7 Bestätigung der funktionalen Sicherheit

Die ISO 26262 sieht drei Maßnahmen vor, die zur Bestätigung der funktionalen Sicherheit für ein Produkt notwendig sind (aus ISO, Teil 2-6.2, General):

- Prüfung (und Bewertung) der Implementierung der notwendigen Prozessaktivitäten zur Erlangung der Funktionssicherheit (Functional Safety Audit)
- Prüfung der relevanten Arbeitsergebnisse bezüglich Einhaltung der ISO-26262- Anforderungen (Confirmation Reviews)
- Beurteilung, ob die Funktionssicherheit für das Fahrzeugsystem erreicht wird (Functional Safety Asessment).

Die ISO 26262 benutzt die englischen Worte „evaluate“ im Zusammenhang mit Functional Safety Audit und Functional Safety Assessment und „check“ für die Confirmation Reviews. Den Bewertungscharakter bei den Functional Safety Audits würde man darin sehen, ob die Sicherheitsaktivitäten wie geplant durchgeführt wurden.

Die Norm verlangt nur eine Beurteilung, ob die Funktionssicherheit für das gesamte Fahrzeugsystem gemäß den gegebenen Sicherheitszielen erreicht wurde. Eine Teilbeurteilung von Elementen (Systeme, die kein Fahrzeugsystem bilden, Komponenten oder Bauelemente, z. B. Mikrokontroller) kann auch in ihren Systemgrenzen bezüglich der funktionalen Sicherheit erfolgen. Man wird hier jedoch nicht die Angemessenheit oder vollständige Erfüllung der Sicherheitsziele für ein konkretes Fahrzeug beurteilen können. Die ISO 26262 empfiehlt eine entwicklungsbegleitende Bewertung der funktionalen Sicherheit.

Nach der Aufzählung der drei Bestätigungsmaßnahmen wird ergänzt, dass zusätzlich Reviews zur Verifizierung durchgeführt werden sollen. Diese Reviews, die in anderen Teilen der Norm gefordert werden, sollen verifizieren, dass die relevanten Arbeitsprodukte die Projektanforderungen erfüllen und die technischen Anforderungen die Anwendungsfälle und Fehlermodi hinreichend berücksichtigen.

Die ISO 26262 gibt folgende Tabelle für die Bestätigungsmaßnahmen vor und verweist auf den Annex D von Teil 2 bezüglich Reviews zur Verifikation der jeweiligen Teile der ISO 26262. Das Kapitel „General“ endet mit dem Hinweis, dass das Sicherheitsmanagement die Verantwortung für die Beschreibung und Überprüfung aller Sicherheitsaktivitäten beinhaltet.

In Teil 2 Kapitel 6.4.7 (Bestätigungsmaßnahmen: Arten (Typen), Unabhängigkeit und Kompetenz (Amtsbefugnis)) wird die Tabelle 1 mit folgender Anforderung eingeleitet:

6.4.7.1 Die Bestätigungsmaßnahmen spezifiziert in Teil 2, Tabelle 1 (Bild 7.1) sollen gemäß dem geforderten Grad der Unabhängigkeit, der Teil2, Tabelle 2 (Bild 7.2) und den Anforderungen 6.4.3.5 i), 6.4.8 und 6.4.9. durchgeführt werden. Darunter gibt es folgende Hinweise:

Hinweis 1: Die Bestätigungsreviews werden für die Arbeitsergebnisse durchgeführt, die in Tabelle 1 spezifiziert und gemäß Sicherheitsplan gefordert sind.

Hinweis 2: Ein Bestätigungsreview beinhaltet die Überprüfung der Korrektheit von formalen Anforderungen, Inhalt, und Vollständigkeit bezüglich der Anforderungen der ISO 26262.

Hinweis 3: Tabelle 1 beinhaltet die Bestätigungsmaßnahmen. Ein Überblick der Verifikationsreviews wird im Annex D gegeben.

Hinweis 4: Ein Bericht, der die Ergebnisse der Bestätigungsmaßnahmen wiedergibt, beinhaltet die Namen, die Revision der Arbeitsergebnisse oder der analysierten Prozessdokumente (siehe ISO 26262-8:2011, 10.4.5).

Hinweis 5: Ändert sich das Fahrzeugsystem nach den Reviews zur Bestätigung oder dem Assessment zur funktionalen Sicherheit, so sind diese zu wiederholen oder entsprechend den Änderungen zu ergänzen. (siehe ISO 26262-8:2011, 8.4.5.2).

Hinweis 6: Das Ziel der jeweiligen Bestätigungsmaßnahmen wird im Anhang C von Teil 2 der ISO 26262 vorgegeben.

Hinweis 7: Bestätigungsmaßnahmen wie die Reviews und Assessments zur funktionalen Sicherheit können zusammengeführt oder mit dem Assessment der funktionalen Sicherheit kombiniert werden, um die Handhabung von Varianten des Fahrzeugsystems zu unterstützen.

