6 Systemintegration

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Nachdem die einzelnen technischen Elemente realisiert sind, müssen sie Ebene für Ebene zusammengeführt werden. Da insbesondere die verschiedenen Aktivitäten bei der Realisierung des Produktes oder Komponenten nicht gesichert sein können, werden viele Sicherheitseigenschaften erst bei der Integration der Elemente geprüft und bestätigt werden können. Formal sollten hier wenig neue Erkenntnisse entstehen, da sämtliche Eigenschaften und auch die Leistungsdaten, die durch das Zusammenwirken der Elemente gefordert werden, bereits Gegenstand der Sicherheitsanalyse und der Verifikationen in den verschiedenen horizontalen Ebenen waren. Da ja auch schon in unterschiedlichen Musterphasen die Elemente miteinander getestet wurden, sind meist die Änderungen, die in den vorherigen Musterphasen nicht berücksichtigt waren, das größte Risiko. Für ein vollständiges softwarebasierendes Fahrzeugsystem gibt es laut ISO 26262 folgende drei Systemintegrationsebenen:

- Fahrzeugintegration
- Komponentenintegration (Systemintegration)
- Integration der Software in die Hardware

In der Elektronikebene wird man ebenfalls eine mehrstufige Integrationsstrategie wählen, wobei hier die Halbleiterelemente (Bustreiber, Mikrokontroller, Leistungstreiber, Multiplexer etc.) als technische Elemente im Wesentlichen diese Strategie vorgeben.

In der Software werden folgende Elemente (Gruppen von Elementen, Komponenten) bei der Integration betrachtet werden müssen:

- Low-Level-Treiber (MCAL, Schnittstelle zum Mikrokontroller)
- Betriebssystem
- Scheduler (Programmablauf, Steuerung, Überwachung, Datenflussüberwachung)
- Real-Time-Environment
- Anwendungssoftware
- Ebenen mit unterschiedlichem ASIL
- Degradationsebene

- Datenaufbereitung (Datenanpassung)
- Kommunikationsdatenaufbereitung
- Fehlermanager
- Diagnoseschnittstelle
- Fehlerbeherrschende Maßnahmen (Sicherheitsmechanismen)

Wie und in welcher Reihenfolge diese Elemente integriert werden sollen, hängt meist mehr von organisatorischen als von technischen Aspekten ab.

6.1 Verifikationen und Tests

Verifikationen dienen in erster Linie zur Überprüfung von Korrektheit, Konsistenz sowie Vollständigkeit und damit Nachvollziehbarkeit von Anforderungen und deren Abbildung auf Funktionen sowie auf logische und technische Elemente. Sind diese Kriterien hinreichend erfüllt, so kann man auch von einer hinreichenden sicherheitstechnischen Durchgängigkeit als Basis für die Sicherheitsvalidierung sprechen. Verifikationen finden nicht nur während der Integration (aufsteigender Ast im V-Modell) statt, sondern spielen auch während der Produktentwicklung (beziehungsweise während der Anforderungsentwicklung im absteigenden Ast des V-Modells) eine wesentliche Rolle. Wann immer ein Arbeitsergebnis als Grundlage für weitere Architekturentscheidungen dienen soll, ist eine vorherige Verifizierung empfohlen, ansonsten sind die folgenden Arbeitsergebnisse nur so sinnvoll wie die zugrundeliegenden Voraussetzungen.

Die Methode Test ist die am häufigsten benutzte Verifikationsmethode. Testmethoden haben unterschiedliche Ziele und werden daher unterschiedlich gruppiert. So gibt es die Tests, die die Entwicklung von Anforderungen unterstützen. Hier wird im Teil 4, Tabelle 2 (Eigenschaften eines modularen Systemdesign) unter Punkt 6 eine „Testbarkeit während der Entwicklung und dem Betrieb“ empfohlen und für ASIL C und D sogar gefordert. Weiter sagt die ISO 26262 dazu nichts. Sicherheitsfunktionen werden allgemein im Rahmen der Designverifizierung alle getestet. Damit wäre der Teil der Anforderung bereits erfüllt. Werden die notwendigen Tests im Rahmen einer Design-FMEA erarbeitet, so werden auf Grund der hohen Bewertung des möglichen Schadensausmaßes (S) bereits (bei QM) solche Tests gefordert. Während des Betriebs wird es die azyklischen Tests (Tests vor und nach dem Zündungslauf oder periodische Tests) geben und die Tests gegen Einzelfehler, die über die Diagnosedeckung definiert sind. Die ISO 26262 (Teil 4,

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Tabelle 3, Systemdesign Verifikation) empfiehlt oder fordert folgende Methoden zur Verifikation:

- Systemdesign Inspektionen (oder Reviews „walktrought“ für ASIL A genügend)
- Systemsimulationen oder alternativ System-Prototypen-oder Fahrzeugtests
- Systemdesignanalysen (hier verweist man auf die Sicherheitsanalysen)

Die ASIL Zuweisung besagt, dass Systemsimulationen oder Tests erst bei ASIL C und D gefordert sind und bei ASIL A und B nur empfohlen sind. In den APQP-Standards werden vollständige Systemdesigntests gefordert, daher wird sich die Empfehlung rein auf die Varianz auf welcher Ebene das Systemdesign getestet wird, beziehen. Weiter wird eine Systemdesignanalyse gefordert (es wird auf Teil 4 Tabelle 1 verwiesen), damit ist die induktive Sicherheitsanalyse (zum Beispiel die Design-FMEA) auf Systemebene (für alle ASIL) gemeint.

Analog zum System findet man in Teil 6 die Tabelle 6 „Methoden für die Verifikation von Software-Architektur-Design“ dort werden ähnliche Anforderungen erhoben wie in Teil 4, ergänzend gibt es die Steuer- und Datenflussanalysen. Die Tabelle 3 (Hardwaredesign-Verifikation) in Teil 5 stellt die analogen Anforderungen zur Elektronik-Hardware. An dem Beispiel sieht man, dass die Analogie, die in Bild (6.1) vertikal über alle Ebenen beschrieben ist, in die ISO 26262 hineininterpretiert werden kann.

Im nächsten Kapitel wird man sehen, dass die gesamte Verifikation geplant werden muss, so dass man unter diesen Anforderungen eine gewisse Dopplung in der Norm sehen kann. Es zeigt sich jedoch, dass ein gewisser Grundprozess sich wie ein roter Faden durch die Norm durchzieht, der in Bild (7.3) später nochmals aufgegriffen wird.

Zu den Integrationstests gibt es viele Tabellen, die die Testplanung im Rahmen der Integration in den entsprechenden horizontalen Ebenen unterstützen soll.

In Teil 4 sind es folgende Tabellen:

- Tabelle 4 – Methoden zur Testfallentwicklung für Integrationstests
- Tabelle 5 – Korrekte Implementierung von technischen Sicherheitsanforderungen auf Hardware-Software-Ebene
- Tabelle 6 – Korrekte funktionale Performance, Genauigkeit und zeitliches Verhalten von Sicherheitsmechanismen auf Hardware-Software-Ebene
- Tabelle 7 – Konsistente und korrekte Implementierung von internen und externen Schnittstellen auf Hardware-Software-Ebene
- Tabelle 8 – Effektivität der Diagnosedeckung von Sicherheitsmechanismen auf Hardware-Software-Ebene
- Tabelle 9 – Niveau der Robustheit auf Hardware-Software-Ebene

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Die Tabellen 10-14 bilden die Methoden zu den Anforderungen auf Systemebene und die Tabellen 15-19 auf Fahrzeugebene ab. Bezogen auf die jeweiligen horizontalen Ebenen sind die Anforderungen und Methoden mit Beispielen und Hinweisen hinterlegt und weichen im Detail von einander ab.

Für Teil 5 Hardware (Tabellen 10–12) und Teil 6 Software (Tabellen 9–16) gibt es ebenfalls vergleichbare Tabellen. Diese verweisen neben der Anpassung der jeweiligen horizontalen Ebene auch auf die Besonderheiten für die Software- und Hardwareentwicklung. Für die Software wird in den Tabellen auch eine Daten- und Steuerflussanalyse (für ASIL C und D gefordert) empfohlen. Diese Analysen sind nicht unbedingt Methoden bezüglich der üblichen Verifikationsziele (vollständig, korrekt und konsistent), sie sind eher vergleichbar mit der parallel zur Architekturentwicklung geforderten Sicherheitsanalyse.

Weitgehend kann man die Methoden in den Tabellen wie folgt gruppieren:

- Methoden zur Testfallentwicklung
- Methoden zu Tests der korrekten Implementierung der jeweiligen Anforderungen
- Methoden zu Tests der Performance, Toleranzen und zeitliches Verhalten
- Methoden zu Tests der internen und externen Schnittstellen
- Methoden zu Tests der Güte der Fehlerbeherrschung
- Methoden zu Robustheitstests
- Methoden zu Komponenten spezifischen Analysen und Tests.

Bei Tests wird oft unterschieden zwischen Komponenten- (Element-, Modul-,) oder Integrationstests. Die genannten Methoden unterscheiden sich namentlich nicht. Bei der Testfallanalyse wird man aber erkennen, dass die Ausprägung der Tests sich auf das Innere der Elemente in ihrer Umgebung bezieht, bei Integrationstests hingegen auf die Schnittstellen und deren gemeinsame Umgebung. Eine besondere Schnittstellenart sind dynamische oder virtuelle Schnittstellen, die nur in bestimmten Betriebssituationen oder Zuständen existieren. Hier ist die Abhängigkeit von der Umgebung sehr wichtig für diese Integrationstests, da die Testumgebung künstlich geschaffen werden muss. Ein typisches Beispiel dazu ist eine Laufzeitumgebung (RTE) in der Software. Formal gibt Teil 8, im Kapitel 9 (Verifikation) die allgemeinen Vorgaben entsprechend global wieder. Hier findet man dann auch die Hinweise, wie diese Methoden in die Verifikation einzubinden sind.

