2 Warum Funktionssicherheit im Automobil?

Das Thema Funktionssicherheit spielte erst sehr spät im Vergleich zu anderen Branchen eine größere Rolle beim Automobilbau. Mehr Funktionalität, Komplexität von Produkt und Markt waren vom Kunden, den Hersteller und den Händlernetzen gefordert. Ein wesentlicher Grund war auf jeden Fall, dass die gesamte Fahrzeugtechnik doch in erster Linie von Maschinenbauern dominiert wurde. Hier waren natürlich auch die Sicherheitsmechanismen aus diesem Bereich entwickelt worden, ohne dass man sich dabei auf Elektronik und sogar Software verlassen hat. Das heißt, die Sicherheitsmechanismen beruhten in erster Linie auf robustem Design und hydraulischen oder pneumatischen Sicherheitsmechanismen. Mit zunehmender Automatisierung und Elektrifizierung von wesentlichen Fahrzeugfunktionen und dem Wunsch, diese Systeme für höhere Geschwindigkeiten und höhere Dynamik anwendbar zu machen, führte kein Weg mehr an der Elektrifizierung vorbei. Auch die Idee von Steer-by-wire und Brake-by-wire bis hin zum heutigen autonomen oder hochautomatisierten Fahren macht die Nutzung von software-basierenden Sicherheitsmechanismen unumgänglich. Sieht man einen heute üblichen Mittelklassewagen wie den Passat, so hat dieser circa 40 Steuergeräte, die weitgehend auch noch immer an einem CAN-Bus hängen. Man hat erkannt, dass es ohne einen Systemansatz keine komplexen Fahrzeugsysteme geben kann. Eine der wesentlichen Herausforderungen für die ISO 26262 war, dass es viele Methoden unterschiedlichster Ausprägung gab, jedoch keinen einheitlichen Systementwicklungsansatz. Es war die wesentliche Aufgabe bei der Entwicklung der ISO 26262, sich auf ein Grundverständnis zum Systemengineering zu einigen. Daher wird es nicht verwundern, dass in der „Introduction“ das Wort „System Engineering“ mehrfach auftaucht.

2.1 Risiko, Sicherheit und Funktionssicherheit im Automobil

Risiko wird allgemein als ein mögliches Ereignis mit einer negativen Auswirkung beschrieben. Der griechische Wortursprung wird auch für die Gefahr benutzt. Im Sinne der Produktsicherheit spricht man von dem Kreuzprodukt aus Eintrittswahrscheinlichkeit und Gefahr. Über den Begriff und die Definition des Risikos gibt es in der wirtschaftswissenschaftlichen Literatur und Diskussion verschiedene Auffassungen. Die Definitionen reichen von „Gefahr einer Fehlabweichung“ bis zur mathematischen Definition „Risiko = Wahrscheinlichkeit x Ausmaß“. Allgemeine Definition: Die Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens; dies bezieht sich auf Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen. Etymologisch kann man Risiko zum einen auf riza (griechisch = Wurzel, Basis) zurückverfolgen; siehe auch risc (arabisch = Schicksal). Auf der anderen Seite kann Risiko auf ris(i)co (italienisch) zurückverfolgt werden; „die Klippe, die es zu umschiffen gilt“. Sicherheit entstammt dem Lateinischen und könnte frei als ohne Sorge (se cura = ohne Sorge) übersetzt werden.

Sicherheit wird heute in verschiedenen Kontexten betrachtet: wirtschaftliche Sicherheit, Sicherheit der Umwelt, Zutritt- oder Zugriffssicherheit (hier wird im Englischen nicht das Wort „Safety“ sondern der Begriff „Security“ verwendet), aber auch im Bereich Arbeitssicherheit, Anlagen- und Maschinensicherheit und der Fahrzeugsicherheit. Der Begriff Sicherheit grenzt sich signifikant von dem Begriff der Funktionssicherheit ab.

Im Zusammenhang mit technischen Systemen oder Produkten wird Sicherheit als die Freiheit von unakzeptablen Risiken beschrieben. Als Schaden wird allgemein die Verletzung oder die Beeinträchtigung von Personen sowie Umweltschäden gesehen.

Folgende Gefährdungen werden unterschieden:

- chemische Reaktionen von Stoffen, Materialien etc. führen zu Brand, Explosion, Verletzung, gesundheitlicher Beeinträchtigung, Vergiftung, Umweltschäden etc.
- toxische Stoffe führen zu Vergiftung (auch Kohlenmonoxid), Verletzung (Folge durch z. B. Ausgasung von Batterie, Fehlreaktion des Fahrers, Werkstattpersonal), andere Schäden etc.
- hohe Ströme und insbesondere hohe Spannungen führen zu Schäden (insbesondere Personenschutz)
- Strahlungen (nuklear oder auch andere Strahlung (Folge z. B. Alpha-Teilchen in Halbleiter))

- thermisch (Schäden durch Überhitzung, Verbrennung, Brand, Schmoren, Rauch etc.)
- Kinetik (Verformung, Bewegung, beschleunigte Masse kann zu Verletzung führen)

Diese potenziellen Ursachen für Gefährdungen lassen sich nicht eindeutig abgrenzen, da chemische Reaktionen auch zu Vergiftungen, Überhitzung bis zum Brand und somit auch zu Rauchvergiftungen führen können.

Ähnliche Zusammenhänge sieht man bei zu hohen Strömen oder bei überhöhten Spannungen. Hohe Spannungen führen bei Berührung zu Verbrennungen von Personen, sie können aber auch die Ursache von Bränden sein. Die Überspannung wird oft als nicht-funktionales Risiko oder Gefahr gesehen. Daher wird in den meisten Standards solchen Gefahren durch Designvorgaben begegnet. Der Berührungsschutz an unserem Schutzkontaktstecker ist ein typisches Beispiel dazu.

Dies führt auch zu folgender Sicht und Abgrenzung zur Funktionalen Sicherheit.

Die Funktionssicherheit wird allgemein als eine korrekte technische Reaktion eines technischen Systems in einem definierten Umfeld, bei gegebener definierter Stimulation am Eingang des technischen Systems umschrieben. In der ISO 26262 wird Funktionssicherheit definiert als Freiheit von unakzeptablen Risiken basierend auf Gefahren, die durch Fehlfunktionen von E/E-Systemen verursacht werden. Hier werden in mechatronischen Systemen auch die Fehlfunktionen der mechanischen oder hydraulischen Systemkomponenten mit elektronischen Sicherheitsmechanismen zu beherrschen sein. Diese Abgrenzung wird später in Bezug auf den Scope der ISO 26262 diskutiert.

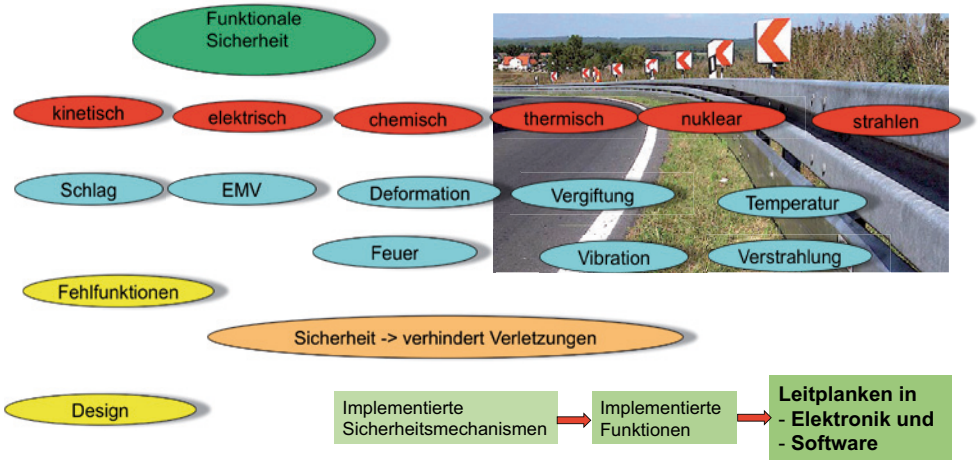

Bild 2.1 Funktionssicherheit und sicheres Design

Gerade beim Automobil hat man funktionale Absicherungen mit hydraulischen Systemen schon immer angewendet. Ein typisches Beispiel war hier das Zweikreisbremssystem oder die hydraulische Lenkung. Elektronische und softwarebasierende funktionale Sicherheitsmaßnahmen wurden erst im Wesentlichen mit ABS bei Bremssystemen vor 30 Jahren eingeführt. Vorher versuchte man allgemein durch hinreichend robuste System- und Komponentenauslegung (also durch das Design) die notwendige Sicherheit zu gewährleisten.

Folgende Definitionen zu Risiko, Gefahr und der Integrität wurden in der DIN EN 61508-1 (VDE 0803 Teil 1):2002-11 ergänzt:

A.5 Risiko und Sicherheitsintegrität

Es ist wichtig, dass die Unterscheidung zwischen Risiko und Sicherheitsintegrität vollständig erkannt wird.