Bestätigungsmaßnahmen	Grad der Unabhängigkeit				Umfang
	Anwendbar bei ASIL				
	A	B	C	D	
Bestätigungsreview der Gefahren und Risikoanalyse des Fahrzeugsystems (siehe ISO 26262-3:, Kapitel 5, ISO 26262-3:, Kapitel 7 und wenn anwendbar, ISO 26262-8:, Kapitel 5) -Unabhängigkeit bezüglich Entwickler des Fahrzeugsystems, Projektmanagement und Autoren der Arbeitsergebnisse.	I3				Der Umfang dieses Reviews sollte die Korrektheit Bestimmung von - ASILs, und - QM Bewertungen Der identifizierten Gefahren, die sich aus dem Fahrzeugsystem ergeben können und das Review der Sicherheitsziele.
Bestätigungsreview des Sicherheitsplans (siehe 6.5.1) - Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und den Autoren der Arbeitsergebnisse.	-	I1	I2	I3	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Bestätigungsreview der Fahrzeugsystemintegration und Testplänen (siehe ISO 26262-4) -Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und den Autoren der Arbeitsergebnisse t	I0	I1	I2	I2	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Bestätigungsreview des Validierungsplans (siehe ISO 26262-4) -Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und den Autoren der Arbeitsergebnisse	I0	I1	I2	I2	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Bestätigungsreview der Sicherheitsanalysen (siehe ISO 26262-9:—, Kapitel 8) -Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und den Autoren der Arbeitsergebnisse	I1	I1	I2	I3	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Bestätigungsreview der Software-Tool-Qualifikationsbericht[a] (siehe ISO 26262-8:—, Kapitel 11) -Unabhängigkeit bezüglich der Personen, die die Software-Tool-Qualifikation durchführen	-	I0	I1	I1	Gilt für den höchsten ASIL der Anforderungen, die durch die Verwendung der Werkzeuge verletzt werden können
Bestätigungsreview der Argumentation zur Betriebsbewährtheit (Analyse, Daten und Sicherheitskredit), des Kandidaten. Siehe ISO 26262-8:—, Kapitel 14. -Unabhängigkeit bezüglich des Autors der Argumentation.	I0	I1	I2	I3	Gilt für die ASILs der Sicherheitsziele und Anforderungen, bezüglich Verhalten oder Funktionen des Kandidaten.
Bestätigungsreview zur Bestätigung der Vollständigkeit des Sicherheitsnachweises (siehe 6.5.3) - Unabhängigkeit bezüglich des Autors des Sicherheitsnachweises.	I0	I1	I2	I3	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Prozessaudit gemäß 6.4.8 - Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und dem Projektmanagement.	-	I0	I2	I3	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems
Assessment der Funktionalen Sicherheit gemäß 6.4.9 - Unabhängigkeit bezüglich der Entwickler des Fahrzeugsystems und dem Projektmanagement.	-	I0	I2	I3	Gilt für den höchsten ASIL der Sicherheitsziele des Fahrzeugsystems

Die Notationen I0, I1, I2 und I3 sind wie folgt definiert:

-: keine Empfehlung oder Anforderung für und weder für diese Bestätigungsmaßnahmen;

I0: die Bestätigungsmaßnahmen wird empfohlen, jedoch wenn die Bestätigungsmaßnahmen durchgeführt wird, dann sollte sie von einer anderen Person durchgeführt werden;

I1: Die Bestätigungsmaßnahmen sollen durch verschiedenen Personen durchgeführt werden;

I2: Die Bestätigungsmaßnahmen sollen von Personen durchgeführt werden von einem anderen Team, zum Beispiel sollten sie nicht an den selben Vorgesetzten berichten;

I3: Die Bestätigungsmaßnahmen soll durch eine Person durch eine unabhängigen Abteilung oder Organisation durchgeführt werden, zum Beispiel unabhängig von der Abteilungsverantwortung für die betrachteten Arbeitsergebnisse, bezüglich Management, Ressourcen und Freigabeverantwortung.

[a] Eine Software-Tool Entwicklung ist außerhalb des Lebenszyklus des Fahrzeugsystems, wobei die Qualifikation eine Maßnahme innerhalb des Lebenszyklus ist.

Bild 7.1 Tabelle 1: Bestätigungsaktivitäten und deren Grad der Unabhängigkeit (Quelle: angelehnt an ISO 26262, Teil2)

Die drei Bestätigungsmaßnahmen werden in Tabelle 2 (Bild 7.1) näher beschrieben.