Eine systematische Integration kann nur erfolgen, wenn verifizierte Elemente bei der Integration verwendet werden. Da dies nicht immer der Fall sein kann, wird die Integration immer entsprechend iterativ erfolgen wie auch die Verifikationsergebnisse vorliegen. Daher ist die Rekursionsstrategie (vergleiche Informationsfluss in Bild 6.1) für die Tests nicht nur auf die Komponenten beziehungsweise Elementtests zu beziehen, sondern mindestens die Integration in die nächsthöhere Ebene muss eingeplant werden.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

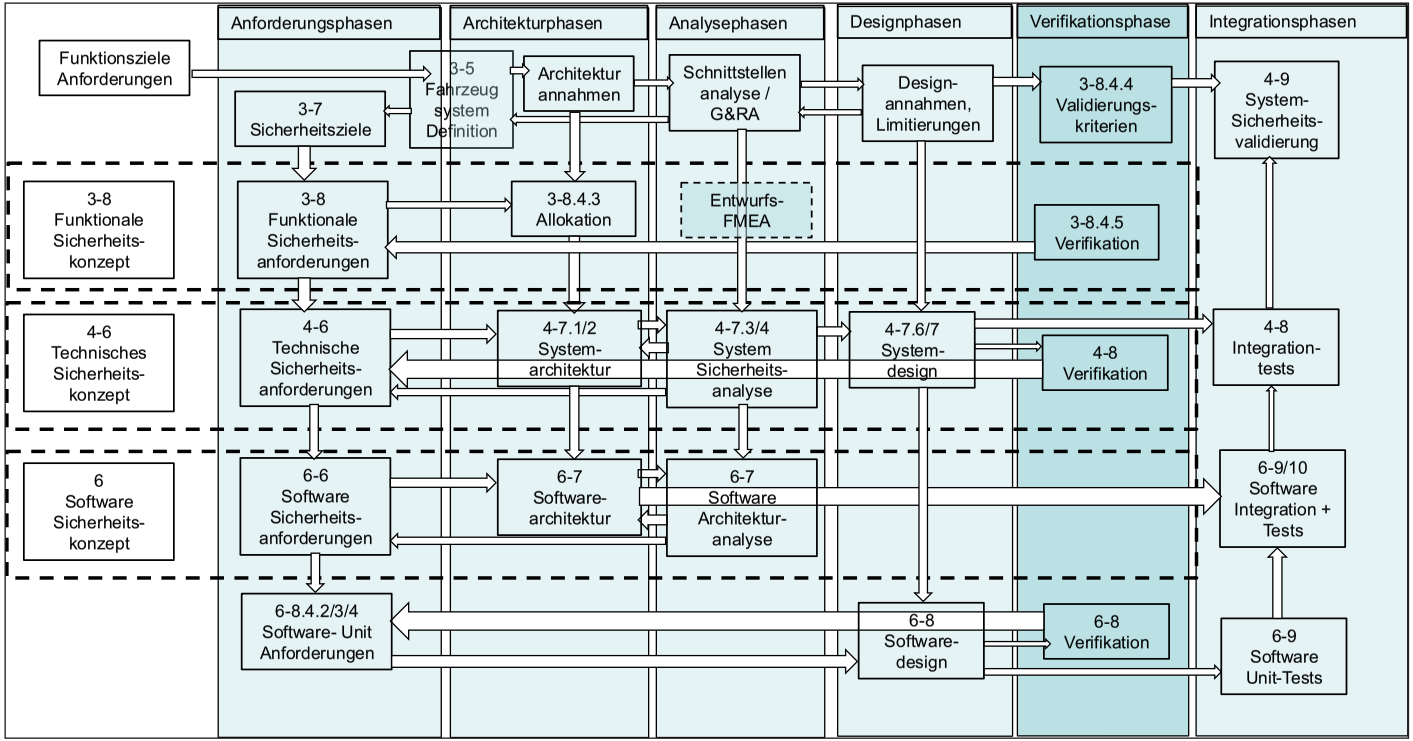

Bild 6.1 Verifikationen zwischen Anforderung und Integration

6.1.1 Grundlagen zu Verifikation und Test

Das Kapitel ISO 26262, Teil 8 Kapitel 9 beschreibt die allgemeinen Anforderungen an die Verifikation. Die Verifikation gemäß dem Kapitel hat die Aufgabe, die Erfüllung der relevanten Anforderungen zu überprüfen. In dem Kapitel „General“ wird beschrieben, in welcher Form in den verschiedenen Lebenszyklusphasen die Verifikation angewendet werden soll. Je nachdem, zu welcher Lebenszyklusphase die Verifikation aufgerufen wird, sind die relevanten Arbeitsergebnisse zugrunde zu legen.

Jede Verifikation muss geplant werden, bei der Planung sollte Folgendes betrachtet werden:

- der Inhalt der Arbeitsergebnisse, die verifiziert werden sollen
- die Methoden, die zur Verifikation genutzt werden sollen

Hinweis: Methoden zur Verifikation beinhalten Reviews, „Walk-through“, Inspektionen, Modellprüfungen, Simulationen, Demonstrationen und Tests. Typische Verifikationen nutzen Kombinationen aus diesen oder ergänzenden Methoden.

- die Akzeptanzkriterien für die Verifikation
- die Bedingungen der Umgebung, in der die Verifikation stattfinden soll

Hinweis: Dies kann eine Test oder eine Simulationsumgebung sein.

- Werkzeuge, die zur Verifikation genutzt werden
- Maßnahmen, die ergriffen werden sollen, wenn Abweichungen festgestellt werden, und
- eine Regressionsstrategie

Hinweis: Eine Regressionsstrategie legt fest, wie Verifikationen wiederholt werden, nachdem Modifikationen am Verifikationsobjekt durchgeführt wurden. Verifikationen können vollständig oder partiell wiederholt werden und auch Elemente oder Systeme beinhalten, die nicht Gegenstand der Verifikation sind.

Die Planung der Verifikation sollte Folgendes berücksichtigen:

- die Angemessenheit der Verifikationsmethode
- die Komplexität der Arbeitsergebnisse, die verifiziert werden
- vorherige Erfahrungen bezogen auf verwendete Materialien, die Einfluss auf die Verifikation haben könnten

Hinweis: Das beinhaltet die Servicehistorie oder den Grad der Betriebsbewährtheit, der erreicht wurde und die Reife der verwendeten Technologie oder Risiken, welche mit der Verwendung der Technologien entstehen könnten.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Spezifikation zur Verifikation

Die Spezifikation zur Verifikation soll die Methoden zur Verifikation zusammenstellen und diese für die Anwendung spezifizieren.

Sie sollte Folgendes beinhalten:

a) Review- oder Analyse-Checklisten,

b) Simulationsszenarien,

c) Testfälle, Testdaten und Testobjekte

Zum Testen soll für jeden Testfall Folgendes spezifiziert werden:

a) eine eindeutige Identifikation,

b) die Referenz zu der zugehörigen Version der Arbeitsergebnisse soll verifiziert werden,

c) die Voraussetzungen und Konfigurationen,

Hinweis: Ist eine vollständige Verifikation von möglichen Konfigurationen (zum Beispiel Systemvarianten) nicht umsetzbar, so muss eine glaubhafte Teilmenge ausgewählt werden (zum Beispiel Min-/Max-Funktionalitäten der Systemkonfigurationen).

d) Die Umgebungsbedingungen, in angemessener Art und Weise,

Hinweis: Umgebungsbedingungen bezüglich physikalischer Eigenschaften (zum Beispiel Temperatur), die die Testumgebung oder Simulationsumgebung repräsentieren.

e) Eingangsdaten, ihre zeitliche Abfolge und die Werte,

f) das erwartete Verhalten inklusive Ausgangsdaten, akzeptierte Datenbereiche und Ausgangswerte, zeitliches Verhalten und tolerierbares Verhalten.

Hinweis 1: Wird das erwartete Verhalten spezifiziert, so kann es notwendig sein, dass initiale Ausgangsverhalten zu spezifizieren, um Änderungen zu entdecken.

Hinweis 2: Um redundantes Spezifizieren und Ablage von Vorbedingungen, Konfigurationen und Umgebungsbedingungen von Testfällen zu vermeiden, wird die Verwendung von eindeutigen Referenzen empfohlen.

Zum Testen sollen alle Testfälle gemäß den Testmethoden gruppiert werden. Für jede Testmethode soll Folgendes spezifiziert werden:

a) die Testumgebung,

b) logische und zeitliche Abhängigkeiten, und

c) Ressourcen

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Durchführung und Bewertung der Verifikation

Die Verifikation soll wie geplant und spezifiziert durchgeführt werden.

Die Bewertung der Verifikationsergebnisse sollte folgende Informationen beinhalten:

a) eine eindeutige Identifikation der verifizierten Arbeitsergebnisse,

b) eine Referenz zum Verifikationsplan und der Verifikationsspezifikation,

c) die Konfiguration der Verifikationsumgebung und genutzten Verifikationswerkzeugen, sowie der verwendeten Kalibrationsdaten

d) den Erfüllungsgrad der Verifikationsergebnisse bezüglich der erwarteten Ergebnisse.,

e) ein eindeutiges Statement, ob die Verifikationsanforderungen erfüllt oder nicht erfüllt sind. Sind die Verifikationsanforderungen nicht erfüllt, sollte eine Argumentation aufgeführt werden und Vorschläge für mögliche Änderungen.

Hinweis: Die Verifikation sollte bezüglich Vollständigkeit und der Beendung der Verifikationsmaßnahme und dem erwarteten Ergebnis untersucht werden.

f) eine Begründung, warum bestimmte Verifikationsschritte nicht durchgeführt wurden.

Diese Auflistungen aus der ISO 262626 stellen viele Anforderungen an die Planung, Durchführung und Bewertung der Verifikation. Werden diese Anforderungen bereits bei der Anforderungsermittlung, Testfallspezifikation und so weiter berücksichtigt, so erleichtert dies die Verifikation selbst sehr.

6.1.2 Verifikation basierend auf Sicherheitsanalysen

Sicherheitsanalysen sind prinzipiell nur besondere Methoden zur Verifikation. Besonders die unterschiedlichen FMEA-Methoden unterstützen die Verifikation von Systemen.

Eine System-FMEA unterstützt in erster Linie die Verifikation der Anforderungen und deren Allokation an Funktionen sowie an logische oder technische Elemente. Eine Design-FMEA hinterfragt die korrekte Auslegung des Designs oder auch der Realisierung. Hier wird meist mit den Designentwürfen begonnen, in den späteren Iterationen wird dann die Realisierung immer mehr eingebunden. Daher unterstützt die Design-FMEA in erster Linie die Designverifikation und wird mit einem Designreview (dies weist auch stark auf die sogenannte Toyota-FMEA hin, DRBFM - **D**esign **R**eview **B**ased on **F**ailure **M**odes) abgeschlossen. In einer Prozess-FMEA wird allgemein der Produktionsprozess analysiert. Formal wäre es aber möglich,

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

jeden beliebigen Prozess mit dieser Methode zu analysieren, dazu gibt es weitere Hinweise in dem Kapitel 7.2 Prozessanalyse zur funktionalen Sicherheit. In jedem FMEA-Standard gibt es die zusätzliche Anforderung, dass das Ergebnis einer FMEA nochmals hinsichtlich des Ziels der Analyse geprüft werden muss. Ein Review der FMEA ist formal Bestandteil einer jeden FMEA-Methode.