Risiko ist ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten auftretenden gefahrbringenden Vorfalls. Es kann für unterschiedliche Situationen ausgewertet werden (EUC-Risiko, notwendiges Risiko, um das tolerierbare Risiko zu erreichen, tatsächliches Risiko (siehe Bild A.1)). Das tolerierbare Risiko wird auf gesellschaftlicher Basis bestimmt und berücksichtigt gesellschaftliche und politische Faktoren. Die Sicherheitsintegrität bezieht sich nur auf die sicherheitsbezogenen E/E/PE-Systeme, sicherheitsbezogene Systeme anderer Technologie und externe Einrichtungen zur Risikominderung. Die Sicherheitsintegrität ist ein Maß für die Wahrscheinlichkeit dieser Systeme/Einrichtungen, die notwendige Risikominderung in Bezug auf die festgelegten Sicherheitsfunktionen zufrieden stellend zu erreichen. Sobald das tolerierbare Risiko festgelegt und die notwendige Risikominderung bestimmt worden ist, können die Anforderungen zur Sicherheitsintegrität für die sicherheitsbezogenen Systeme zugeordnet werden (siehe 7.4, 7.5 und 7.6 der IEC 61508-1).

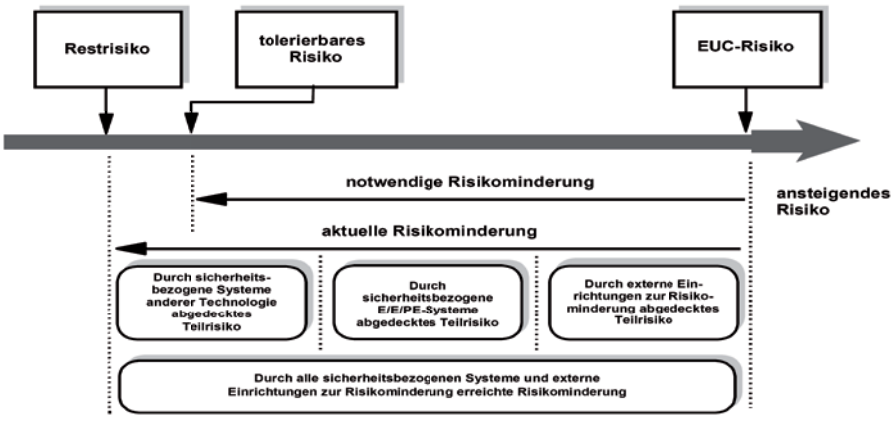

Bild 2.2 Risikominimierung gemäß IEC 61508 (Quelle: DIN EN 61508-1 (VDE 0803 Teil 1):2002-11)

Weiter zeigt die IEC 61508 folgende Darstellungen zu den Zusammenhängen:

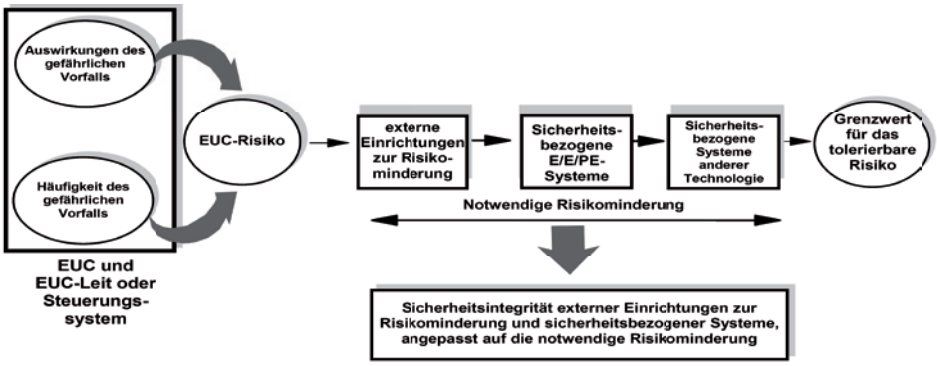

Bild 2.3 Risiko- und Sicherheitsintegrität gemäß IEC61508 (Quelle: DIN EN 61508-1 (VDE 0803 Teil 1):2002-11)

In der ISO 26262 wurde der Bezug zwischen Risiko, Gefahr und Sicherheitsintegrität anders definiert. Der Begriff der Sicherheitsintegrität wird in der ISO 26262 nicht direkt verwendet. Besonders der Begriff EUC (Equipment under Control) wurde nicht verwendet. EUC würde man mit dem „Gerät oder System welches sicherheitstechnisch beherrscht werden soll“ beschreiben. Die ISO 26262 lässt unter bestimmten Randbedingungen auch zu, dass die gewünschte Fahrzeugfunktion selbst sicherheitstechnisch ausprägt werden kann. In dem Fall, enthält das System keine Sicherheit durch das EUC selbst. Formal muss ja gemäß IEC 61508 das EUC und die Sicherheitsfunktionen einen Fehler zur gleichen Zeit verursachen, damit eine gefahrbringende Fehlerfolge entsteht. Wäre zum Beispiel ein hydraulisches Bremsensystem das EUC, welches in seiner Funktionen durch ein EE-System überwacht wird, dann könnten Fehler des hydraulischen Bremsensystems durch das EE-System abgewendet werden. In der Automobiltechnik nimmt dann meist von den mechanischen oder Systemen in anderer Technologie Kredit als „sichere“ Rückfallebene.

Wie bereits oben beschrieben, definiert die ISO 26262 die Funktionale Sicherheit als Freiheit von unakzeptablen Risiken basierend auf Gefahren, die durch Fehlfunktionen von E/E-Systemen verursacht werden. Jedoch werden auch Interaktionen von Systemen mit E/E-Funktionen eingeschlossen, somit wären mechatronische Systeme eingeschlossen. Ob rein mechanische Systeme in heutigen Automobilen wirklich keine Interaktion mit E/E zeigen, ist wohl zweifelhaft. Weiter schließt der Scope der ISO 26262 (einleitendes Kapitel, welches den Umfang der Norm beschreibt) wieder Gefährdungen wie elektrischer Schlag, Feuer, Rauch, Hitze, Strahlung, Vergiftung, Entflammung, (chemische) Reaktion, Korrosion, Freiwerden von Energie oder vergleichbare Gefahren aus, solange sie nicht durch Fehlfunktionen von elektrischen

Komponenten verursacht sind. Hier wird man wohl schnell die Batterie sehen, aber auch die giftigen Elektrolyte in Kondensatoren. Weiter kann man diskutieren, ob eine Motorwicklung eine elektrische Spule ist oder eine mechanische Komponente. Allgemein wird es schwer, bei nicht-funktionalen Gefahren tatsächlich den ASIL zu bestimmen. Grundsätzlich wurden bisher solche Komponenten hinreichend robust ausgelegt, so dass eine Gefährdung vermieden werden konnte. Im Rahmen der Gefahren- und Risikoanalyse ist es sehr schwer einer Design- oder Auslegungsschwäche einen ASIL zuzuordnen.

Der Scope der ISO 26262 schließt auch die funktionale Performance aus. Das heißt Funktionen, die bei korrekter Funktion bereits eine Gefährdung darstellen, werden allgemein durch die Gebrauchssicherheit vorab schon ausgeschlossen.

Die ISO 26262, Teil 3, Anhang B9 beschreibt die Zusammenhänge zwischen Risiko und Schaden wie folgt:

Ein Risiko (R = Risk) kann grundsätzlich als Kombination der Häufigkeit (f = frequency), mit der ein gefährlicher Vorfall auftritt, und dem möglichen Ausmaß des Schadens (S = Severity) beschrieben werden:

$R = f \cdot S$

Die Auftretenshäufigkeit (f) wird wiederum durch mehrere Parameter beeinflusst:

Da ist zum einen die Wahrscheinlichkeit, mit der das später realisierte System selbst ein gefährliches Ereignis bewirkt. Dieser Parameter ist gekennzeichnet durch unerkannte zufällige Fehler der Systemkomponenten und durch gefährliche systematische Fehler, die im System verblieben sind. Da eine Entwicklung gemäß dieser Norm solche Fehler vermeiden soll, ergibt sich dieser Parameter als Mindestforderung an das fertige System (Probability of dangerous failure). Er bleibt bei der Risikobestimmung deshalb zunächst außer Betracht.

Zum anderen ist die Dauer und Häufigkeit zu berücksichtigen, in der sich Personen in einer Situation befinden, in der die o. g. Gefahren gegeben sind (E = Exposure).

Nicht zuletzt, ist die Abwendbarkeit von Schäden durch rechtzeitige Reaktionen von beteiligten Personen (C = Controllability) mitentscheidend für den Eintritt eines Unfalls.