Aspekt	Review zur Bestätigung	Audit zur Funktionalen Sicherheit	Assessment zur Funktionalen Sicherheit
Gegenstand der Bewertung	Arbeitsergebnis	Durchführung der Prozesse die zur Funktionalen Sicherheit gefordert sind.	Definiertes Fahrzeugsystem, gemäß ISO 26262-3:2011, Kapitel 5
Ergebnis	Reviewbericht (a)	Auditierungsbericht(a) gemäß ISO, Teil 2, 6.4.8	Assessmentbericht ISO, Teil 2, 6.4.9
Verantwortung der Person, die die Maßnahme durchführt	Bewerten der Konformität der Arbeitsergebnisse zu den relevanten Anforderungen der ISO 26262	Bewertung der durchgeführten geforderten Prozesse	Bewerten der erreichten Funktionssicherheit. Erstellen einer Empfehlung zur Akzeptanz, einer bedingten Akzeptanz oder eine Zurückweisung gemäß ISO, Teil 2-6.4.9.6
Zeitpunkt während der Sicherheitslebenszyklus	Nach der Fertigstellung der relevanten Sicherheitsaktivitäten.. Fertigstellung vor der Serienfreigabe.	Während Durchführung der geforderten Prozesse.	Fortschreitend während der Entwicklung oder in einem Block. Fertigstellung vor der Serienfreigabe.
Umfang und Detailtiefe	Gemäß des Sicherheitsplans	Durchführung der Prozesse gemäß den definierten Aktivitäten , wie referenziert oder spezifiziert im Sicherheitsplan.	Die Arbeitsergebnisse gemäß des Sicherheitsplans, den geforderten durchgeführten Prozessen und den Reviews der durchgeführten Sicherheitsmaßnahmen, die während der Entwicklung des Fahrzeugsystems bewertet werden können.
(a) Diese Berichte können im Assessmentbericht der Funktionalen Sicherheit eingebracht werden.			

Bild 7.2 Tabelle 2: Bestätigungsmaßnahmen und deren Charakterisierung (Quelle: angelehnt an ISO 26262, Teil 2)

Diesen Überblick liefert die ISO 26262. In einer Fußnote weist die ISO darauf hin, dass der Review- und Auditbericht in den Assessmentbericht eingebunden werden können.

Allgemein wird man nie beschreiben können, welche Sicherheitsaktivitäten für welche Risiken geeignet sind, auf jeden Fall war nicht Ziel der ISO 26262 konkrete Sicherheitsmaßnahmen für bestimmte Fehlerszenarien normativ vorzugeben. Daher wird man jedoch auch nicht allgemein sagen können, welche Bestätigungsmaßnahmen für welche Sicherheitsaktivität notwendig oder geeignet sind. Die Bestätigungsmaßnahmen müssen auf Basis des Sicherheitskonzeptes geplant werden.

In dem weiteren Kapitel werden Beispiele genannt, wie man eine sinnvolle Planung der Bestätigungsmaßnahmen vorsehen kann.

7.1 Reviews zur Bestätigung der Normerfüllung

„Confirmation Review“ wird nur in den Tabellen von Teil 2 betrachtet. Es gibt außer den Tabellen keine Anforderungen zu dieser Bestätigungsmaßnahme. Aus den Tabellen geht hervor, dass die Kernaufgabe die Konsistenz und Normerfüllung zur ISO 26262 gewährleisten soll sowie dass es um die Normerfüllung der Arbeitsergebnisse geht. Jedoch werden auch die meisten Ergebnisse einer Verifikation gemäß Teil 8 unterzogen, die die Konsistenz, Korrektheit und Vollständigkeit der wesentlichen Arbeitsergebnisse zeigen soll. Wesentlich wäre jedoch eine Konsistenzprüfung aller Arbeitsergebnisse, wie es später für den Sicherheitsnachweis (Safety Case) gefordert wäre. Die Tabellen rufen die Bestätigungsreviews nach den wichtigen Arbeitsergebnissen auf:

- Gefahren- & Risikoanalyse
- Projekt-Sicherheitsplan
- Fahrzeugsystemintegration und Testpläne
- Validierungsplan
- Sicherheitsanalysen
- Tool-Qualifizierung
- Argumentation zur Betriebsbewährtheit (Proven-in-Use, PIU)
- Vollständigkeit des Sicherheitsnachweises

Warum die Definition des Fahrzeugsystems, das funktionale Sicherheitskonzept, die Komponentenintegrationen und deren Tests, die Sicherheitsvalidierung und die Qualifikationen von Hard- und Softwarekomponenten nicht einem Bestätigungsreview unterzogen werden sollen, ist nicht nachvollziehbar. Einige dieser Arbeitsergebnisse müssen jedoch verifiziert werden.

Da die Bestätigungsreviews zwischen den Verifikationen und der Beurteilung der funktionalen Sicherheit platziert sind, wäre es empfehlenswert, diese Aktivitäten so gut wie möglich zu kombinieren. Da man bei den Verifikationen die notwendige Unabhängigkeit schon durch eine andere Person erreichen kann, sollten alle Inhalte, die spezifisches Fachpersonal verlangen, über Verifikationen eingeplant werden. Über die Bestätigungsreviews würde man dann mangelnde Unabhängigkeit gegenüber der Norm ergänzend prüfen. Wird durch die sinnvolle Kombination von Bestätigungsreviews und Verifikationen eine fachlich hinreichende Prüfung auf Konsistenz, Vollständigkeit, Nachvollziehbarkeit und Korrektheit festgestellt, würde man durch eine gestufte Vorgehensweise wesentlichen Input für die Sicherheitsbeurteilung liefern.