Folgende Verifikationen können durch Sicherheitsanalysen unterstützt werden:

Vollständigkeit der relevanten Sicherheitsziele

In erster Linie werden Sicherheitsziele so formuliert: „Vermeide, dass eine mögliche Fehlfunktion des Fahrzeugsystems zu einer Gefährdung führt". Sämtliche Fehlfunktionen können in einer System-FMEA als Fehlerfolge der Systemfehler strukturiert werden, somit kann man sämtliche Fehlerfolgen gegen die definierten Fehlfunktionen, die zu einer Sicherheitszielverletzung führen, abprüfen, sodass man zu einer Vollständigkeitsaussage kommt.

Vollständigkeit der adressierten Elemente, die für eine sicherheitsrelevante Funktion notwendig sind

Diese Analyse basiert auf den Funktionsnetzen der VDA-FMEA. Hier würden jedoch automatisierte Tests in den Architekturtools wesentlich effektiver sein. Diese Prüfung kann in der horizontalen Abstraktionsebene stattfinden. So wie man eine System-FMEA auf Komponentenebene durchführen wird, kann die Verifikation nach der Methode auf Systemebenen oder auch in den Software- und Hardwarekomponentenebenen stattfinden. Selbst innerhalb von Halbleiterstrukturen ist diese Analyse zu empfehlen. Das Grundprinzip der Analyse ist die Identifizierung der Wirkkette, welche von Robert Lusser bereits vor über 80 Jahren beschrieben wurde. Weiter gibt es eine Methode „FAST, Functional Analysis System Technique", die diese Ableitung von Funktionen auf eine untere Elementstruktur und deren induktive Prüfung beschreibt.

Prüfung, ob eine Funktion in einer unteren horizontalen Ebene vollständig aus einer oberen horizontalen Ebene abgeleitet wurde (Funktionsdekomposition)

Hier bezieht man sich nicht wie in der Analyse zuvor auf die Elemente, die eine Funktion abbilden, sondern auf die Funktion selbst. In einer VDA-FMEA könnte man über die Funktionsnetze wieder prüfen, ob die Funktionen in den Komponenten (SW oder HW) vollständig auf der Systemebene abgebildet sind. Diese Analyse unterstützt auch die Analyse der abhängigen Fehler, da Abhängigkeiten in unteren Ebenen in Bezug zur Abhängigkeit in oberen Ebenen gebracht werden. Dies ist nicht nur für funktionale Abhängigkeiten analysierbar, auch physikalische Abhängigkeiten (zum Beispiel Temperatureinfluss, EMV) oder Energieabhängigkeiten können so analysiert

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

werden. Auch hier sind die Architekturtools mit entsprechenden Prüfalgorithmen wesentlich besser geeignet als eine VDA-FMEA. Auch diese Prüfung kann in Anlehnung an die Methode „SADT, Structured Analysis Design Technique“ zu einer systematischen Funktionszerlegung und deren Nachvollziehbarkeit genutzt werden.

Konsistenzprüfung der Schnittstellen (Produktdekomposition)

In der VDA-FMEA werden durch die Strukturnetze die Schnittstellen für die gesamte Produktstruktur beschrieben. Hier gibt es die Herausforderung, dass funktionale und technische Schnittstellen nicht immer deckungsgleich sind. Das heißt, man kann durch den Vergleich der funktionalen Struktur deren Abhängigkeit und deren Konsistenz bezogen auf die horizontalen Ebenen analysieren. Eine Dekomposition von funktionalen oder logischen Elementen führt zu anderen Schnittstellen als eine Dekomposition von technischen Elementen. Sind Schnittstellen oder Abhängigkeiten im System anders als auf der Komponentenebene, führt dies zu Inkonsistenzen. Auch hier sind Architekturtools und mögliche Prüfroutinen wesentlich effektiver als eine VDA-FMEA.

Vollständigkeit der betrachteten Fehlermöglichkeiten

Insbesondere bei der deduktiven Analyse ist es wichtig, eine gewisse Vollständigkeit der Fehleranalyse zu argumentieren. Klar ist jeder gefundene mögliche Fehler gut zur Verbesserung der nicht-funktionalen Eigenschaften eines Produktes, aber für eine Sicherheitsargumentation wird Vollständigkeit gefordert. Daher wird in der VDA-FMEA die Fehleranalyse erst als dritter Schritt nach der Produkt- und Funktionsdekomposition gesehen. Das heißt, für jede Funktion eines Strukturelementes müssen die möglichen Fehlfunktionen ermittelt werden. Für die Verifikation der sicherheitsrelevanten Anforderungen gilt es erstens zu prüfen, ob die möglichen Fehlfunktionen, die zu einem Fehlverhalten der Funktion führen können, vollständig betrachtet wurden. Dies kann man bei einer rein funktionalen Analyse dadurch sicherstellen, dass man sagt, ein Signal kann nicht ankommen oder falsch sein. Somit kommt man mit den beiden Fehlfunktionen „keine Information“ oder „falsche Information“ bereits zu einer Vollständigkeitsaussage. In den tiefergehenden Analysen kann man die Vollständigkeit der Fehlfunktionen dahin gehend prüfen, ob folgende Fehlfunktionen betrachtet wurden:

- keine Funktion
- unerwartete Funktion (übersprechen von anderen Systemen)
- systematisch verfälschte Funktion oder Informationen (zum Beispiel Signaldrift)
- sporadisch oder unerwartet falsche Funktion oder Informationen
- Modul oder Element wurde nicht ausgeführt, adressiert oder betrachtet

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

- Funktion oder Element verläuft nicht kontinuierlich oder wird nicht kontinuierlich berücksichtigt (kein unterbrechungsfreier Betrieb, Oszillationen)
- falsches Zeitverhalten

Diese Fragen bilden meist den Kontext für die deduktiven Methoden, wie HAZOP und Fehlerbaumanalyse. Im Wesentlichen bilden sie auch die Fehlfunktionen in den Tabellen des Teils 5, Anhang D der ISO 26262 ab, die die Grundlage für die Diagnosedeckung darstellen. Diese Betrachtungen sind meist kontextabhängig sowie abhängig von den Anforderungen, die an die Funktionen gestellt sind. Daher wird in dieser Tiefe nicht mehr nur die Architektur analysiert, sondern das Design und die Realisierung. Somit sind diese Analysen oft Bestandteil der Design-FMEAs und im Wesentlichen unterstützen diese Prüfungen die Anforderungsverifikation.

Vollständigkeit der betrachteten Einfachfehler

Dies ist die klassische Domäne der FMEA, hier werden alle möglichen Fehlfunktionen einer entsprechenden Ebene darauf geprüft, ob sie zu einem Sicherheitsziel propagieren können. Eine klassische System-FMEA hat unter diesem Aspekt in ihrem Betrachtungsumfang den Anspruch vollständig zu sein.

Vollständige Betrachtung von Doppelfehlern

Mehrfachfehler bilden immer hohe Permutationen bezogen auf ihre Einflussfaktoren, daher wird bei einfachen Systemen bereits eine Mehrfachfehleranalyse zur Herausforderung. Baut man aber Sicherheitsmechanismen in Form von Barrieren auf, die eine Fehlerpropagation verhindern sollen, so sind Durchbrüche durch Barrieren, die direkt unter dem Sicherheitsziel angeordnet sind, wie Einfachfehler zu betrachteten. Muss man Mehrfachfehlersicherheit wie bei ASIL-C- und ASIL-D-Systemen aufzeigen, wird man über eine einzelne Analyse nicht zum Ziel kommen. In der ISO 26262 wird die Möglichkeit eingeräumt, dass man Fehler eines Sicherheitsmechanismus als Doppelfehler ansehen kann, wenn der Fehler des Sicherheitsmechanismus selbst kein Sicherheitsziel verletzen kann. Das heißt, man untersucht die Fehler der Sicherheitsmechanismen zweimal, einmal bezüglich ihrer Verletzung des Sicherheitsziels selbst und dann bezüglich ihres Potentials, das zum Versagen des Sicherheitsmechanismus führen kann. Somit ist auch eine gewisse Vollständigkeit der Betrachtung der relevanten Doppelfehler argumentierbar.

Korrektheit des Sicherheitsziels selbst

Dies ist nur möglich bezüglich vorab definierter Gefahren, die als vollständig und korrekt angesehen werden. Es geht nunmehr in die Domäne der Ereignisbaumanalyse, es kann jedoch geprüft werden, welche Fehlfunktionen der Sicherheitsziele in welchen

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Situationen zu welchen Gefahren führen. Ein weiterer offener Punkt ist, wie man die Vollständigkeit der zu betrachtenden Fahrsituationen und deren Kombinatorik zu den Gefahren oder Fehlfunktionen argumentieren kann.

6.1.3 Testmethoden

Die Ziele des Teils 4, Kapitel 8 Integration und Test wurden bereits bei der Planung der Architektur diskutiert.

Die Integrations- und Testphasen bestehen aus drei Phasen und zwei vorrangigen Zielen: Die erste Phase ist die Integration der Hardware und Software von jedem Element, aus dem das Fahrzeugsystem besteht. Die zweite Phase ist die Integration der Elemente eines vollständigen Systems, welche das Fahrzeugsystem bilden. Die dritte Phase ist die Integration des Fahrzeugsystems mit anderen Systemen des Fahrzeugs und deren Integration in das Fahrzeug selbst.

Daraus entstanden drei horizontale Systemebenen, in denen Elemente hierarchisch bis zur Fahrzeugintegration integriert werden. An die Methode, wie diese Integration erfolgen soll, richten sich dann diese beiden Ziele:

Das erste Ziel des Integrationsprozesses ist die Erfüllung jeder Anforderung gemäß ihrer Spezifikation und ASIL-Klassifikation.

Das zweite Ziel ist die Verifikation, dass das Systemdesign die Sicherheitsanforderungen (siehe Kapitel 7 Systemdesign) korrekt für das gesamte Fahrzeugsystem abdeckt.

