durch den Fahrzeughersteller. Dafür stützt er sich in der Praxis auf die Freigaben seiner Lieferanten. Bestandteil dieser Freigaben ist unter anderem auch eine Verbauempfehlung für den OEM (Original Equipment Manufacturer). Nun kommen Fahrzeuge nicht erst nach SOP (Start of Production) erstmals auf die Straße. Während der Serienentwicklung werden mehrere Versionen von Vorserienfahrzeugen gebaut und erprobt. Für diese Fahrzeuge wird vom Lieferanten eine vorläufige Produktfreigabe verlangt. Diese unterliegt bestimmten Einschränkungen, zum Beispiel einem Geschwindigkeitslimit, nur für Testfahrer oder mit eingeschränktem Temperaturbereich. Üblich ist auch, dass ein Not-Aus-Knopf installiert sein muss. ISO 26262 schweigt sich über eingeschränkte Freigaben aus.

Eingeschränkt fahrtauglich

Die Norm führt nicht aus, wie komplette Fahrzeuge zum Straßenverkehr zugelassen werden. Dies ist nicht verwunderlich, handelt es sich doch einerseits um eine weltweit anwendbare Norm, und andererseits sind Zulassungsverfahren weitgehend national geregelt – und zwar nicht einheitlich. Außerdem spielen bei der Zulassung neben der Sicherheit eine Reihe von anderen Aspekten eine Rolle, wie zum Beispiel die Einhaltung von Abgasgrenzwerten.

Die Zulassung von Fahrzeugen zum Straßenverkehr, auch Straßenzulassung genannt, ist überall auf der Welt amtlich geregelt und erfolgt nach einem bestimmten Verfahren, das auch als Homologation bezeichnet wird. Dabei wird auf der Basis von Zulassungsvorschriften (nicht von Normen) überprüft, ob eine Vielzahl von Fahrzeugmerkmalen mit den Vorschriften übereinstimmen. Die ECE-Homologation ist eine überstaatliche Regelung und vermeidet durch gegenseitige Anerkennung die erneute Homologation in jedem einzelnen Land. Die gravierendste Ausnahme sind die USA, die ein inkompatibles System für die Fahrzeug- und Teilezulassung, die Federal Motor Vehicle Safety Standards (FMVSS), haben. Die Homologation erfolgt für Serienfahrzeuge als Typprüfung, also für eine ganze Klasse von Fahrzeugen oder auch nur einzelne Bauteile. Über die Prüfung wird ein Zertifikat ausgestellt, die Typgenehmigung. Die europäische Typgenehmigung hat für die gesamte EU Gültigkeit. Eine solche Typgenehmigung ist Voraussetzung für die Erteilung der Straßenzulassung durch die zuständige Straßenverkehrsbehörde, in Deutschland das Kraftfahrt-Bundesamt. Der Fahrzeughersteller beantragt die Typgenehmigung und muss dazu eine Vielzahl von Unterlagen zur Verfügung stellen, unter anderem auch die zum Sicherheitsnachweis. (jd)

Quelle

Der Artikel ist ein überarbeiteter Auszug aus diesem Buch:

Peter Löw, Roland Pabst, Erwin Petry

Funktionale Sicherheit in der Praxis; Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten

dpunkt.verlag 2010

Webseite des Buches: www.dpunkt.de/buecher/2929.html