$f = E \cdot C$

Das (Kreuz-)Produkt E*C stellt einen Wert für die Auftretenswahrscheinlichkeit oder -häufung der äußeren Umstände dar, unter denen ein Fehler ein entsprechendes Potenzial für das angegebene Schadensausmaß besitzt.

Die ISO 26262 beschreibt eine normative Methode, nach der eine systematische Ableitung des potentiellen Risikos, das von der zu untersuchenden Betrachtungseinheit

(Item, Fahrzeugsystem) ausgehen könnte, auf Basis einer Gefahren- und Risikoanalyse durchgeführt werden kann. In anderen Sicherheitsstandards wird die Gefahren- oder Risikoanalyse nicht normative vorgegeben. Die Methoden werden nur beispielhaft beschrieben oder es werden Anforderungen an die Methoden formuliert.

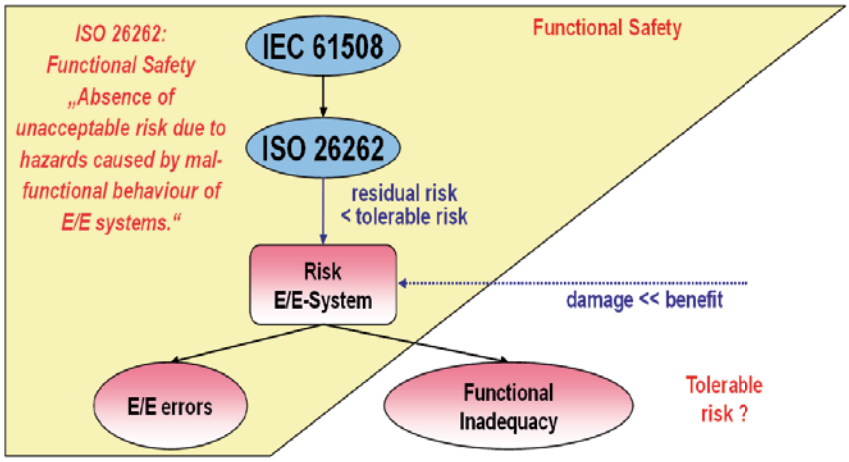

Bild 2.4 Abgrenzung zu Gefahren, basierend auf korrekt funktionierenden Systemen (Quelle: nicht realisiertes Forschungsprojekt)

Insbesondere wenn eine Funktion nicht geeignet ist beziehungsweise für bestimmte sicherheitsrelevante Funktionen falsch beschrieben ist, wird mit den in der ISO 26262 beschriebenen Aktivitäten und Methoden die notwendige Risikominimierung nicht erzielt werden können. Dies ist eine besondere Herausforderung, da die ISO 26262 weder das EUC (System, Maschine oder Gerät welches sicherheitstechnisch beherrscht werden soll) noch den Unterschied zwischen Sicherheitsfunktionen auf Anforderung (low demand) oder kontinuierlicher (high demand) Absicherung betrachtet. Woher leitet man ab, ob eine Reaktion des Fahrzeugsystems oder eine Messung (oder Ermittlung von Gefahrensituationen oder Objekten etc.) hinreichend, tolerierbar oder sicherheitstechnisch angemessen ist?

2.2 Qualitätsmanagementsystem

Prof. Dr. rer. nat. Dr. oec. h. c. Dr.-Ing. E. h. Walter Masing gilt als der Vater der Qualitätsmanagementsysteme, auf jeden Fall hier in Deutschland. Sein Standardwerk „Masing Handbuch Qualitätsmanagement" hat die Normierung und die Interpretation

von Qualitätsmanagementsystem weitgehend geprägt. Dieses Handbuch, ähnlich dem Dubbel für Maschinenbauer, geht in einigen Punkten massiv in die Tiefe. Insbesondere gilt dies für die Kapitel Statistik und Versuchsmethoden.

Dazu wurde folgende Kurzbeschreibung gegeben:

Dieses Werk fasst das gesamte Wissen über die moderne industrielle Qualitätssicherung von Wissenschaft und Technik zusammen. Zu jedem Beitrag wird eine sorgfältige Auswahl der wichtigsten Literatur gebracht, so dass dem Leser die vertiefende Beschäftigung mit seiner speziellen Problemstellung ermöglicht wird (Quelle: Masing Handbuch Qualitätsmanagement, Klappentext).

Dieser Text bezieht sich auf eine vergriffene oder nicht verfügbare Ausgabe dieses Titels.

Viele dieser Methoden und Systematiken sind dann auch in die ISO Reihe 9000 eingegangen. Als 2005 jedoch die Prozessorientierung mehr in den Mittelpunkt der Normenreihe gestellt wurde, sind die Themen Statistik und Versuchsmethodik immer mehr in die Fachliteratur verbannt worden.

In der Automobilindustrie gibt es eine Ergänzung zur ISO 9001, die ISO TS 16949. Hier werden Ergänzungen speziell zur Produktentwicklung und Produktion beschrieben, die sich weitgehend als Standards in der Automobilindustrie entwickelt haben.

Heute ist die Zertifizierung nach ISO TS 16949 die Grundlage, um als Zulieferer überhaupt an einen Automobilhersteller liefern zu dürfen. Asiatische Hersteller sehen hier noch andere Standards, jedoch liegt dies meist an einer anderen Historie. Besonders die Japaner haben ihre Qualitätsanforderungen mehr nach den Idealen der Six-Sigma-Philosophie (zum Beispiel DFSS, **D**esign **f**or **S**ix **S**igma) ausgeprägt. Insbesondere die statistischen Analyse- und Versuchsmethoden beruhen bei Masing, bei DSFF als auch in der Funktionssicherheit oft auf vergleichbaren Prinzipien.

Die ISO TS 16949 fordert in folgenden Kapiteln wesentliche Grundlagen für die Funktionssicherheit nach ISO 26262:

(Kapitel 4.2.3.1) Technische Vorgaben

„Die Organisation muss einem Prozess folgen, um die rechtzeitige Bewertung, Verteilung und Verwirklichung aller technischen Normen, Vorgaben und Änderungen des Kunden in Übereinstimmung mit der Terminplanung des Kunden sicherzustellen. Eine zeitgerechte Bewertung sollte unverzüglich durchgeführt werden und muss innerhalb von zwei Arbeitswochen erfolgen.

Die Organisation muss das Datum aufzeichnen, an dem jedwede Änderung in der Produktion verwirklicht wird. Zur Verwirklichung muss die Aktualisierung der Dokumente gehören.

Anmerkung: *Eine Änderung in diesen Normen oder Vorgaben erfordert eine aktualisierte Produktionsprozess- und Produktfreigabe des Kunden, wenn auf diese Normen*

oder Vorgaben in den Entwicklungsunterlagen Bezug genommen wird, oder wenn sie Auswirkungen auf die Dokumente der Produktions- und Produktfreigabe des Kunden haben, wie z. B. Produktionslenkungsplan, FMEA, usw.

Hier wird auf Dokumenten- und Änderungsmanagement, Verwendung von notwendigen Normen und Standards, Methoden, Arbeitsergebnisse und die Regelung von Verantwortungen (Freigaben) verwiesen, die in der ISO 26262 als QM-Maßnahmen angesehen werden.

(Kapitel 5.6.1.1) Leistung des Qualitätsmanagementsystems

Diese Bewertungen müssen alle Anforderungen des Qualitätsmanagementsystems und dessen Leistungstrends als wesentlichen Bestandteil des Prozesses der ständigen Verbesserung enthalten.

Bestandteil der Managementbewertung muss die Überwachung der Qualitätsziele sowie die regelmäßige Berichterstattung und Auswertung über die qualitätsbezogenen Verluste sein (siehe 8.4.1 und 8.5.1).

Diese Ergebnisse müssen dokumentiert werden, um mindestens einen Nachweis zu liefern über die Erreichung

- *der Qualitätsziele aus dem Geschäftsplan*
- *der Kundenzufriedenheit mit dem gelieferten Produkt.*

Im wesentlich ergibt sich hieraus, dass auch die Produktentwicklung sowie die Zufriedenheit der gelieferten Produkte dokumentiert und nachgewiesen werden müssen. Sollten es sich um sicherheitsrelevante Eigenschaften handeln, bedeutet dies, dass der Kunde im Besonderen beeinträchtigt werden kann.

(Kapitel 5.6.2) Eingaben für die Bewertung

Eingaben für die Managementbewertung müssen Informationen zu Folgendem enthalten:

a) *Ergebnisse von Audits,*

b) *Rückmeldungen von Kunden,*

c) *Prozessleistung und Produktkonformität,*

d) *Status von Vorbeugungs- und Korrekturmaßnahmen,*

e) *Folgemaßnahmen vorangegangener Managementbewertungen,*

f) *Änderungen, die sich auf das Qualitätsmanagementsystem auswirken könnten*

g) *Empfehlungen für Verbesserungen.*

Diese Aufzählung gehen auch unter dem Namen „Sicherheitskultur“ in Infrastrukturanforderungen ein, die für die Funktionssicherheit notwendig sind.