Die Norm gibt hier den Hinweis, dass alle Anforderungen umgesetzt sein müssen und die Verifikation final das Design des gesamten Fahrzeugsystems abdecken muss. Um die korrekte Integration zu zeigen, schreibt die ISO 26262 die Methode Test vor. Das heißt, eine reine Modellintegration ist nicht hinreichend, bestimmte Tests müssen die korrekte Implementierung des Systemdesigns gemäß den Anforderungen nachweisen.

Da es sich bei einem System gemäß ISO 26262 um ein hierarchisch gegliedertes System handeln muss, ergeben sich zwei grundsätzliche Arten von Tests:

- Elementtests
- Integrationstests

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

In vielen Standards geht man davon aus, dass bei Integrationstests vorab verifizierte Elemente mit eindeutig spezifizierten und verifizierten Schnittstellen den Testgegenstand ergeben. Hier wurde bisher nur die ISO 26262 für das System zitiert, im Prinzip gilt das hierarchische Design auch für die Software- und Hardwarekomponenten. Daher kann man die Methoden für Element- und Integrationstests weitgehend unabhängig von den horizontalen Ebenen, auf denen sie angewendet werden, beschreiben. Die ISO 26262 empfiehlt beziehungsweise fordert bereits bei der Anforderungsentwicklung, aber spätestens bei deren Verifikation, die Planung beziehungsweise die Testbarkeit der korrekten Implementierung durch die Realisierung der Anforderungen zu prüfen. Das heißt, wenn man eine Anforderung entwickelt, muss man bereits ein Konzept haben, wie man am realisierten Produkt die korrekte Umsetzung der Anforderungen nachweisen kann. Würde man die Testplanung zu einem späteren Zeitpunkt in der Entwicklung beginnen, so könnte man systematisch wohl eine Änderung der entwickelten Anforderungen hervorrufen. Solche Schlagworte, wie „Design2Test“, DoE (Design of Experiment), anforderungsbasierendes Testmanagement oder risikobasierendes Testen, beschreiben mögliche Testmethoden.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

6.1.4 Integration technischer Elemente

Die verschiedenen Stufen der Integration dienen zum Verifizieren der Schnittstellen der relevanten Elemente. Die Grundlage dazu bilden wieder die typischen Verifikationskriterien für die Schnittstellen. Es wird geprüft, ob die Schnittstellen vollständig, konsistent, korrekt und hinreichend für den Sicherheitsnachweis nachvollziehbar realisiert wurden.

Neben den Komponenten aus Software, Elektronikhardware und den Komponenten andere Technologie gibt es noch 3 weitere Gruppen von Elementen oder Komponenten, die in ein sicherheitsrelevantes Fahrzeugsystem integriert werden müssen, ohne dass sie nach dem Standard ISO 26262 entwickelt wurden. Die Herausforderung besteht darin, die Schnittstellen zur Integration und ihre Fehlerpropagation an diesen Schnittstellen hinreichend korrekt beschreiben können. Auch für Komponenten, die außerhalb des Kontexts der Norm oder des jeweiligen Fahrzeugsystems entwickelt worden sind besteht dieses Schnittstellenrisiko. Sämtliche Design- und Architekturannahmen müssen harmonisiert werden, damit die Fehlerpropagation dieser Komponenten zu den Sicherheitszielen bewertet werden kann. Ein prägnantes Beispiel für die Herausforderung ist ein Mikrokontroller, der vielleicht für ein System, welches energielos immer den sicheren Zustand erreicht nun für ein System eingesetzt wird wo Verfügbarkeit

auch eine Sicherheitsanforderung darstellt. In der ISO 26262 findet man folgende Klassen von Elementen, die unterschiedliche Anforderungen an die Integration solcher Elemente stellen.

Sicherheitselement entwickelt außerhalb des Scope des Fahrzeugsystems (SEooC, Safety Element out of Context)

Hierunter fallen fast alle Elemente und Komponenten, die in ein Fahrzeug integriert werden. Mikrokontroller, Software-Komponenten bis hin zu Bremssystemen werden nicht für ein bestimmtes Fahrzeug mit bestimmten Fahrdynamikkenndaten entwickelt, sondern historisch gemäß den Marktanforderungen. In anderen Branchen sind deswegen viele Schnittstellen auch elektrische Schnittstellen normiert. Das ist insbesondere bei elektrischen Schnittstellen in der Automobilindustrie gar nicht der Fall. Somit ist man gezwungen für diese SEooC Schnittstellen festzulegen. Dies mag für Mikrokontroller an den Pins für die elektrischen Signale noch lösbar sein, aber Diagnoseschnittstellen für fehlerbeherrschende Maßnahmen, die im SEooC oder außerhalb abgesichert werden, sind sehr schwierig. Daher gibt es in Teil 10 der ISO 26262 bereits Hinweise, wie man solche Elemente integrieren kann, aber normative Lösungen fehlen derzeit. Bei einem SEooC geht man jedoch davon aus, dass das Element bereits nach der ISO 26262 entwickelt wurde. Der Unterschied zu anderen Elementen besteht darin, dass die Anforderungen nicht aus einem konkreten Fahrzeugsystem heruntergebrochen werden, sondern auf Annahmen basieren. Bei der Integration muss man daher nachweisen, dass die Annahmen auch korrekt und gültig für das Ziel-Fahrzugsystem sind.

Qualifizierte Komponenten

Die ISO 26262 adressiert im Teil 8 jeweils separat die Qualifikation von Software- und von Hardwareelementen. Beide Elemente haben dieselben Herausforderungen, hier geht man davon aus, dass diese nicht nach der ISO 26262 entwickelt wurden. Dadurch dass die ISO 26262 immer noch recht neu ist, gibt es gar nicht so viele Komponenten, die nach dieser Norm entwickelt wurden. Daher hat man sich vor der Veröffentlichung natürlich an anderen Sicherheitsstandards orientiert. Ist eine Komponente nach einem anderen Sicherheitsstandard entwickelt worden, dann kann man davon ausgehen, dass es eine hinreichende Sicherheitsdokumentation gibt. Ob jedoch die Fehlerpropagation dieser Komponenten in einem Fahrzeugsystem, wie bei einem Flugzeug oder einem stationärem Kraftwerk ist und ob das zeitliche Verhalten im Verbund mit anderen Sicherheitsmechanismen hinreichend ist, kann zu einer Herausforderung werden. Insbesondere die geforderte Mehrfachfehlerbeherrschung ab ASIL C kann nicht ohne weiteres beurteilt oder analysiert werden. Da Hardwarekomponenten in ihrer Physik beschreibbar sind, erlaubt die ISO 26262

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

auch für Neukomponenten eine solche Qualifikation. Es ist nicht die Absicht der Automobilindustrie irgendwann mal Widerstände nach dieser Norm entwickeln zu müssen. Bei Softwareelementen ist dies anders, hier gibt es ein Hinweis in der Norm, dass diese Art der Qualifikation für Neuentwicklungen nicht angewendet werden sollte. Verhält sich Software in einem anderen Mikrokontroller nicht oft anders? Dies wird insbesondere bei sicherheitsrelevanten Kommunikationssystemen noch eine Herausforderung, zumal dieser Hinweis einen Widerspruch zu den Anforderungen darstellt, auf bewährte Sicherheitsprinzipien zu setzen.

Bewährte Elemente, Betriebsbewährtheit (Proven in Use, PIU)

Dies ist einer der schwierigsten Themen der Sicherheitstechnik. In erster Linie hört man hier von den erfahrenen Entwicklern, dass es bisher doch keine Sicherheitsrisiken gab. Warum ist ein System nun nicht mehr „sicher"; nur weil so eine Norm veröffentlicht wurde? Das Risiko wurde bereits zum Einen am Anfang des Kapitels beschrieben, man weiß nicht ob der Anwendungsfall und die Integrationsumgebung und die an den Schnittstellen stattfindende Fehlerpropagation tatsächlich so identisch sind. Diese PIU gemäß ISO 26262 geht hier sogar von einem „Black-Box-Ansatz" aus, das heißt man kennte nicht das gesamte Innenleben der Elemente oder des Kandidaten, sondern man will hier die Sicherheit rein anhand der Eigenschaften an den äußeren Schnittstellen bewerten. Dies wird durch die Norm erschwert, denn sie fordert, die Performance und die Fehlerhäufigkeit im Feld zu quantifizieren. Diese Quantifizierung soll aber auf einem vergleichbaren Einsatzfall in einem vergleichbaren Integrationsumfeld basieren. Da insbesondere Mikrokontroller sich permanent ändern, bedeutet dies eine enorm große Hürde für Softwareelemente.

6.2 Validierung

Validierung wird oft als die Bestätigung von Zielen beschrieben. Valide verlangt auch eine gewisse Allgemeingültigkeit der Aussage, somit kann man sagen:

„Validieren ist der Nachweis, dass ein Ziel reproduzierbar erreicht wird."

Im Gegensatz zur Verifikation hat aber die Validation trotzdem einen Unschärfecharakter, den wir hier darin sehen wollen, dass man Ziele oft nicht so präzise formuliert wie Anforderungen, die allgemein verifiziert werden. Im Automobilsektor wird auch oft folgende Definition vorgefunden: „Die Kundenanforderungen werden validiert, aber die Anforderungen zum Beispiel im Lasten- oder Pflichtenheft werden verifiziert." Wobei dann das Lastenheft als der formulierte Kundenwunsch angesehen

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

wird und somit wieder validiert werden könnte. Folgende Aspekte werden mit dem Begriff Validieren zusammengebracht:

- lateinisch validus: stark, wirksam, gesund
- Validität: Gewicht einer Aussage, Untersuchung, Theorie oder Prämisse
- Englisch „valid“ wird im Deutschen oft mit „gültig sein“ übersetzt.
- Validation ist eine Methode zur Kommunikation mit Demenzpatienten.
- Validierung: Nachweis, dass ein Prozess, ein System und/oder die Produktion eines Wirkstoffes reproduzierbar die Anforderungen im praktischen Einsatz erfüllen
- Validierung bei einem Halbleiter sagt aus, dass der Halbleiter gemäß Spezifikation produziert werden kann.
- Validierung: externe Prüfung von Großprojekten und deren Nachhaltigkeitsberichten
- Validierung in der Informatik stellt den Nachweis dar, dass ein System die Anforderungen in der Praxis erfüllt.
- Validator bezeichnet eine Methode oder ein Programm , welches die Überprüfung gegenüber einem Standard bestätigen soll.
- Validierung oder Prüfung der Gültigkeit von Werten in der Statistik oder deren Plausibilität
- Methodenvalidierung weist nach, dass eine analytische Methode für ihren Einsatzzweck geeignet ist.
- Validierung beschreibt oft einen statistischen Nachweis.
- Validierung von Bildungsleistung
- Modellvalidierung soll zeigen, dass bei einer Implementierung des Modells durch das entstandene System die Realität ausreichend genau wiedergegeben wird.