Geht man mit den Bestätigungsreviews bis zur Fertigstellung des Sicherheitsnachweises, wäre das finale Assessment zur funktionalen Sicherheit eine entsprechende ergänzende Prüfung. Diese ergänzt den Sicherheitsnachweis, die Sicherheitsvalidierung und die Feststellung der Angemessenheit der Sicherheitsziele und deren Erreichen zur Bestätigung der funktionalen Sicherheit für das Fahrzeugsystem.

7.2 Prozessanalyse zur funktionalen Sicherheit

Die Beziehung von CMMi Appraisal und Assessment zu Automotive SPICE werden immer in diesem Zusammenhang erwähnt. Wobei es hier im Rahmen der ISO 26262 nicht um die Ermittlung von Prozessverbesserungspotential geht. Die Angemessenheit der Sicherheitsaktivitäten zur Umsetzung derselben wird gemäß Teil 2, Tabelle 2 (Bild 7.2) als Bestätigungsreview gesehen. Ob die Sicherheitsaktivitäten angemessen zur Sicherheitszielerreichung sind, wird im Assessment zur funktionalen Sicherheit bewertet. Das heißt auch, um den Sicherheitslebenszyklus gemäß dem vereinbarten Sicherheitskonzept zuzuschneiden (tailoring) braucht es keinen SPICE-Assessor, sondern mehr einen Sicherheitsspezialisten. Das heißt nicht, dass man nicht auch über den Prozess gewisse Sicherheitsaspekte argumentieren kann, sollte oder darf. Dies ist besonders beim Anpassen der Aktivitäten wegen bestimmter Werkzeuge oft der Fall oder als verschlankter Prozess beim Applizieren oder der Entwicklung von Varianten eine sinnvolle Vorgehensweise. Dazu muss ein solcher Sicherheitsprozess (auch als Sicherheitshandbuch) jedoch in der Konzeptphase auch entsprechend geplant werden. Zur Planung eines solchen Prozesses ist wiederum ein Sicherheitsspezialist notwendig.

Der Sicherheitsprozess muss sehr eng an die Aufgabenstellung, die Sicherheitsziele und die Sicherheitskonzepte angepasst werden, da man ansonsten aus den unterschiedlichen Aktivitäten nicht die notwendigen Arbeitsergebnisse für den Sicherheitsnachweis bekommt. In einem Projektsicherheitsplan werden nicht nur die Ziele der Aktivitäten beschrieben, sondern auch die Ziele für die einzelnen Methoden. Somit kann zum Beispiel eine Fehlerbaumanalyse zur Anforderungsanalyse, zur Identifizierung der Cutsets, zur Definition der Sicherheitsarchitektur oder zur Identifizierung von Fehlern gemeinsamer Ursache dienen. Selbst bei demselben Produkt würde der Fehlerbaum, je nach Zielsetzung und welche Anforderungen der ISO 26262 man zu erfüllen beabsichtigt, sehr unterschiedlich aussehen. Diese Art von Prozessanalyse basiert auf vielen einzelnen Aktivitäten, die aus der ISO/

IEC12207 auch in SPICE oder CMMi abgewandelt wurden. Aber die Strategie oder die Zielsetzung verfolgt das bestimmte Ziel, den Sicherheitsnachweis bezogen auf korrekte Sicherheitsziele zu führen.

Verifikation der Sicherheitsaktivitäten

Die ISO 26262 stellt wenige Anforderungen an die Verkettung der Sicherheitsaktivitäten (Prozesse). Auch sind die Bestätigungsmaßnahmen in der Norm sehr unpräzise beschrieben worden, sodass die Verifikation der Sicherheitsaktivitäten, die sich durch die Verschachtelung der Arbeitsergebnisse zwar ergeben kann, nie beschrieben wurde. Nur bei der Tool-Sicherheitsanalyse findet man einen Hinweis, dass der Prozess, der der ISO 26262 zugrunde liegt, in sich sicher sein sollte. Da die Norm diesen Prozess nie beschrieben hat, kann man bei der Projektplanung leider diese Ketten zerstören.