(Kapitel 5.6.2.1) Eingaben für die Bewertung – Ergänzung

Eingaben für die Managementbewertung müssen eine Analyse der tatsächlichen und potentiellen Ausfälle in der Gebrauchsphase und deren Einfluss auf die Qualität, Sicherheit und Umwelt enthalten.

Diese Kapitel verweist direkt auf die notwendige Feldbeobachtung, die auch gesetzlich im Rahmen der Produkthaftungsgesetze gefordert sind. Hier wird auch auf Sicherheitsmängel direkt verwiesen.

(Kapitel 5.6.3) Ergebnisse der Bewertung

Die Ergebnisse der Managementbewertung müssen Entscheidungen und Maßnahmen zu Folgendem enthalten:

a) *Verbesserung der Wirksamkeit des Qualitätsmanagementsystems und seiner Prozesse,*

b) *Produktverbesserung in Bezug auf Kundenanforderungen,*

c) *Bedarf an Ressourcen.*

Insbesondere zu dieser Aufzählung wird man in der ISO 26262 weitere Ergänzungen finden.

(Kapitel 6) Management von Ressourcen

6.1 Bereitstellung von Ressourcen

Die Organisation muss die erforderlichen Ressourcen ermitteln und bereitstellen, um

a) das Qualitätsmanagementsystem zu verwirklichen und aufrechtzuerhalten und seine Wirksamkeit ständig zu verbessern,

b) die Kundenzufriedenheit durch Erfüllung der Kundenanforderungen zu erhöhen.

6.2 Personelle Ressourcen

6.2.1 Allgemeines

Personal, das die Produktqualität beeinflussende Tätigkeiten ausführt, muss auf Grund der angemessenen Ausbildung, Schulung, Fertigkeiten und Erfahrungen fähig sein.

Diese Kapitel 6.1 und 6.2 zeigen, dass auch bei Entwicklungen gemäß einem Qualitätsmanagementsystem bereits wesentliche Anforderungen an die Personen, deren Qualifikation sowie an die Art und Weise wie die Produktentstehung organisiert werden soll, formuliert sind.

(Kapitel 7.3.1.1) Bereichsübergreifender Ansatz

Die Organisation muss einen bereichsübergreifenden Ansatz anwenden, um die Produktrealisierung vorzubereiten, einschließlich:

- *Entwicklung, Festlegung und Überwachung besonderer Merkmale,*
- *Entwicklung und Überarbeitung der FMEA, einschließlich Maßnahmen zur Reduzierung potentieller Risiken, Entwicklung und Überarbeitung der Produktionslenkungspläne.*

Anmerkung: *Ein bereichsübergreifender Ansatz umfasst normalerweise das Personal aus den Organisationsbereichen Entwicklung, Produktion, Produktionsplanung, Qualität, und anderes zu beteiligendes Personal.*

Dieser bereichsübergreifende Ansatz der ISO TS 16949 definiert die Grundlagen für die notwendige Sicherheitskultur als Grundlage zur Funktionssicherheit.

(Kapitel 7.3.2.3) Besondere Merkmale

Die Organisation muss besondere Merkmale ermitteln (siehe 7.3.3 d) und

- *alle besonderen Merkmale in den Produktionslenkungsplan einbeziehen*
- *den vom Kunden festgelegten Definitionen und Symbolen entsprechen,*
- *Dokumente zur Lenkung des Produktionsprozesses einschließlich Zeichnungen, FMEA, Produktionslenkungspläne und Bedienungsanweisungen kennzeichnen mit dem Symbol des Kunden für besondere Merkmale oder einem entsprechenden Symbol oder Hinweis der Organisation, um diejenigen Prozessschritte einzuschließen, die sich auf besondere Merkmale auswirken.*

Anmerkung: *Zu den besonderen Merkmalen können Produktmerkmale und Prozessparameter gehören.*

Dieses Kapitel definiert eigentlich den bisherigen Weg, wie man mit Sicherheitsanforderungen in der Automobilindustrie umgegangen ist. Besonders für eine sichere Auslegung von Mechanikteilen werden „Besondere Merkmale“ auch weiterhin benutzt. Auch für die Schnittstelle zur Produktion von sicherheitsrelevanten Komponenten definiert dieses Kapitel die Grundlage.

(Kapitel 7.3.3.1) Ergebnisse der Produktentwicklung - Ergänzung

Die Ergebnisse der Produktentwicklung müssen in einer Form vorliegen, die gegenüber den Anforderungen bezüglich der Eingaben für die Produktentwicklung verifiziert und validiert werden kann. Die Ergebnisse der Produktentwicklungen müssen Folgendes enthalten:

- *Design-FMEA, Zuverlässigkeitsprüfungen,*
- *besondere Merkmale für das Produkt, Spezifikationen,*
- *Fehlervermeidung für das Produkt, soweit anwendbar,*
- *Produktfestlegung einschließlich Zeichnungen oder mathematische Daten,*

- *Ergebnisse von Produktentwicklungsbewertungen,*
- *Diagnoseleitfäden, falls zutreffend.*

Hier handelt sich es um eine Aufzählung von Arbeitsergebnissen der Produktentwicklung, die in der ISO 26262 entsprechend für sicherheitsrelevante Produkte und Komponenten erweitert werden muss. Auch diese Arbeitsergebnisse würden im Falle einer sicherheitsrelevanten Produktentwicklung Bestandteil des Sicherheitsnachweises sein.

(Kapitel 7.3.3.2) Ergebnisse der Produktionsprozessentwicklung

Die Ergebnisse der Produktionsprozessentwicklung müssen in einer Form vorliegen, die gegenüber den Anforderungen bezüglich der Eingaben für die Produktionsprozessentwicklung verifiziert und validiert werden können. Die Ergebnisse der Produktionsprozessentwicklung müssen Folgendes enthalten:

- *Spezifikationen und Zeichnungen,*
- *Produktionsprozess-Flussdiagramm oder -Layout,*
- *Prozess-FMEA,*
- *Produktionslenkungspläne (siehe 7.5.1.1),*
- *Arbeitsanweisungen,*
- *Annahmekriterien für die Prozessfreigabe,*
- *Daten zu Qualität, Zuverlässigkeit, Instandhaltbarkeit und Messbarkeit,*
- *Ergebnisse der Maßnahmen zur Fehlervermeidung, soweit anwendbar, – Methoden zur schnellen Ermittlung und Rückmeldung von Fehlern am Produkt oder im Produktionsprozess*

Diese Liste ergänzt die notwendigen Arbeitsergebnisse während der Produktion. Hier gibt es in der ISO 26262 recht wenige weitere Anforderungen, da dieser Bereich durch die Qualitätsmanagementsysteme sehr gut geregelt ist.

7.5.1.1 Produktionslenkungsplan

Die Organisation muss

- *Produktionslenkungspläne (siehe Anhang A) auf den Ebenen System, Subsystem, Bauteil und/oder Material für das zu liefernde Produkt erstellen einschließlich jener für Prozesse zur Produktion von verfahrenstechnischen Produkten und Teilen,*
- *einen Produktionslenkungsplan für die Phasen Vorserie und Serie erstellen, der die Ergebnisse der Design-FMEA und Prozess-FMEA berücksichtigt.*

Der Produktionslenkungsplan muss

- *die zur Produktionsprozesslenkung verwendeten Lenkungsmaßnahmen aufführen,*
- *Methoden zur Überwachung der Lenkung von besonderen Merkmalen (siehe 7.3.2.3) enthalten, die vom Kunden und der Organisation festgelegt wurden,*
- *die vom Kunden geforderten Informationen, falls zutreffend, enthalten*
- *festgelegte Reaktionspläne auslösen (siehe 8.2.3.1), wenn der Prozess nicht mehr beherrscht oder die statistische Prozessfähigkeit nicht mehr gegeben ist.*

Produktionslenkungspläne müssen bewertet und aktualisiert werden, wenn Änderungen eintreten, die das Produkt, den Produktionsprozess, Messgrößen, Logistik, Lieferquellen oder FMEA (siehe 7.1.4) beeinflussen.

Anmerkung: *Nach Bewertung oder Aktualisierung des Produktionslenkungsplanes kann eine Freigabe durch den Kunden gefordert sein.*

Insbesondere die Anforderungen an die Produktionslenkung, an die vorausgehende Entwicklung und die notwendigen Analysen, wie FMEAs sind in der ISO TS 16949 beschrieben. Selbst, wenn diese Produkte ohne jegliche Sicherheitsanforderungen gemäß eines Qualitätsmanagementsystems zu entwickeln sind müssen diese Analysen für die Produktentwicklung vorliegen.