Die hier adressierten Interpretationen stellen auch alle Aspekte dar, die in der Funktionssicherheit eine Rolle spielen. Durch diesen Fassettenreichtum des Begriffes war es jedoch schwierig, eine Definition des allgemeinen Validationsbegriffes zu finden. Somit hat man in der ISO 26262 den Begriff wesentlich enger gefasst. Alle anderen Validierungsaspekte wurden mit Verifikation oder Analyse umschrieben.

In Teil 4 Kapitel 9 wird die Aktivität der Sicherheitsvalidierung wie folgt beschrieben:

Das erste Ziel ist, aufzuzeigen, dass die Sicherheitsziele erfüllt werden und dass das Funktionale Sicherheitskonzept angemessen ist, die Funktionssicherheit des Fahrzeugsystems zu erlangen.

Das zweite Ziel ist aufzuzeigen, dass die Sicherheitsziele korrekt, vollständig und umfassend auf der Fahrzeugebene erreicht werden.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Hier in der Übersetzung wird der Begriff „aufzeigen“ verwendet, weil der Nachweis als solcher formal im Sicherheitsnachweis erbracht wird.

Unter der weiteren Überschrift „9.2 Allgemein“ wurde folgendes beschrieben:

> Die vorgelagerten Verifikationsaktivitäten (wie Designverifikation, Sicherheitsanalysen, Hardware-, Software-und Fahrzeugsystemintegrationen und Tests) dienen dem Zweck, dass die Ergebnisse der jeweiligen Aktivitäten die spezifizierten Anforderungen erfüllen. Die Validierung des integrierten Fahrzeugsystems soll die Angemessenheit für die beabsichtigte Verwendung und die Sicherheitsmaßnahmen für eine Fahrzeugklasse oder ein Fahrzeug aufzeigen. Die Sicherheitsvalidierung bietet die Sicherheit auf Basis von Untersuchungen und Tests, dass die Sicherheitsziele ausreichend abgedeckt sind.

Das heißt, alle Verifikationen sind Eingangsbestätigungen, dass alle relevanten Anforderungen und Spezifikationen korrekt für ein bestimmtes Fahrzeugsystem in einem bestimmten Fahrzeug oder einer Fahrzeugklasse umgesetzt sind. Die Validierung selbst basiert wiederum auf darauf aufbauenden Untersuchungen und Tests.

6.3 Modellbasierende Entwicklung

Modellbasierende Entwicklung wird viel diskutiert. Am häufigsten versteht man darunter die automatisierte Codegenerierung. Simulationen werden jedoch im Kontext der Funktionssicherheit insbesondere für Verifikationsaktivitäten genutzt. Da man zum Verifizieren den Gegenstand der Verifikation in abstrahierter Form eingeben muss, empfiehlt es sich, ein Modell entlang der Produktentwicklung reifen zu lassen. Ob man wirklich ein vollkommenes Modell, welches das gesamte Produkt in seiner Integrationsumgebung wiedergibt, erstellen möchte oder die Modelle für ihre Anwendungszwecke anpassen oder gar unabhängig entwickeln sollte, hängt von vielen Faktoren ab. Wichtig sollte es jedoch sein, dass Modelle, die in der Entwicklung genutzt werden, auch im Rahmen der Projektplanung betrachtet werden. Es stellt sich die Frage: „Was kann man von den notwendigen Aktivitäten automatisieren und welchen Zweck erfüllt das Modell?“.

Auf der Fahrzeugebene (vergleiche Informationsfluss Bild 6.2) wird ein Modell sehr sinnvoll sein, da man in der Entwurfsphase bereits sämtliche Annahmen am Modell va-

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

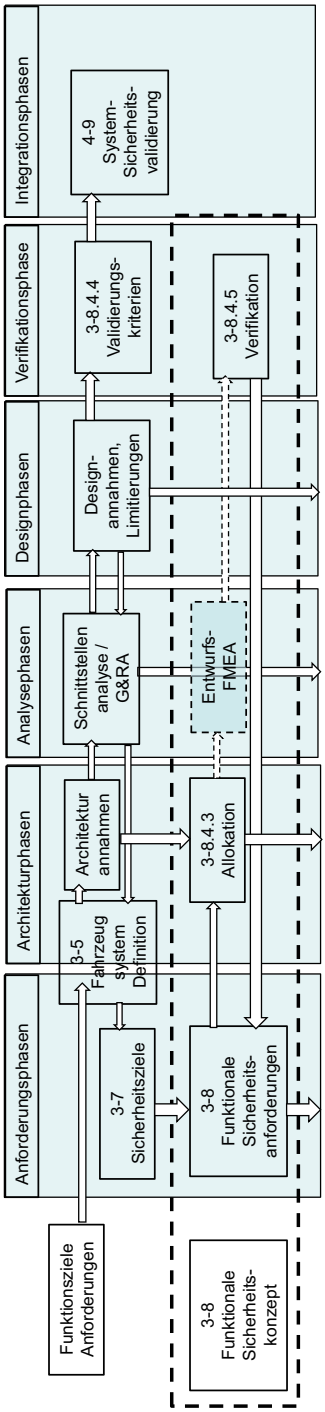

Bild 6.2 Aktivitäten auf Fahrzeugebene

lidieren kann. In der Anfangsphase der Entwicklung ist es ganz deutlich, dass Modelle dazu dienen, die Anforderungen besser zu verstehen oder das dynamische Verhalten überhaupt beschreiben zu können. Auf dem aufsteigenden Ast sind Modelle meist Abstrahierungen der entsprechenden Produktrealisierungen, an denen man dann prüfen kann, ob die Produkte hinreichend integriert werden können. Diese Modelle haben im Fokus die Realisierung so zu beschreiben, dass das Verhalten dem realisierten Produkt entspricht. Neben der Fehleranalyse dienen diese Modelle oft als Grundlage für Prüfstände (zum Beispiel HIL, (Hardware-in-the-Loop)), um automatisiert testen zu können. Das Realisierungsmodell wird oft nicht aus dem Anforderungsmodell abgeleitet, sondern unabhängig entwickelt. Dies hat den Vorteil, dass Tester nicht in die Anforderungsentwicklung eingebunden sein müssen und somit ein unabhängiges Testen gewährleistet sein kann. Geht es aber um die Verifizierung oder Validierung der Modelle oder um deren Konsistenz, so wird man sehen, dass die Aussagekraft solcher Modelle eingeschränkt ist. Weiter wird die Verifizierung der Anforderungen bezüglich korrekter Implementierung bei inkonsistenten Modellen nicht einfach sein. Der Vorteil solcher unabhängig entwickelten und validierten Modelle sind die Erkenntnisse bei einer Konsistenzprüfung. Hier werden natürlich die entsprechenden systematischen Fehler augenscheinlich. Eine parallele Entwicklung und Reifung des Modells und die systematische Verifikation oder Validation des Modells gegen die Anforderungen sowie gegen die bereits realisierten Eigenschaften wäre empfehlenswert. Dies kann natürlich nur für reduzierte Abstraktionen gelten. Eine vollständige Modellierung der Elektronik oder gar des verwendeten Mikrokontrollers ist heute möglich, aber doch sehr aufwendig.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

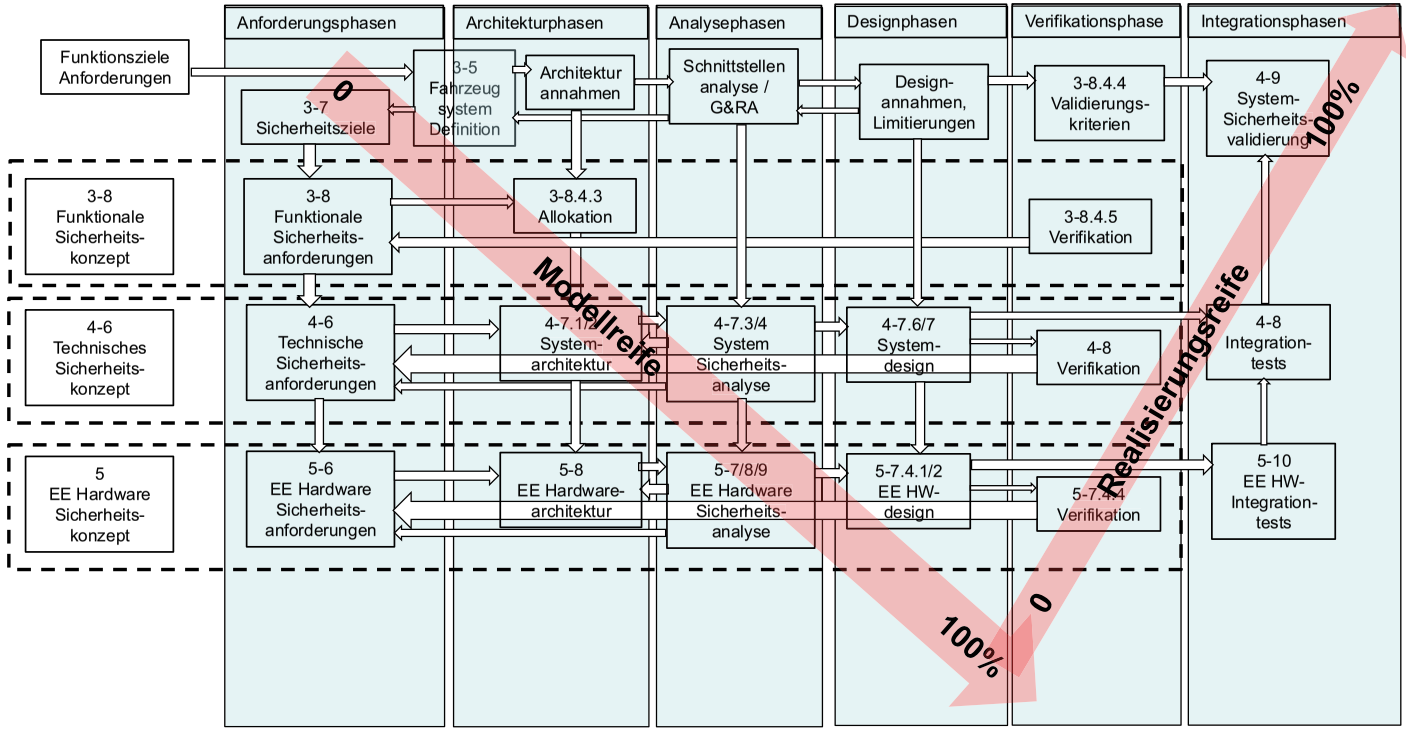

Bild 6.3 Modellreife gegenüber Reife des realisierten Produktes

Das Modell muss bis zur Realisierung der einzelnen Komponenten die beabsichtigte Zielreife erreicht haben. Das heißt, das Modell sollte den relevanten Anforderungen zu 100 % entsprechen. Die Integration der Komponenten, die anhand des Modells geplant und deren Korrektheit mit Hilfe des Modells argumentiert werden kann, erreicht ihre vollständige Reife mit der finalen Validierung. Diese Aussagen können jedoch nur gelten, wenn keine Änderungen in den Anforderungen während der Entwicklung zugelassen werden. Auf Basis der Architektur lassen sich aber wieder die Einflüsse der Änderungen erklären. Das Modell wird hier die Einflussanalyse, insbesondere für das technische Verhalten und die dynamischen Effekte, unterstützen.