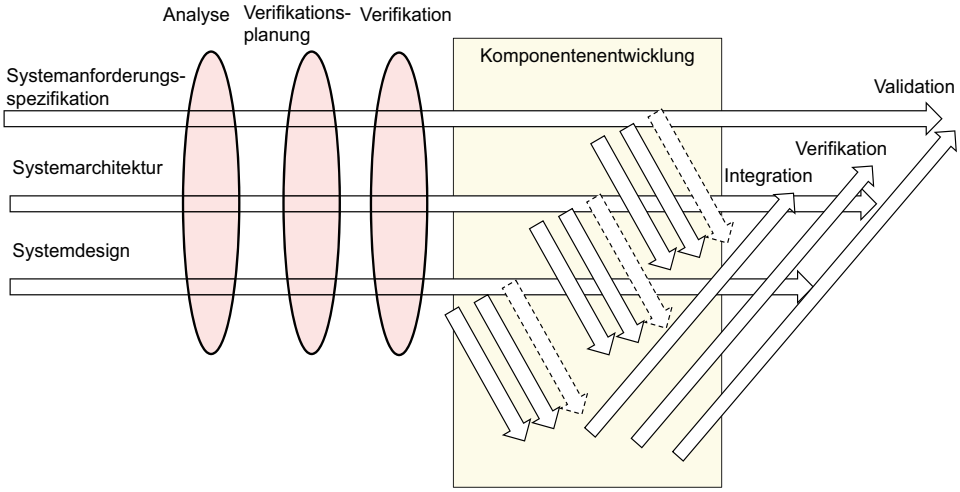

Bild 7.3 Prozessverifikation in Anlehnung an ISO 26262

Diese Muster für die Prozessstruktur der ISO 26262 ziehen sich weitgehend durch die gesamten Anforderungen der Norm. Das Bild 7.2 könnte man sogar noch um den Problemlösungs- und Änderungsprozess, das Konfigurations- und Dokumentationsmanagement sowie den Variantenmanagementprozess erweitern. Grundsätzlich wird die Verifikation an allen horizontalen Schnittstellen aufgerufen. Oben ist das Beispiel für die System-Komponentenschnittstelle dargestellt. Aber auch zwischen funktionalem Sicherheitskonzept und technischem Sicherheitskonzept soll genauso verifiziert werden wie an den horizontalen Architekturschnittstellen in den Komponenten. Grundsätzlich sollte jeder Input und Output einer Sicherheitsaktivität

verifiziert werden. Bei mehreren horizontalen Systemebenen wird die Verifikation nach jeder Schnittstelle aufgerufen. Der Vorteil und damit die Sicherheit entstehen dadurch, dass die Arbeitsergebnisse nach der Verifikation wieder Input für die nächste Phase sind. Das heißt, wenn man zum Beispiel die Systemarchitektur inklusive der allokierten Anforderungen verifiziert und in einer weiteren Verifikation später das Systemdesign auf Basis der vorherigen Anforderungen und Architekturen verifiziert wird, entsteht eine Schleife. Das heißt, man prüft den Input von allen Aktivitäten gegen den entstandenen Output der Aktivitäten. Die Verifikation läuft aber prozesstechnisch parallel mit, somit werden Anforderungen, Architektur und Design kontinuierlich überprüft, und zwar gegen den Output aus Anforderungen, Architektur und Design der vorherigen Phase. Somit würde jeder Prozessfehler bei der Verifikation durch den Vergleich des vorliegenden Outputs gegen den jeweiligen Input aufgedeckt werden müssen. Eine Grundanforderung nicht nur für Sicherheitsanforderungen heißt, dass der Output auf Basis des definierten Inputs reproduzierbar generiert werden muss. Da man bei jeder Verifikation auch noch die Konsistenz, Vollständigkeit und Korrektheit feststellen muss, wird man auch durch diese Prüfung Prozessfehler bei Anforderungs-, Architektur- oder Designentwicklung aufdecken können. Hat man diese Prozessfehler bei der Verifikationsplanung nicht berücksichtigt, dann ist die Aussage, dass der Prozess der ISO 26262 in sich sicher ist, nicht haltbar. Ursprünglich wurden diese Aspekte mal in den Reviews zur funktionalen Sicherheit (Funktional Safety Reviews) beschrieben. Bei der Umbenennung in die Bestätigungsreviews (Confirmation Reviews) in der späteren endgültigen Form ging leider viel von diesen Aspekten verloren. Da systematische Fehler, die durch Prozessfehler, Toolfehler oder auch menschliche Irrtümer verursacht werden, zu Inkonsistenzen führen können, sollten diese bei gut geplanten Verifikationen entdeckbar sein. Da die Idee der Entwicklungsprozesse aus den Produktionsprozessen abgeleitet wurde, findet man dort auch gute Beispiele für die Prozessverifikation. In der Produktionstechnik nennt man eine solche Prozessverifikation ein Verriegelungskonzept. Hier weist man nach, dass selbst bei inkorrektem Input der Produktionsprozess in der Lage ist, diese Fehler durch die Produktionsüberwachung aufzudecken. Auch hier wird das Produkt durch die Verifikation nicht verändert. Die Veränderung entsteht z. B. durch eine Nachbehandlung oder es werden fehlerhafte Teile aussortiert. Formal kann man sagen, dass die Verifikationen und die Analysen (als Spezialform der Verifikation) die wesentlichen Initiatoren des Änderungsprozesses bilden. Das nachbehandelte Teil muss jedoch wieder an der Verifikationsstelle vorbei, bevor es weiterbearbeitet werden darf. In der Produktionstechnik gilt die Maxime, je früher man eine Inkonsistenz entdeckt, umso kostengünstiger ist die Nachbehandlung. Auch diese Maßnahme kann man sehr gut auf die Entwicklungsprozesse übertragen. In der ISO 26262 gibt es ein Kapitel in Teil 8, welches sich mit der Tool-Qualifikation beschäftigt. Da es