2.2.1 Qualitätsmanagementsysteme aus Sicht der ISO 26262

Die ISO 26262 verweist nur in wenigen Kapiteln auf die Qualitätsmanagementsysteme. Diese Anforderungen sind im Allgemeinen die Grundlage um Funktionssicherheit überhaupt in der Automobilindustrie anwenden zu können. Inhaltlich findet man viele Themen in dem Beispiel zur Sicherheitskultur im Anhang von Teil 2 der ISO 26262 wieder. Die ISO 26262 fasst diese grundlegenden Anforderungen sehr kurz wie folgt zusammen:

ISO 26262 Teil 2:

(Kapitel 5.3.2) Weitere unterstützende Informationen

Die folgenden Informationen können betrachtet werden:

Existierendes Vertrauen aus einem Qualitätsmanagementsystem, gemäß von Qualitätsstandards wie ISO TS 16949, ISO 9001 oder ähnliche.

(Kapitel 5.4.4) Qualitätsmanagement während des Sicherheitslebenszyklus

5.4.4.1 Die Organisation, die in die Umsetzung des Sicherheitslebenszyklus eingebunden ist muss ein gelebtes Qualitätsmanagementsystem haben, welches den Qualitätsstandards wie ISO TS 16949, ISO 9001 oder ähnliche entspricht.

Das heißt, ein gelebtes (und bei der Produktentwicklung angewendetes) Qualitätsmanagementsystem ist die Grundlage zur Funktionssicherheit. Weltweit wird von allen Fahrzeugherstellern die ISO TS 16949 gefordert. Daher kann man die anderen Qualitätsmanagementstandards zurzeit vernachlässigen. Im Rahmen der ISO 26262 wird man immer wieder Arbeitsergebnisse finden, die nur um die Sicherheitsaspekte ergänzt werden müssen.

In weiteren Ergänzungen zur ISO TS 16949 findet man folgende Definition zur Qualität:

Qualität ist definiert als „die Gesamtheit von Merkmalen einer Einheit bezüglich ihrer Eignung, festgelegte oder vorausgesetzte Erfordernisse zu erfüllen". Der Begriff „Einheit" ist hierbei weit gefasst und wie folgt festgelegt: „Das, was einzeln beschrieben und betrachtet werden kann." Die Qualität bezieht sich demnach auf Merkmale und Eigenschaften eines fertigen Produktes nach dessen Herstellung. Allgemein wird angenommen, dass diese Eigenschaften noch eine gewisse Zeit nach der Herstellung erhalten bleiben. Häufig wird dieser Zeitraum mit der Garantiezeit gleichgesetzt. Sofern in der Spezifikation festgelegt wurde, dass die nach der Fertigung vorhandenen Merkmale und Eigenschaften über die definierte Nutzungszeit erhalten bleiben sollen, ist die Zuverlässigkeit ein Bestandteil der Qualität.

In dieser Definition wird auch bereits ein Lebenszyklusansatz gefordert, daher sollte es für Qualitätsmerkmale wie Sicherheit eine Selbstverständlichkeit sein.

2.3 Qualitätsvorausplanung

Die ISO TS 16949 ist für die einzelnen Anwendungsfälle sehr unterschiedlich interpretierbar. Auch bereits früher haben die verschiedenen Automobilhersteller daher Standards definiert, wie man die Qualität in der Produktentstehung gewährleisten kann. Die amerikanischen Hersteller (Ford, GM und Chrysler) haben sich dann zur AIAG zusammengefunden und haben gemeinsame Vorgaben zur Qualitätssicherung herausgegeben. In Deutschland wurden im Rahmen des VDAs vergleichbare Stan-

dards erarbeitet. Zusammenfassend definierte man Prozesse für die Entwicklung wie Qualitätsvorausplanung, APQP (Advanced Product Quality Planning, gemäß AIAG) oder PQVP (Produkt Qualitätsvorausplanung).

Der VDA und die AIAG veröffentlichen eine Reihe von Dokumenten, die als Grundlagen für die VDA- oder AIAG-Mitglieder gesehen werden. Diese Bände sind oft auch in den Vertragsunterlagen für Zulieferer verbindlich referenziert. Leider ist die Konsistenz dieser Dokumente nicht vorbildlich. Zum Beispiel beschreiben beide Organisationen eine FMEA-Methode (oder auch mehrere FMEA-Methoden), die als Grundlage für die ISO 26262 betrachtet werden können. Auch Meilenstein- oder Reifegradkonzepte wurden von diesen Verbänden erarbeitet. Diese dienten in erster Linie der Synchronisierung zwischen Automobilhersteller und Zulieferer.

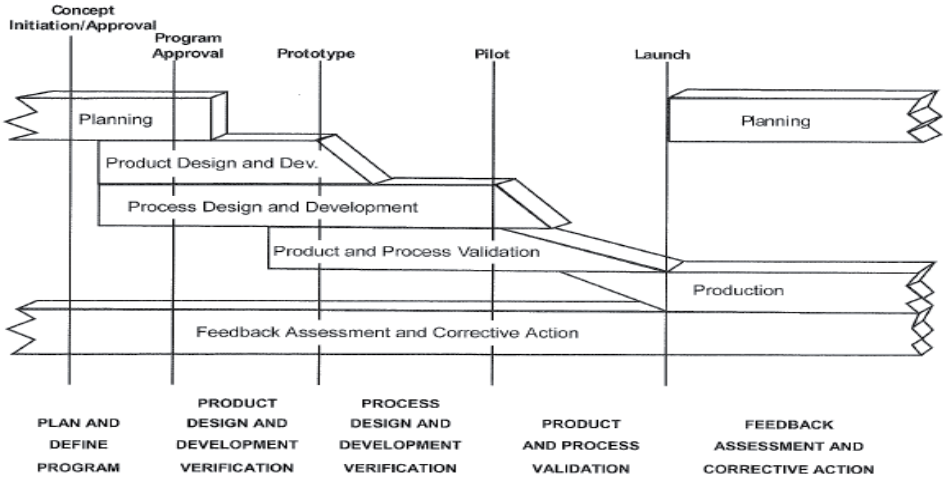

Bild 2.5 Qualitätsvorausplanung (Quelle: APQP AIAG 4th Edition)

Die AIAG hat die APQP in 5 „Meilensteine“ definiert.

- Die erste Phase „Konzept, Initiierung, Prüfung“ ist eine reine Planungsphase.
- In der zweiten Phase, vor der Programmprüfung soll die Planung, sowie die Produkt- und Prozessentwicklung eine gewisse Reife haben. Im Rahmen der Programmprüfung soll die Realisierbarkeit des Produktes geprüft werden.
- In der dritten Phase sollen die ersten Prototypen entstehen, Verifikationen (meist Prototypentests) und die Produkt- und Prozessvalidierung sollen angestoßen werden. Produktdesign sollte weitgehend abgeschlossen sein.
- In der vierten Phase entstehen die ersten seriennahen (Pilot-)Produkte. Diese sollten auch mit Serienwerkzeugen gefertigt werden.

- Mit dem Produktlaunch beginnt die Serienentwicklung, das heißt alle Lieferketten müssen stehen und die Produktion muss Serienstückzahlen in hinreichender Menge und Qualität sicher liefern können.

Nach dem Produktlaunch wird erwartet, dass eine Bewertung der Produktentwicklung stattfindet und entsprechende Korrekturmaßnahmen initiiert werden. Alle Aktivitäten unterliegen einer kontinuierlichen Monitoring und notwendige Korrekturmaßnahmen auch bei Feldauffälligkeiten sollen entsprechend eingeleitet werden.

Der VDA hat zu dem Themenkomplex folgende Veröffentlichungen:

VDA:

- Band 1

  Qualitätsmanagement in der Automobilindustrie - Dokumentation und Archivierung; Leitfaden zur Dokumentation und Archivierung von Qualitätsforderungen und Qualitätsaufzeichnungen -insbesondere bei kritischen Merkmalen; 3. vollständig überarbeitete Auflage, Oktober 2008

- Band 2

  Sicherung der Qualität von Lieferungen - Lieferantenauswahl, Qualitätssicherungsvereinbarung, Produktionsprozess- und Produktfreigabe Qualitätsleistung in der Serie, Deklaration von Inhaltsstoffen (4.Auflg.2004) (diese wird wohl bald neu veröffentlicht).

- Band 3 Teil 01

  Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten - Zuverlässigkeitsmanagement / 3. Auflage 2000

- Band 3 Teil 02

  Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten- Zuverlässigkeits- Methoden und -Hilfsmittel / 3. Auflage 2000, akt. 2004

- Band 4 Kapitel Produkt- und Prozess FMEA

  Einlage Ringbuch - Produkt- und Prozess FMEA, 2. überarbeitete Auflage 2006, aktualisierter Nachdruck 2009 (schon im Ringbuch Band 4 enthalten!)