6.3.1 Modelle für die Funktionale Sicherheit

Fahrzeugmodell: Ein solches Modell kann das Verhalten des Fahrzeugs im Kontext der Fahrsituationen zeigen, weiter kann es die Fahrzeugreaktion auf Basis möglicher Fehlfunktionen des zu integrierenden Fahrzeugsystems verdeutlichen. Solche Modelle unterstützen die Analyse und Verifikation der Fahrzeugsystemgrenzen sowie die Anforderungsanalyse für die beabsichtigten Funktionen. Im Wesentlichen kann ein solches Modell die Gefahren-und Risikoanalyse unterstützen und auch zu deren Verifikation wesentliche Hinweise liefern. Ein solches Modell kann um das Funktionale Sicherheitskonzept ergänzt werden, so dass die Ableitung der Funktionalen Sicherheitsanforderungen aus den Sicherheitszielen gegen die Sicherheitsarchitektur auf dieser horizontalen Ebene und damit die Allokation verifiziert werden. Auf einer funktionalen Ebene ist auch die Art und Weise simulierbar, wie bestimmte funktionale Sicherheitsmechanismen auf die möglichen Fehlfunktionen der Fahrzeugsysteme reagieren. Durch entsprechende zeitliche Simulationen ist auch die Intensität der Fehlfunktion während verschiedener Fehlertoleranzzeiten simulierbar, so dass die Fehlertoleranzzeitintervalle analysiert und definiert werden können. Weitgehend können diese Modelle auch die Integration des Fahrzeugsystems und deren Verifikation und Validation unterstützen.

Fahrzeugsystemmodell: Dieses Modell würde das Verhalten des Fahrzeugsystems darstellen, aber nicht das Verhalten und die Effekte des Fahrzeugsystems beziehungsweise die Fahrzeugreaktion im Verkehrsumfeld verdeutlichen können. Daher wäre das Modell geeignet, die relevanten Fehlfunktionen der Gefahren-und Risikoanalyse zu verifizieren. Es wäre nicht in der Lage die Sicherheitsziele selbst zu verifizieren oder gar zu validieren. Die Fahrzeugsystemgrenzen könnten analysiert und verifiziert werden, somit würde das Fahrzeugsystemmodell einen wichtigen und verifizierbaren Input für die Gefahren-und Risikoanalyse liefern. Auch bei der Integration des

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Fahrzeugsystems und der Verifikation würde ein Fahrzeugsystemmodell unterstützen können. Bei der Sicherheitsvalidierung wäre dieses Modell wieder nur eingeschränkt nutzbar, weil die Korrektheit der Sicherheitsziele nicht hinterfragt werden könnte. Mit heutigen Modellierungswerkzeugen kann man sehr gut Fahrzeugsystemmodelle in Fahrzeugmodelle überführen.

Systemmodell: Schwerpunkt eines Systemmodells bilden die Schnittstellen zu den Komponenten. Ein Systemmodell kann verschiedene horizontale Ebenen beschreiben, daher sollten die Ebenen, auf denen das Modell abstrahiert ist, klar definiert sein.

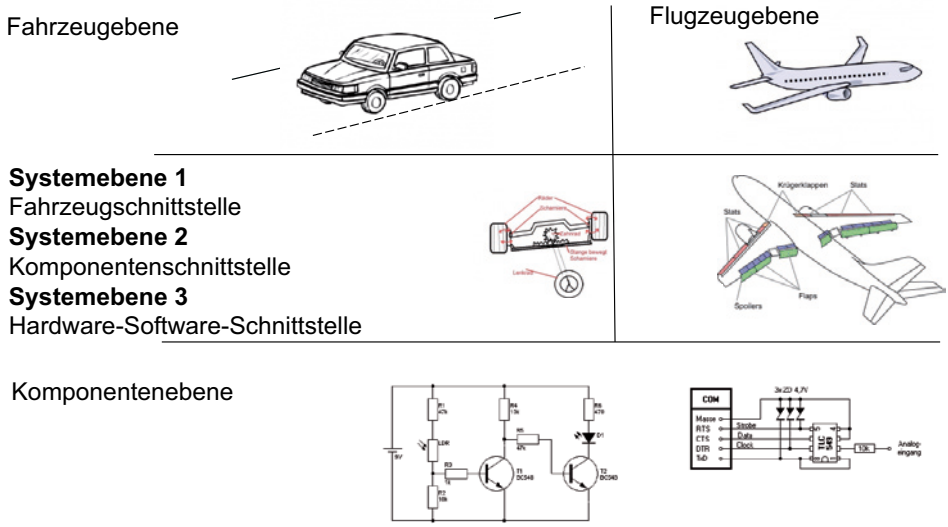

Bild 6.4 Horizontale Systemebenen

Das Systemmodell kann die Fahrzeugschnittstellen beschreiben, somit wären die unter dem Punkt Fahrzeugsystemmodell beschriebenen Aspekte gültig. Die Komponentenschnittstellen können auf dieselbe Art und Weise definiert werden, so dass das Verhalten der Komponenten und ihrer Funktionen beziehungsweise Funktionalitäten beschrieben beziehungsweise analysiert oder verifiziert werden. Ebenso könnte ein Modell des Mikrokontrollers genutzt werden, um die Hardware-Software-Schnittstelle und das Verhalten der Software im Mikrokontroller zu beschreiben, zu analysieren oder zu verifizieren. Selbst im Silizium benutzt man heute weitgehend Modelle zur Beschreibung der Halbleiterfunktionalitäten und validiert diese gegen die verschiedenen realisierten Muster. Das heißt, man nutzt einen Systemansatz, um das Innenleben des Siliziums darzustellen. Spezifikatio-

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

nen, Analysen und deren Verifikation und Validation (Validation als Prüfen gegen Kundenanforderungen) können auf Modellebene argumentiert werden. Bei der Fehleranalyse am Modell kann man wieder genauso vorgehen wie bei anderen Hardwaresystemen. Als Fehlerartenebene sollte man die Ebene der gewünschten Funktionalität und ihre Fehler sehen. Die Ursachenebene sollte die Ebene sein, auf der messbare oder beobachtbare Anomalien der realisierten Muster sowie die typischen systematischen Fehler beschreibbar sind. Wichtig ist hierbei in erster Linie, dass das Modell und die Realisierung kontinuierlich reifen, sodass das Modell mit jeder realisierten Eigenschaft auch entsprechend validiert wird. Korrekterweise würde nach ISO 26262 die Modellvalidierung auch eine Verifikation sein, aber auf diese für die Halbleiterindustrie branchenuntypische Bezeichnung wird hier verzichtet. Ein gutes Modell ist als Referenz für die technische Beschreibung reproduzierbar und hinreichend valide (gültig, geeignet), um die Analysen und Verifikationen am Modell zu argumentieren.

Grundsätzlich sind alle Modelle in der Sicherheitstechnik „Systemmodelle“. Die gesamte ISO 26262 beruht auf der Struktur, dass die Software- und Hardwarekomponenten auch über einen systemischen Ansatz beschrieben werden. Somit wird aus den Systemelementen immer eine solche Kombination gewählt, dass die gewünschte Funktionalität umgesetzt werden kann.

Modelle der Elektronik: Modellierung der Elektronik ist eine recht alte Disziplin. Bis heute hat sich SPICE (Simulation Program with Integrated Circuit Emphasis) als Grundlage erhalten. SPICE (PSPICE ist die PC-Version von SPICE) wurde 1973 ursprünglich am Electrical Engineering and Computer Sciences (EECS)-Fachbereich der University of California in Berkeley, entwickelt. Ein vergleichbarer noch älterer Algorithmus ist CANCER (Computer Analysis of Nonlinear Circuits Excluding Radiation). Kontinuierlich wurden diese Algorithmen verbessert und sie dienen heute noch als Grundlage zur Beschreibung von Elektronik inklusive der Halbleiter. Bekannte Systemmodellierungswerkzeuge haben die SPICE-Algorithmen integriert. Der Begriff SPICE hat nichts mit der Prozessbewertungsmethode zu tun, auf der zum Beispiel heute Automotive-SPICE beruht. Es ist nur ein Beispiel dafür, dass Elektroniker und „Softwerker“ keine systematische Kommunikation führen. Solche SPICE-Algorithmen können grundsätzlich in jede Systemumgebung eingebettet werden, sodass auch die System- und Softwareschnittstellen beschrieben werden können. Die SPICE-Algorithmen können das Temperatur-, Spannungs-, Stromverhalten sowie mechanische Einflüsse auf das Verhalten der elektrischen Bauelemente zueinander simulieren. Besonders aussagekräftig werden die Modelle dadurch, dass es für weitgehend alle elektrischen Bauelemente entsprechende Modellbibliotheken gibt, die auch das Verhalten der Bauelemente in ihrer Integrationsumgebung zeigen. Somit sind sogar Antenneneffekte durch