derzeit noch wenige Tools gibt, die danach entsprechend qualifiziert sind oder, wenn sie qualifiziert sind, so angewendet werden, sollten die Verifikationen entsprechend geplant werden. Das heißt, wenn die Aktivitäten, die durch Tools gestützt werden, sicherheitsrelevante Produkteinflüsse hervorheben können, dann sollten die Verifikationen zu Inkonsistenzen führen. Rein von der Methodik sind sich Prozess- und System-FMEAs sehr ähnlich. Sprich, interpretiert man die System-FMEA so, dass sich systematische Fehler auf die Funktionen des Produkts auswirken können, so sind gegen deren Ursachen Maßnahmen zu ergreifen. Bei einer möglichen Fehlfunktion in der Prozess-FMEA führt man eine Überprüfung an der Produktionslinie ein, bei der System-FMEA wäre es ein Sicherheitsmechanismus. Ob man bei jedem möglichen systematischen Fehler, der sich auf ein Fehlverhalten des Produktes oder auf wichtige Eigenschaften des Produktes auswirken kann, mit Sicherheitsmechanismen kompensieren muss, geben die FMEA-Methoden oder die ISO 26262 weitgehend in den weiteren Anforderungen vor. Die ISO 26262 hat an zwei Stellen solche Verifikationen nicht erwähnt. Die erste Verifikation, die dringend empfohlen werden sollte, ist die Prüfung der Zielfunktion als beabsichtigte Funktion, die als Grundlage für das Fahrzeugsystem gilt. Diese Prüfung gibt Hinweise, ob die Funktion, auch wenn sie korrekt funktioniert, nicht schon zu Gefährdungen führt. Man spricht hier von der Gebrauchssicherheit. Weiter sollte die Definition des Fahrzeugsystems verifiziert werden. Ist diese inkorrekt, muss man auch mit unentdeckten Inkonsistenzen in der Gefahren- und Risikoanalyse rechnen.

Wichtig ist, dass die Planung der Analysen und Verifikationen diesen Umstand berücksichtigt und entsprechende Prozessverriegelungen auch wirksam eingeplant werden. Besonders wird es deutlich bei der Planung von diversitären Funktionen zum Beispiel für eine ASIL-Dekomposition. Lässt man den einen Algorithmus in Australien und den anderen Algorithmus in Skandinavien entwickeln, so ist dies noch lange kein Indiz dafür, dass man nicht die gleichen systematischen Fehler produziert. Plant man jedoch als Prozessvorgabe eindeutig unterschiedliche Entwicklungsziele ein, die aber das gleiche Sicherheitsziel abdecken, so kann man dann durch die sicherheitstechnische Inkonsistenz die systematischen Fehler entdecken. Hierzu gibt es das Beispiel, dass man den einen Algorithmus auf realen Zahlen und den anderen auf ganzen Zahlen rechnen lässt oder die eine Funktion durch Multiplikation integriert und die andere Funktion wie in einer Laplace-Transformation addiert. Es gibt auch die Möglichkeit, in der Produktentwicklung asymmetrische Konzeptionen zu den Testkonzepten einzuplanen, die dann zu den gewünschten Inkonsistenzen führen. Durch Fehlerinjektionen oder Grenzmustertests über mehrere Serien kann man, wie bei Produktionssystemen die Prozessfähigkeit, auch bei Produkten die Prozessfehlertoleranz prüfen.

7.3 Bewertung / Assessment der funktionalen Sicherheit

Das Assessment der funktionalen Sicherheit wird im Teil 2 unter den Bestätigungsmaßnahmen und im Teil 4 der ISO 26262 zum Abschluss der Systementwicklung nach der Sicherheitsvalidierung und vor der Freigabe für die Serienproduktion des Produktes beschrieben. Der Bezug zum Sicherheitsnachweis ergibt sich in erster Linie auch aus den Beschreibungen im Teil 2. Die Anforderungen, wie das Assessment zur funktionalen Sicherheit in den Entwicklungsablauf eingeordnet wird, stehen in Teil 4 der ISO 26262.

In Teil 4, Kapitel 10 der ISO 26262 werden folgende Ziele und Anforderungen an das Assessment zur funktionalen Sicherheit gestellt:

Ziel der Anforderungen in diesem Kapitel ist es, dass die Bewertung der funktionalen Sicherheit für das betrachtete Fahrzeugsystem erreicht werden kann.

Im Absatz „General, Allgemein" wird beschrieben, dass die Organisation, die für die Funktionssicherheit (zum Beispiel Fahrzeughersteller oder Zulieferer, wenn Letzterer verantwortlich für die Funktionssicherheit ist) verantwortlich ist, das Assessment der funktionalen Sicherheit zu initiieren.