Die genannten Bände werden kontinuierlich überarbeitet. Weitere Themen, wie Reifegrad von Produkt und Prozess, standardisierte Lastenhefte usw. werden in dem Rahmen immer wieder veröffentlicht.

2.4 Prozessmodelle

Vorgehensmodelle oder Prozessmodelle haben auch bereits eine lange Geschichte. Folgende Historie zeigt den Ursprung insbesondere für Software-intensive Produkte:

1. Erster Ansatz zur Entwicklung übersichtlicher Programme (1968)

Dijkstra schlägt die „strukturierte Programmierung" vor (Vermeidung von GOTO-Anweisungen).

2. Entwicklung von Software-Engineering-Prinzipien (1968–1974)

Es werden die theoretischen Grundlagen (Prinzipien) erarbeitet, die der strukturierten Entwicklung von Programmen zugrunde liegen: strukturierte Programmierung, schrittweise Verfeinerung, Geheimnis-Prinzip, Programmodularisierung, Software-Lifecycle, Entity-Relationship-Modell, Software-Ergonomie

3. Entwicklung von phasenspezifischen Software-Engineering-Methoden (1972–1975)

Umsetzen der Software-Engineering-Prinzipien in Entwurfsmethoden: HIPO, Jackson, Constantine-Methode, erste Version von Smalltalk

4. Entwicklung von phasenspezifischen Werkzeugen (1975–1985):

Der Einsatz von SE-Methoden mit maschineller Unterstützung (z. B. Programminversion, Batchwerkzeuge)

5. Entwicklung von phasenübergreifenden (integrierten) Software-Engineering-Methoden (ab 1980)

Es sollen die Ergebnisse einer Phase des Software-Lifecycles automatisch an die nächste Phase weitergegeben werden: Methodenverbund

6. Entwicklung von phasenübergreifenden (integrierten) Werkzeugen (ab 1980)

Einsatz einer Datenbank als automatischer Schnittstelle zwischen den einzelnen Phasen des Software-Lifecycles. Interaktiver Programmaufruf durch CAS-Werkzeuge

(Computer Aided Softwaredesign)

7. Definition verschiedener, konkurrierender objektorientierter Methoden (ab 1990)

Es entstanden parallel verschiedene objektorientierte Analyse- und Entwurfsmethoden

(Booch, Jacobson, Rumbaugh, Shlaer/Mellor, Coad/Yourdon u. a.).

Die Methoden wurden in CASE Tools (Computer Aided Software Engineering) realisiert.

8. Integration der OO-Methoden zur UML – Unified Modeling Language (ab 1995)

Jacobson, Booch und Rumbaugh schließen sich zusammen und entwickeln die UML. In der UML sollen die Schwächen der frühen OO-Methoden beseitigt werden und ein weltweit gültiger, einheitlicher Standard geschaffen werden. Die UML 1.0 wurde 1997 verabschiedet.

9. UML 2.0

Nachdem die UML 1.0 bis zur Version UML 1.5 erweitert wurde, erschien 2004 die UML 2.0. In dieser Version wurden die Sprachelemente der UML an aktuelle Technologien angepasst; es wurden Redundanzen und Inkonsistenzen in der Sprachdefinition beseitigt.

Quelle: Liste ohne Quelle aus dem Internet.

Diese Historie zeigt, dass es rein erfahrungsbasierende Ansätze sind. Einschränkungen für die Programmierung haben im Laufe der Zeit zu formalisierten Beschreibungsformaten geführt. Als man dann im Rahmen der Prozessorientierung diese „Best Practices“ als formalisierte Aktivitäten beschrieb, entstanden die Prozessmodelle als Referenzmodelle oder wie das Beispiel UML zeigt formalisierte Beschreibungssprachen. Bestimmte Prinzipien, wie auch dass man Anforderungen nur annimmt, wenn man diese umsetzen und mittels Tests die korrekte Umsetzung zeigen kann, sind in diese Vorgehensweisen eingeflossen.

2.4.1 V-Modelle

Das nachfolgende Bild zeigt die Entwicklung der Prozessmodelle und ihre Modelle zur Prozessverbesserung, wie CMM, SPICE oder ähnliche. Als Ursprung wird hier auch die ISO 9001 und die ISO 12207 genannt. Die ISO 12207 ist in der Bibliographie der ISO 26262 genannt. Es steht aber nirgends in der ISO 26262 welchen Bezug die ISO 12207 zur ISO 26262 hat.

Überraschend ist, dass sich die Prinzipien der Prozessorientierung für die Produktentwicklung bei den Asiaten lange nicht so ausgebildet haben, wie wir es heute aus den Prozessmodellen kennen. Die ISO 12207 bildete weitgehend auch die Basis für die Prozess-Assessmentmodelle (PAM) auf Basis von CMM oder SPICE. Insbesondere diese Prozess-Assessmentmodelle in Bezug zur Sicherung von Eigenschaften von Software zu bringen, entstand erst später.

Die Kernfrage ist, ob ein solcher generischer Prozess wirklich mehr darstellt, als er nach den SPICE-Definitionen auch darstellen sollte. Hier ist das V-Modell als Referenzmodell beschrieben. Sprich, wenn man Anforderungen an Entwicklungsaktivitäten beschreibt, dann ist es sinnvoll, diese gemäß einem Referenzmodell zu strukturieren.

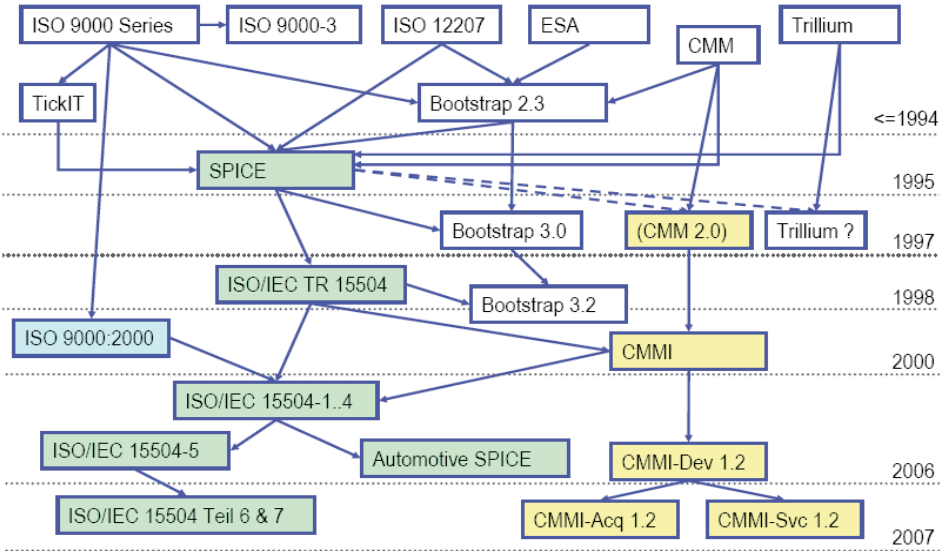

Bild 2.6 Historie von V-Modell basierenden Vorgehensmodellen (Quelle: Flecsim)

Das V-Modell XT, welches nun schon in der Version 1.2 vorliegt, beschreibt das V nur für die Entwicklung der einzelnen Produkte.

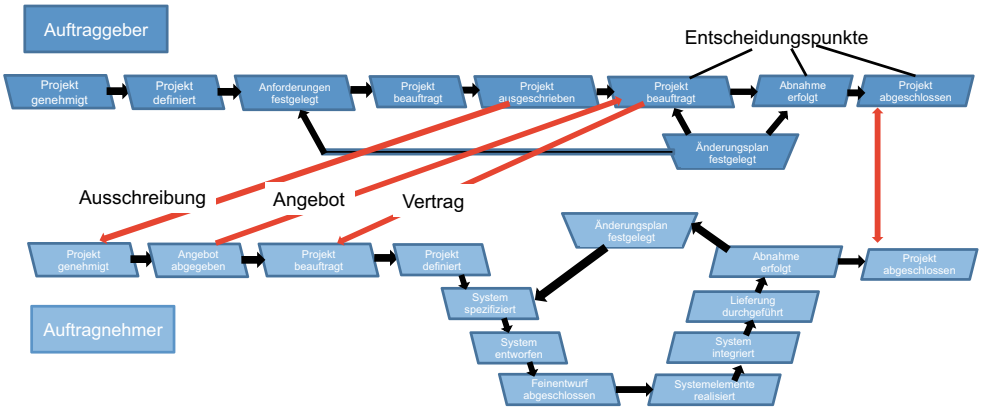

Bild 2.7 Schnittstelle V-Modell Auftragnehmer, Auftraggeber gemäß V-Modell XT (Quelle: V-Modell XT 1.2)

Das V-Modell XT hat eine längere Einlaufstrecke in der zuerst die Kundenlieferanten Beziehung definiert wird. In dieser Phase werden der Produktumfang und die grundlegenden Anforderungen festgelegt. Diese Einlaufstrecke ist vergleichbar

mit dem Teil 8, Kapitel 5 (Schnittstellen in der verteilten Entwicklung), wo auf die Schnittstellenvereinbarung (DIA, Development Interface Agreement) zwischen Entwicklungspartner hingewiesen wird. Hier soll vereinbart werden, wer welche Aktivitäten, wie umsetzt und wer für die verschiedenen Produktpakete (oder Produktelemente) verantwortlich ist.