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

EMV-Störungen oder Drifts an Transistoren simulierbar, die als solches selbst mit Oszilloskopen nicht messbar sind. Weiter sind auch Wärmeverhalten und deren Propagationen innerhalb von Bauelementen und Steuergeräten simulierbar. Insbesondere bei der Analyse der abhängigen Fehler kann eine solche Simulation sinnvolle Ergebnisse liefern. Da die Fehlerpropagation basierend auf unterschiedliche Effekte simuliert werden kann, erkennt man Fehlerkaskaden. Hier hat man zum Beispiel die Möglichkeit die Ursachen der Fehlerkaskaden oder das propagieren der Fehlerkaskade mit adäquaten Maßnahmen zu reduzieren. Das heißt, die grundsätzlichen Prinzipien des Systemengineering inklusive der Fehlerpropagation sind auch für diese Elektronikmodelle auf der Elektronik- und Halbleiterebene anwendbar. Werden die Zuverlässigkeitsmethoden, die Prinzipien der statistischen Fehlerverteilung sowie der Umgebungs- oder Integrationsprofile in die Modellierung (zum Beispiel Arrhenius-Ansatz) einbezogen, so sind sogar quantitative Sicherheitsanalysen oder Analysen der Importanzen (Cut-Set-Analyse) am Modell darstellbar.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

6.3.2 Grundlage für Modelle

Die Grundlagen der Modelle gehen eigentlich wieder auf die Fragen von Paramides zurück, der vor 2500 Jahren bereits darauf hinwies, dass nicht alles so erklärbar ist, wie man es beobachtet. Sobald Einflussparameter dazukommen oder weggelassen werden, kann das beobachtete Verhalten sich ändern. Somit zeigt es sich, dass die Art der Abstraktion des Modells eine wesentliche Grundlage für die Aussagekraft bezüglich der Realisierung oder der Realität das Modell aufzeigen kann.

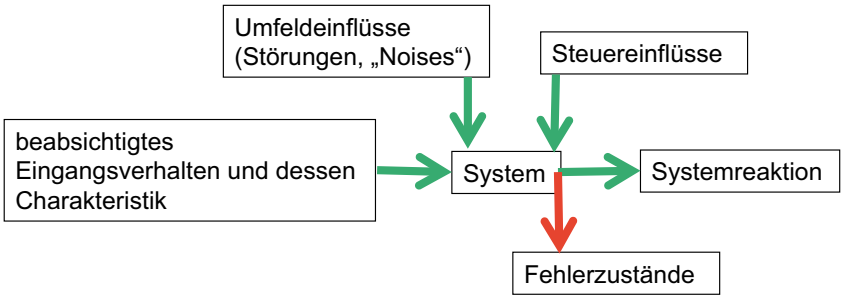

Bild 6.5 P-Diagramm

Bereits in den 50er Jahren wurde das P-Diagramm in der oben abgebildeten Form diskutiert. Die Basis bildet die Idee des Energietransfers. Die Eingangsgröße wird mit 100 % als die ideale Funktion angesehen. Könnte 100 % der Eingangsgröße

zu 100 % der Ausgangsgröße transformiert werden, würde es sich um ein ideales System handeln. Dies gibt es in der Realität nicht. Der zweite Satz der Thermodynamik bestätigt, dass eine 100prozentige Transformation nicht möglich ist, es gibt kein „Perpetuum mobile“. Das heißt, man prüft welche Einflüsse auf das abgeschlossene System aus der Umgebung für welche Abweichung am Ausgang sorgen. Durch diese 100 %-Regel kann die Referenz zu den Anforderungen (wurde das Modellverhalten zu 100 % spezifiziert) sowie zur Realisierung (sind die beobachtbaren Verhalten der Realisierung zu 100 % am Modell erklärbar) argumentiert werden, sodass Aussagen über den Grad der Abstrahierung und zur Modellreife möglich sind. Dies wurde methodisch zum Beispiel im Ford-FMEA-Handbuch inklusive der Auswertung der Störeinflüsse (Robustheitsmatrix) beschrieben. Dieses P-Diagramm dient als Grundlage für alle Metamodelle, die auch das Fehlverhalten von Systemen beschreiben können. Das heißt, alle Beschreibungen und auch Verhaltensmodelle weisen eine solche oder vergleichbare Struktur auf. Über den 100 %-Abgleich kann eine Vollständigkeitsargumentation geführt werden, sodass hier ein wesentliches Ziel der Verifizierung erreichbar wird. Diese Parameter des P-Diagramms müssen jedoch konsistent durch das gesamte Modell geführt werden. Ist das Modell nicht aus vergleichbaren (konsistenten) Metamodellen entstanden, so werden Konsistenz- und Vollständigkeitsaussagen aus dem Modell nicht ableitbar sein. Da beide Verifikationsziele die Grundlage für sicherheitstechnische Korrektheit bilden, ist ohne ein konsistentes Metamodell auch keine sicherheitstechnische Korrektheit aus einem Modell ableitbar. Sämtliche Parameter des Produktes bezüglich Anforderungen, Designeigenschaften, Architektur und die Realisierung selbst, inklusive aller Maßnahmen am Produkt, sowie sekundär die Verifikationen und Validation müssen sich auf P-Diagramme beziehen, technisch konsistent abgespeichert und archiviert werden. Ansonsten ist ein Change-Management, Konfigurationsmanagement, Variantenmanagement oder Base-lining für sicherheitstechnische Systeme nur bedingt möglich. Wird jedes Produkt, egal auf welcher horizontalen Abstraktionsebene, durch solche P-Diagramme beschrieben, ist auch der systemische Ansatz in jeder horizontalen Ebene konsistent, so dass die System-Engineering-Prinzipien auch auf der Software- und Hardwareebene angewendet werden können.

6.3.3 Modellbasierende Sicherheitsanalyse

Da klassische deduktive und induktive Analyseverfahren wie die FMEA oder Fehlerbaumanalyse nur begrenzt die Anforderungen oder die Realisierung wiedergeben können, sind modellbasierende Sicherheitsanalysen wichtige Methoden zur

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Erfüllung der Anforderungen der ISO 26262. Natürlich kann man nur automatisiert analysieren, was man auch automatisiert oder ins Modell eingebracht hat. Wie man aus der Idee der P-Diagramme sieht, sind Analysen und Verifikationen nur so gut wie die Grundlagen, die zur Analyse oder Verifikation zur Verfügung stehen, auch eine Basis dazu liefern. Der Vorteil der modellbasierenden Analyse liegt nur darin, dass man die Vorgänge automatisieren und auch Ergebnisse automatisiert weiteren Analysen zuführen kann.

Ein wesentlicher Vorteil der modellbasierenden Analyse beruht darauf, dass man mit heutigen Rechnern auch das dynamische Verhalten formalisiert darstellen und somit auch das dynamische Verhalten sicherheitstechnisch analysieren kann. Insbesondere das Verhalten im Fehlerfall sowie das Verhalten im Übergang von einem statischen Zustand in einen anderen, wie es bei verschiedenen Betriebsmodi der Fall ist, müssen sicherheitstechnisch betrachtet werden. Fehlverhalten bei solchen Übergängen von Systemzuständen führen bei heutigen hochdynamischen Systemen oft zu gefährlichen Effekten, die, zum Beispiel durch den Fahrer, nicht mehr beherrschbar sind. Selbst die Effekte, die bei den Übergängen der Systemzustände in den einzelnen Fahrsituationen zu Gefährdungen führen, können mit klassischen Analysemethoden nicht systematisch und vollständig beschrieben oder analysiert werden. Bei einem validen Modell kann man die Zustandsübergänge mit unterschiedlichen Parametern konfigurieren und über eine ganze Modellierungsreihe automatisiert auf jeder horizontalen Abstraktionsebene (zum Beispiel im Mikrokontroller, auf Komponentenebene oder auf beliebigen Systemebenen) modellieren. Die Beobachtung der Ausgangszustände und Abweichungen sowie die Fehlerreaktionen, wie am P-Diagramm beschrieben, erlauben eine systematische Auswertung.

Somit sind Fehlerkombinationen und sogar Kombinationen von dynamischen und statischen Fehlern darstellbar. So kann zum Beispiel ein Parametersatz von verschiedenen Drifts eines Kondensators am Eingang eines Transistors das veränderte Schaltverhalten bezüglich verschiedener Parameterfelder aufzeigen. Dieses Beispiel für eine Fehlerkaskade kann einen Doppelfehler oder gar einen Einzelfehler aufzeigen, der ohne eine solche Simulation nur durch aufwendige Tests und Berechnungen darstellbar wäre. Dies zeigt, dass die Simulation wesentlich mehr Transparenz bei der Analyse der abhängigen Fehler sowie der Mehrfachfehlerbetrachtung bietet. Dieses Beispiel aus der Elektronik ist natürlich auch auf Mechanik- oder Softwarekomponenten übertragbar sowie auf die Systemebene. Auf Systemebene sind insbesondere Fehlerkombinationen im Zusammenhang mit EMV-Einflüssen sehr schwer zu beschreiben, hier kann die Simulation eine wesentliche Unterstützung bieten. Ob die klassischen Sicherheitsanalysemethoden nun auf das Anforderungsmodell, das Realisierungsmodell oder auf die Realisierung

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

selbst angewendet werden, sollte von der Verifikations- und Validierungsstrategie abhängen. Man sollte jedoch die Modellbasierende Sicherheitsanalyse zuerst nur als Ergänzung für die klassischen Analysemethoden sehen. Es wäre eine Überlegung wert, die modellbasierende Sicherheitsanalyse als deduktive Analyse bevorzugt zu betrachten und die klassische FMEA als weiterhin induktive Analyse. Somit kann wiederum der systematische Ansatz eines konsistenten System-Engineering von der Fahrzeugebene bis hinunter in Siliziumstrukturen und die Software-Realisierung angewendet werden.

6.4 Freigaben

Freigaben werden bereits in der ISO 9000 und damit auch in der ISO TS 16949 adressiert.

Aus der ISO 9001:2008, Kapitel 7.3.3 „Entwicklungsergebnisse“:

Die Entwicklungsergebnisse müssen eine Form haben, die für die Verifizierung gegenüber den Entwicklungseingaben geeignet ist, und vor der Freigabe genehmigt werden.

Auch der Begriff „Produktfreigabe“ wird in unterschiedlichen Bezügen verwendet. Das heißt, dass bestimmte Aktivitäten sowie das Produkt einer Freigabe bedürfen. Wie eine solche Freigabe erfolgen soll, lässt die ISO 9001 offen. Es ist wiederum Aufgabe des jeweiligen Managementsystems die Art und Weise, wie eine solche Freigabe durchgeführt wird und was Gegenstand der jeweiligen Freigaben ist, zu definieren.