Als Inputs werden folgende Arbeitsprodukte gefordert:

- Sicherheitsnachweis gemäß ISO 26262-2:2011, 6.5.3;
- Sicherheitsplan (detailliert) gemäß 5.5.2, ISO 26262-5:2011, 5.5.2 und ISO 26262-6:2011, 5.5.2;
- Bericht der Bestätigungsmaßnahmen gemäß ISO 26262-2:2011, 6.5.5;
- Auditierungsbericht, wenn verfügbar gemäß ISO 26262-2:2011, 6.5.4 und
- Plan zum Assessment der funktionalen Sicherheit (detailliert) gemäß 5.5.5 (im Teil 4 dieser Norm).

Die Norm fordert keine weiteren unterstützenden Dokumente.

Überraschenderweise fordert die Norm nicht das Produkt- oder das Fahrzeugsystem als einen der Inputs für die Aktivität, was nicht darauf schließen lässt, dass das Assessment der funktionalen Sicherheit rein auf eine Dokumentenprüfung zu reduzieren sein könnte. Dem widersprechen einige weiterführende Anforderungen, die sich mit den Verifikations- und Validationsaktivitäten und deren Anforderungen ergeben. Auch der in Kapitel 5.5.5 geforderte Assessmentplan, der sich aus einer einzigen Anforderung ergibt, etwa dass das Assessment der funktionalen Sicherheit zu Beginn der Systementwicklung geplant werden muss, weist darauf hin, dass die gesamte

Produktentwicklung im Rahmen des Assesssments zur funktionalen Sicherheit bewertet werden muss. Weiter ist der Sicherheitsnachweis ein wesentlicher Input für das Assessment, womit auch die Sicherheitsvalidierung bereits einen wesentlichen Input für das Assessment darstellt.

Folgende Anforderungen und Empfehlungen werden in Kapitel 10 erhoben:

Für Sicherheitsziele bis ASIL B empfohlen und für ASIL C und D gefordert, müssen für jeden Schritt des Sicherheitslebenszyklus gemäß ISO 26262-2:2011, Bild 2, die jeweiligen spezifischen Aspekte adressiert und entsprechend für das Assessment der funktionalen Sicherheit identifiziert werden.

Für Sicherheitsziele bis ASIL B empfohlen und für ASIL C und D gefordert, muss das Assessment der funktionalen Sicherheit gemäß ISO 26262-2:2011, 6.4.9 (Functional Safety Assessment) durchgeführt werden.

Als Arbeitsergebnis wird ein Bericht zur funktionalen Sicherheit gefordert.

Grundsätzlich sagen diese zwei Anforderungen aus, dass der gesamte Sicherheitslebenszyklus bei der Bewertung der funktionalen Sicherheit betrachtet werden muss. Das beinhaltet ausdrücklich damit auch, dass die korrekte Planung der Sicherheitsaktivitäten (Tailoring des Sicherheitslebenszyklus) in die Bewertung bereits einfließt. Weiter wird ein direktes Assessment der funktionalen Sicherheit nur für ASIL B empfohlen und für ASIL C und D gefordert. Dies ist der reine Standpunkt der Norm und betrifft auch nur die Anforderungen, die die Norm an die Umsetzung des Assessments zur funktionalen Sicherheit stellt. Da die Sicherheitsvalidierung und die notwendigen Verifizierungen auf jeden Fall für alle ASIL durchgeführt werden müssen, kann man jedem nur empfehlen, hier eine sinnvolle Lösung innerhalb der relevanten Organisationen zu finden. Eine Bewertung von sicherheitsrelevanten Produkten muss schon aus produkthaftungstechnischen Gründen durchgeführt werden. Welche Abstufung hier im Einzelfall möglich ist, kann nur die jeweilige Organisation für sich bestimmen.

7.4 Sicherheitsnachweis

Ziel des Sicherheitsnachweises ist es, die sichere Funktion des Fahrzeugsystems zu argumentieren. Das heißt, es geht um die sicherheitstechnisch korrekte Funktion und deren deterministisches Verhalten im Fehlerfall.