SPICE (Software Process Improvement and Capability Determination) wird in der öffentlichen Diskussion oft in Zusammenhang mit der ISO 26262 gebracht. SPICE basiert weitgehend auf zwei Normen, der ISO 12207 sowie der ISO 15504.

Die ISO 12207 „Prozesse im Software Lebenszyklus“ bot ein Prozessreferenzmodell mit folgenden Kategorien:

- Kunden-Lieferanten-Prozesse,
- Entwicklungsprozesse,
- unterstützende Prozesse,
- Managementprozesse,
- Organisationsprozesse.

In Teil 6 der ISO 26262 steht die ISO 12207 unter der Bibliographie im Anhang, es gibt aber keinen Verweis, welchen Bezug diese Normen zueinander haben.

Hier wurden 40 Prozesse beschrieben, die als Grundlage für SW basierende Produkte als wichtig betrachtet wurden. Daraus hat die ISO 15504 ein Prozessassessmentmodell (PAM) abgeleitet.

Die ISO 15504 besteht aus folgenden Teilen:

ISO 15504-1: Konzepte und Vokabeln

Begriffe und generelle Konzeption.

ISO 15504-2: Durchführung eines Assessments

- die Anforderungen für ein Prozessreferenzmodell,
- die Anforderungen für ein PAM,
- die Definition eines Rahmenwerks zur Messung für die Prozessfähigkeitslevel (Process Capability),
- die Anforderungen für ein Assessmentprozess-Rahmenwerk.

ISO 15504-3: Guideline zur Assessmentdurchführung

Guideline zur Durchführung eines zu ISO 15504-2 konformen Assessments:

- Bewertungsframework für die Prozessfähigkeitslevel,
- PRM und PAM,
- Auswahl und Benutzung von Assessment-Tools,

- Kompetenz von Assessoren,
- Überprüfung der Konformität.

ISO 15504-4: Guideline zur Benutzung von Assessmentergebnissen

- Auswahl von PRM,
- Bestimmen der Zielfähigkeit,
- Definition des Assessment-Inputs,
- Schritte der Prozessverbesserung,
- Schritte zur Bestimmung von Fähigkeitsleveln,
- Vergleichbarkeit von Assessment-Outputs.

ISO 15504-5: Beispielhaftes Prozessassessmentmodell (PAM)

Beispielhaftes PAM, welches die Anforderungen an ISO 15504-2 erfüllt, und Informationen über die Assessment-Indikatoren.

ISO 15504-6: Beispielhaftes PAM ISO 15228

- Struktur des PAM's
- Prozess Performance-Indikatoren
- Prozess Fähigkeits-Indikatoren

ISO 15504-7: Guideline zur Bestimmung des Unternehmensreifegrad

Zwischen CMMI und SPICE gab es immer einen Unterschied hinsichtlich der Bewertung. So bewertet SPICE immer einzelne Prozesse, kann aber nicht wie CMMI an der Stelle den Reifegrad eines Unternehmens messen. CMMI fasst an der Stelle bestimmte Prozesse zusammen und leitet einen Reifegrad für das Unternehmen ab. Dieses wird mit dieser ISO 15504-7 auch möglich.

ISO 15504-8: Beispielhaftes Prozessassessmentmodell (PAM) für ISO 20000

Beispielhaftes PAM für das IT Service Management

ISO 15504-9: Prozessprofilziele

Teil 9 ist als Technische Spezifikation (TS) eine Vorstufe zur Norm, die Prozessprofilziele beschreibt.

ISO 15504-10: Safety Extension (Sicherheitserweiterung)

Aspekte zur Sicherheit

Die ISO 15504 wurde von der AutoSIG als Grundlage für Automotive SPICE® genutzt. Für das PAM (Prozess-Assessmentmodell) und die PRM (Prozess-Referenzmodell) wurden die Teile 2 und 5 verwendet. Auf Automotive SPICE® wird im Kapitel Prozessanalyse zur Funktionalen Sicherheit näher eingegangen.

Weitere Lebenszyklusansätze zur SW Entwicklung:

- ISO/IEC/IEEE 16326 Systems and software engineering – Life cycle processes – Project management (2009)
- SAE J2640, General Automotive Embedded Software Design Requirements (April 2006)
- IEEE STD829, Standard for Software and System Test Documentation (2008)
- ISO/IEC 9126 Software engineering – Product quality (2001)
- ISO/IEC 15288 Systems engineering – System life cycle processes (2002)
- ISO/IEC 26514 Systems and software engineering – Requirements for designers and developers of user documentation (2008)

All diese Standards haben bei der Entwicklung der ISO 26262 eine Rolle gespielt, somit sind Erfahrungen mit diesen Standards auch in die ISO 26262 eingeflossen. Jedoch steht keiner dieser Standards aus der Aufzählung in einer normativen Beziehung zur ISO 26262.

Eine besondere Rolle spielen die Normen der ISO/IEC 25000er Reihe. Parallel zur ISO 26262 wurde die ISO Reihe 25000 entwickelt, diese ersetzt seit 2005 die ISO/IEC 9126.

Die Basisnorm heißt:

ISO/IEC 25000 Software engineering – Software product Quality Requirements and Evaluation (SQuaRE)

Diese Normenreihe stellt Qualitätskriterien auf. Die ISO-Organisation fordert alle Normenarbeitsgruppen auf, sich an diesen Festlegungen zu orientieren.

Folgende Definitionen werden exemplarisch aus Sicht der ISO/IEC 25000 betrachtet und der Sichtweise der ISO 26262 gegenübergestellt:

Funktionalität: Inwieweit besitzt die Software die geforderten Funktionen? – Vorhandensein von Funktionen mit festgelegten Eigenschaften. Diese Funktionen erfüllen die definierten Anforderungen.

Widerspricht weitgehend nicht dem Verständnis der ISO 26262.

Angemessenheit: Eignung von Funktionen für spezifizierte Aufgaben, zum Beispiel aufgabenorientierte Zusammensetzung von Funktionen aus Teilfunktionen.

Der Begriff wird in der ISO 26262 so nicht verwendet. Dagegen wird der Begriff „Fähigkeit“ verwendet. Zum Beispiel: „Hat ein Sicherheitsmechanismus die Fähigkeit das spezifizierte Fehlerbild zu beherrschen?“.

Richtigkeit: Liefern der richtigen oder vereinbarten Ergebnisse oder Wirkungen, zum Beispiel die benötigte Genauigkeit von berechneten Werten.

Im Rahmen der Verifikation wird von Korrektheit gesprochen. Die Richtigkeit einer Anforderung ein wichtiges Kriterium in der Sicherheitstechnik.

Interoperabilität: Fähigkeit, mit vorgegebenen Systemen zusammenzuwirken.

Sicherheitstechnisch ist eine gewollte korrekte Interoperabilität ähnlich zu verstehen. Jedoch wird in der ISO 26262 mehr auf das fehlerhafte Zusammenwirken von Elementen und Systemen eingegangen.

Sicherheit: Fähigkeit, unberechtigten Zugriff, sowohl versehentlich als auch vorsätzlich, auf Programme und Daten zu verhindern.

Hier geht man mehr auf Sicherheit im Sinne des englischen Wort „Security“ ein. Schwerpunkt in der ISO 26262 ist die Sicherheit im Sinne des englischen Worts „Safety“.

Ordnungsmäßigkeit: Merkmale von Software, die bewirken, dass die Software anwendungsspezifische Normen oder Vereinbarungen oder gesetzliche Bestimmungen und ähnliche Vorschriften erfüllt.

Erfüllen von Standards wie der ISO 26262 selbst wird mit Konformität übersetzt.

Zuverlässigkeit: Kann die Software ein bestimmtes Leistungsniveau unter bestimmten Bedingungen über einen bestimmten Zeitraum aufrechterhalten? – Fähigkeit der Software, ihr Leistungsniveau unter festgelegten Bedingungen über einen festgelegten Zeitraum zu bewahren.

- *Reife: Geringe Versagenshäufigkeit durch Fehlerzustände.*
- *Fehlertoleranz: Fähigkeit, ein spezifiziertes Leistungsniveau bei Software-Fehlern oder Nicht-Einhaltung ihrer spezifizierten Schnittstelle zu bewahren.*

Zuverlässigkeit wird im vergleichbaren Kontext verwendet, jedoch auch für System und Hardware.