Dokumentierte Freigaben verlangen von dem Freigebenden, dass er sich über die Korrektheit und Angemessenheit der relevanten Aktivitäten und die erreichten Eigenschaften vergewissert hat und bestätigt, dass diese eingehalten werden. Das setzt voraus, dass er die hinreichende Kompetenz für diese Freigabe hat. Führt eine fahrlässig oder gar grob fahrlässig durchgeführte Freigabe zu einer Schädigung oder einer Gefährdung, so kann es sein, dass der Gesetzgeber oder auch Versicherungen aktiv werden. Was eine Fahrlässigkeit oder eine grobe Fahrlässigkeit im Einzelfall für rechtliche Folgen für das Unternehmen oder auch die Einzelperson selber haben kann, sollte hier nicht diskutiert werden. Hier sollte nur darauf aufmerksam gemacht werden, dass es hier weitergehende Regularien und Gesetze gibt. Insbesondere, wenn es sich bei der Freigabe um eine eindeutig gekennzeichnete Sicherheitsaktivität beziehungsweise um ein sicherheitsrelevantes Produkt handelt.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

6.4.1 Prozessfreigaben

In vielen APQP-Standards wird zuerst das Produkt und dann der Prozess freigegeben. Dies baut auf der Vermutung auf: Wenn das Produkt den Anforderungen und Zielen entspricht, dann kann der Prozess nicht vollkommen falsch gewesen sein. Wird der Prozess zuerst freigegeben, dann handelt es sich weitgehend um die Produktionsprozessfreigabe, die dann die Vorrausetzung für ein marktgerechtes Produzieren des Produktes ist. Weiter vermutet man, dass, wenn der Prozess gut abgelaufen ist, auch das Produkt eine entsprechende Qualität vorweist. Dies kann im Einzelnen zu gewaltigen Irrtümern führen.

Daher schlägt der VDA in seinem Band eine Prozess-, Produkt- und Projektfreigabe vor.

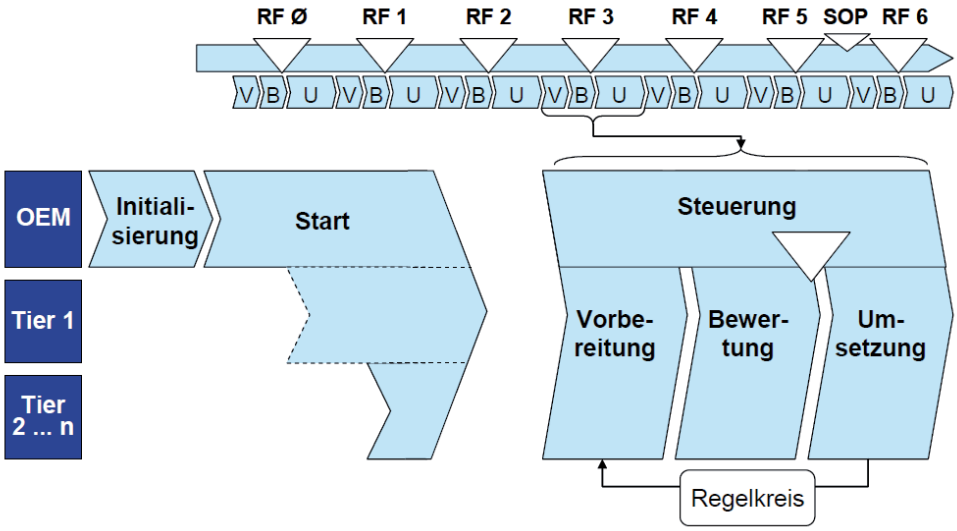

Bild 6.6 Phasenmodell der Reifegradabsicherung (Quelle: VDA Reifegradmodell für Neuteile)

Dies zeigt die entsprechende Reifegradabhängigkeit bei mehrstufigen Lieferketten.

Man sieht hier Arbeitsergebnisse und Meilensteine für die Lieferkette und die Projekte und Produkte, die die Lieferkette stützen.

Diese Meilensteinkonzepte und deren Prozessabsicherung dienen in erster Linie der Früherkennung von Projektrisiken, wobei Sicherheitsmängel am Produkt einer dieser Risiken sind.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.

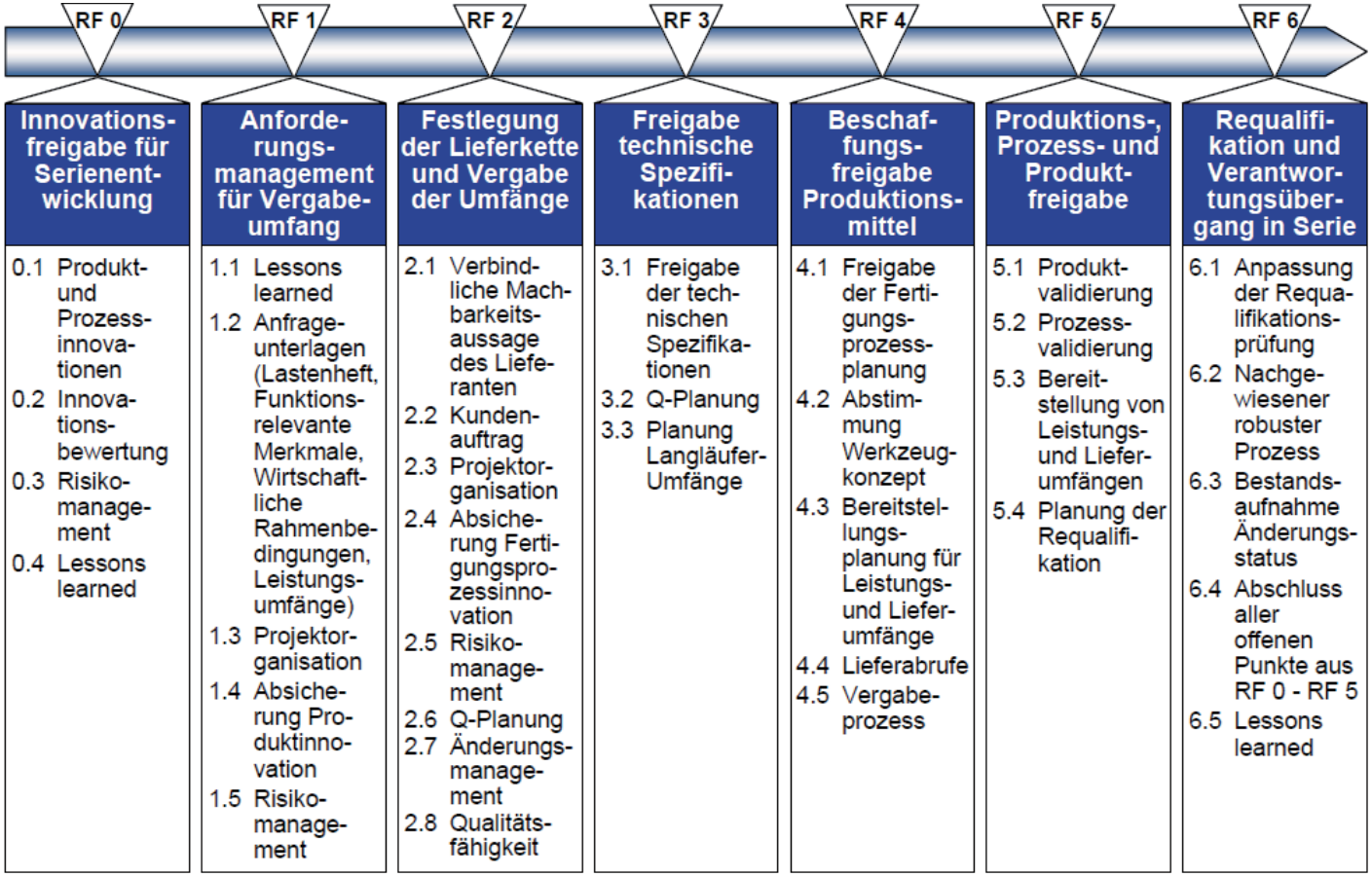

Bild 6.7 Übersicht über die Reifegrad-Inhalte RF 0 bis RF 6 und deren Reichweite (Quelle: VDA Reifegradmodell für Neuteile)

6.4.2 Freigabe zur Serienproduktion

Gemäß allen APQP-oder PPAP-Standards wird die Freigabe für die Serienproduktion, auch an die Zulieferer, durch den Fahrzeughersteller oder den Verantwortlichen in der darüberlegenden Hierarchie der Lieferkette gegeben. Aber in allen Standards behalten sich die Fahrzeughersteller vor, auch bei Sublieferanten von Lieferanten, die Korrektheit von Produktion und Produkt prüfen zu können.

Die ISO 26262 hat einige Anforderungen im Teil 4 Kapitel 11 dazu formuliert:

Freigabe zur Produktion

Ziel von diesem Kapitel ist es, die Freigabekriterien zur Produktion nach Fertigstellung der Fahrzeugsystementwicklung zu spezifizieren. Die Freigabe zur Produktion bestätigt, dass das Fahrzeugsystem die Anforderungen zur Funktionalen Sicherheit auf der Fahrzeugebene erfüllt.

Die Freigabe zur Produktion bestätigt, dass das Fahrzeugsystem für einen Serienproduktion und -betrieb geeignet ist.

Das Vertrauen für eine Serienentwicklung erfolgt aus

- der vollständigen Verifikation und Validierung von Hardware, Software, System, Fahrzeugsystem und der Fahrzeugebene und
- einem allumfassenden erfolgreichen Assessment der Funktionalen Sicherheit

Diese Freigabedokumentation bildet die Basis für die Produktion von Komponenten, Systemen oder Fahrzeugen. Die Freigabe sollte von einer Person unterschrieben werden, die für diese Freigabe verantwortlich ist.

Besonders die letzte Anforderung, dass eine solche Freigabe von Personen unterschrieben werden soll, ist zwar üblich in der Automobilindustrie. Ein Produkthaftungsanwalt, würde der Person nicht uneingeschränkt raten, eine solche Freigabe zu unterschreiben.

Funktionale Sicherheit im Automobil downloaded from www.hanser-elibrary.com by HS Ulm on February 2, 2019
For personal use only.