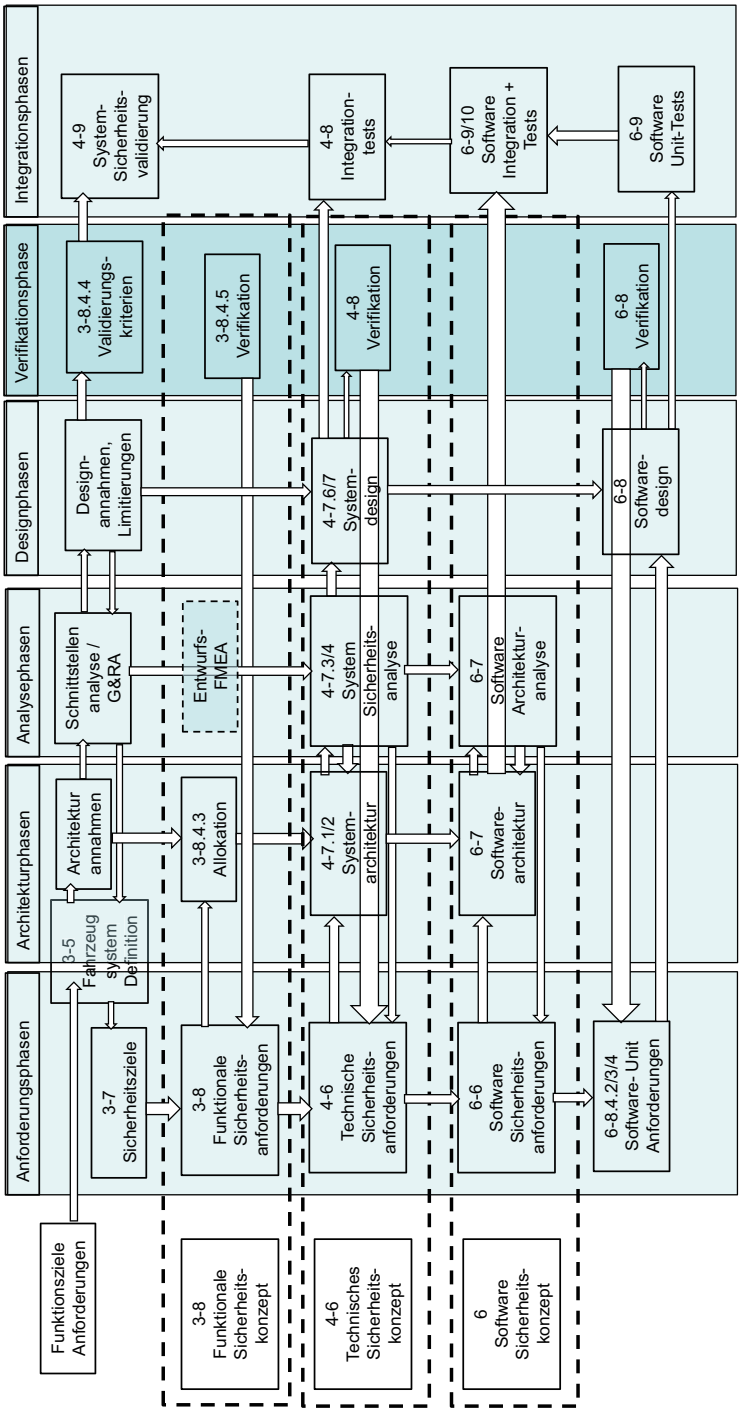

Bild 7.4 Sicherheitsnachweis als argumentierte Bestätigung der Funktionssicherheit basierend auf den validierten Sicherheitszielen und verifizierten Arbeitsergebnissen der geplanten Sicherheitsaktivitäten

In der ISO 26262 wird dies weitgehend als eine zusammenfassende Argumentation auf Basis der Arbeitsergebnisse der geplanten Sicherheitsaktivitäten gesehen.

Der Sicherheitsnachweis baut die Sicherheitsargumentation aus folgenden Aspekten auf:

- Sind der Betrachtungsumfang und die Arbeitsergebnisse der einzelnen Sicherheitsaktivitäten konsistent?
- Wurden die Fehler- und Sicherheitsanalyse hinreichend und korrekt durchgeführt?
- Wurden für die relevanten Fehler oder Fehlfunktionen sicherheitstechnisch adäquate Maßnahmen umgesetzt?
- Verifikation aller relevanten Arbeitsergebnisse
- Validierung der Sicherheitsziele (sind diese korrekt, hinreichend und erfüllt worden)
- Beurteilung aller Aktivitäten und Arbeitsergebnisse inklusive des Sicherheitsnachweises

Das Kapitel zum Sicherheitsnachweis wurde bewusst ans Ende des Buches gesetzt, weil die reproduzierbare Nachweisfähigkeit der funktionalen Sicherheit für ein Fahrzeugsystem das Ziel der ISO 26262 darstellt. Da die Sicherheitsvalidierung ein wesentlicher Input dazu ist und das Assessment der funktionalen Sicherheit die gesamten Bestandteile des Sicherheitsnachweises bewerten muss, sind dies Aspekte, die man nicht in einer eindeutigen Sequenz einbringen kann. Dazu sind die Sicherheitskonzepte der verschiedenen Fahrzeugsysteme doch zu unterschiedlich, um hierzu einen statischen Prozess beschreiben zu können. Wie bereits eingangs beschrieben war es auch nie Ziel der ISO 26262, eine Richtlinie für die sichere Fahrzeugentwicklung zu sein. Ziel war es immer, Hinweise in Form von Anforderungen zu geben, auf die man bei der sicheren Fahrzeugentwicklung achten sollte. Ob man nun glaubt, dass man, wenn man alle diese Anforderungen erfüllt, auch ein funktional sicheres System hat, muss jeder, der dieses Buch gelesen hat, für sich selbst bewerten.