Wiederherstellbarkeit: Fähigkeit, bei einem Versagen das Leistungsniveau wiederherzustellen und die direkt betroffenen Daten wiederzugewinnen. Zu berücksichtigen sind die dafür benötigte Zeit und der benötigte Aufwand.

Der Begriff wird so nicht verwendet, würde aber keinen Widerspruch darstellen.

Konformität: Grad, in dem die Software Normen oder Vereinbarungen zur Zuverlässigkeit erfüllt.

Konformität wird in der ISO 26262 besonders in Bezug zur Sicherheit gestellt.

Benutzbarkeit: Welchen Aufwand fordert der Einsatz der Software von den Benutzern und wie wird er von diesen beurteilt? – Aufwand, der zur Benutzung erforderlich ist, und individuelle Beurteilung der Benutzung durch eine festgelegte oder vorausgesetzte Benutzergruppe.

Die Qualifikation von zum Beispiel Komponenten, beschreibt die Eignung der Komponenten in Sicherheitsanwendungen.

Effizienz: Wie liegt das Verhältnis zwischen Leistungsniveau der Software und eingesetzten Betriebsmitteln? – Verhältnis zwischen dem Leistungsniveau der Software und dem Umfang der eingesetzten Betriebsmittel unter festgelegten Bedingungen.

- *Zeitverhalten: Antwort- und Verarbeitungszeiten sowie Durchsatz bei der Funktionsausführung.*
- *Verbrauchsverhalten: Anzahl und Dauer der benötigten Betriebsmittel bei der Erfüllung der Funktionen. Ressourcenverbrauch, wie CPU-Zeit, Festplattenzugriffe usw.*

Effizienz wird in der ISO 26262 mehr mit Güte einen Fehler zu beherrschen gesehen, jedoch stellt diese Beschreibung keinen Widerspruch dar.

Wartbarkeit/Änderbarkeit: Welchen Aufwand erfordert die Durchführung vorgegebener Änderungen an der Software? – Aufwand, der zur Durchführung vorgegebener Änderungen notwendig ist. Änderungen können Korrekturen, Verbesserungen oder Anpassungen an Änderungen der Umgebung, der Anforderungen oder der funktionalen Spezifikationen einschließen.

- *Analysierbarkeit: Aufwand, um Mängel oder Ursachen von Versagen zu diagnostizieren oder um änderungsbedürftige Teile zu bestimmen.*
- *Modifizierbarkeit: Aufwand zur Ausführung von Verbesserungen, zur Fehlerbeseitigung oder Anpassung an Umgebungsänderungen.*
- *Stabilität: Wahrscheinlichkeit des Auftretens unerwarteter Wirkungen von Änderungen.*
- *Testbarkeit: Aufwand, der zur Prüfung der geänderten Software notwendig ist.*
- *Konformität: Grad, in dem die Software Normen oder Vereinbarungen zur Änderbarkeit erfüllt.*

Insbesondere die Änderbarkeit wird im Rahmen eines unterstützenden Prozess (Änderungsmanagement) mehr spezifisch gesehen.

Übertragbarkeit: Wie leicht lässt sich die Software in eine andere Umgebung übertragen? – Eignung der Software, von der Umgebung in eine andere übertragen werden zu können. Umgebung kann organisatorische Umgebung, Hardware- oder Software-Umgebung sein.

- *Anpassbarkeit: Fähigkeit der Software, diese an verschiedene Umgebungen anzupassen.*
- *Installierbarkeit: Aufwand, der zum Installieren der Software in einer festgelegten Umgebung notwendig ist.*
- *Koexistenz: Fähigkeit der Software neben einer anderen mit ähnlichen oder gleichen Funktionen zu arbeiten.*

- *Austauschbarkeit: Möglichkeit, diese Software anstelle einer spezifizierten anderen in der Umgebung jener Software zu verwenden, sowie der dafür notwendige Aufwand.*
- *Konformität: Grad, in dem die Software Normen oder Vereinbarungen zur Übertragbarkeit erfüllt.*

Diese Gedanken und Begriffe erhalten in der ISO 26262 einen andern Kontext. Zum Beispiel Koexistenz von Software unterschiedlicher Kritikalität (unterschiedlicher ASIL) sieht kein Risiko darin, dass die Funktionen ähnlich sind, sondern dass diese Funktionen sich negativ beeinflussen könnten. Weiter muss darauf hingewiesen werden, dass die ISO 26262 die Begriffe validieren, verifizieren, analysieren, Audit, Assessment und Review im Kontext der Funktionssicherheit für Straßenfahrzeuge anders definiert und verwendet. Diese Beispiele zeigen auch, dass Anforderungen, Begriffe oder Definitionen innerhalb der ISO 26262, je nach dem aus welcher Aktivität oder Kontext diese aufgerufen werden, zu unterschiedlichen Interpretationen führen können.

Weiter gibt es noch zwei Basisprozessmodelle, auf die man eingehen sollte, um die zulässige Varianz der Prozesse in der Entwicklung gemäß ISO 26262 zu betrachten.

2.4.2 Wasserfallmodell

Das Wasserfallmodell ist ein Vorgehensmodell, das man häufig in der Tool-Entwicklung vorfindet.

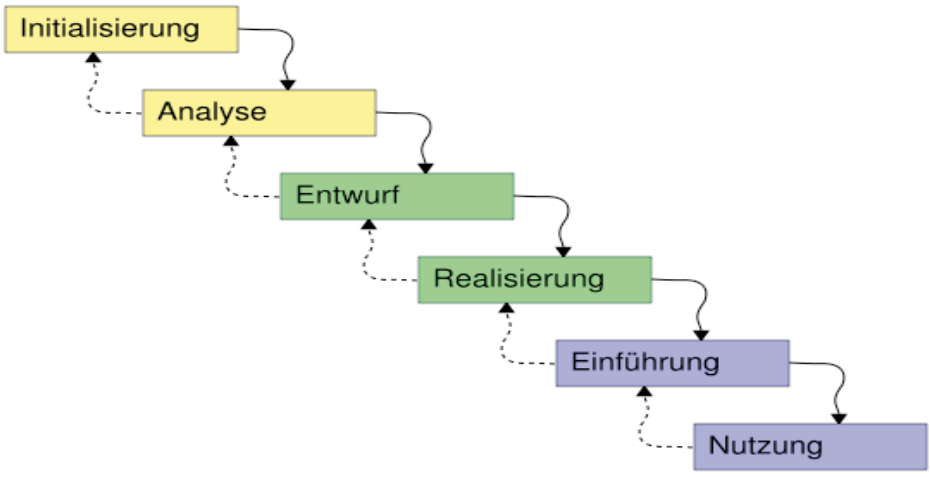

Bild 2.8 Wasserfallmodell (Quelle: Wikipedia)

Es gibt in der Literatur keine eindeutige Quelle für das Wasserfallmodell. So gibt es auch unterschiedliche Beschreibungen und Interpretationen, wie das Wasserfallmodell für die verschiedenen Anwendungen genutzt werden kann. Der Wasserfall beschreibt im Allgemeinen eine höhere Abstraktionsebene als dies die meisten V-Modelle beschreiben. Grundsätzlich kann man sich auch vorstellen, dass das Wasserfallmodell für die Entwurfs- und Realisierungsphase in einen V-Zyklus übergeht.

Vergleicht man die Wasserfallmodelle mit den V-basierenden Prozessmodellen, so beschreiben diese auch einen größeren Anteil eines Lebenszyklus.

Die Initialisierungsphase wird in allen anderen Vorgehensmodellen auch als linearer Startpunkt gesehen, wo die Interessenten (Stakeholder, dazu im Kapitel „Stakeholder einer Architektur“ mehr) oder die Quellen von Anforderungen (Vergleiche mit Eng. 1 von SPICE; Anforderungserhebung; „Requirement Elicitation“) für ein System identifiziert werden.

Einführung und Nutzung bis hin zur Produktdefinition beziehungsweise zum Lasten-Pflichtenheftabgleich werden bei den Prozessmodellen oft als linearer Einlauf beschrieben. Die Iterationen werden in den weiteren Phasen nicht näher dargestellt. Iterationen der Planungs- und Definitionsaktivitäten zwischen Kunde und Dienstleister werden nicht unbedingt in die Entwicklungsaktivitäten eingeschlossen.

Hier zeigt es sich sehr deutlich, dass die meisten Vorgehensmodelle aus der IT-Welt abgeleitet sind. Eine Ableitung des Wasserfallmodells für die Automobilindustrie würde wohl dem Sicherheitslebenszyklus der ISO 26262 oder den verschiedenen APQP-Standards ähneln.

2.4.3 Spiralmodell

Das V-Modell wird auch immer wieder im Automotive-Kontext diskutiert. Jedoch scheint das traditionelle Vorgehensmodell im Automotive-Bereich das Spiralmodell zu sein.

Wie bereits in dem Kapitel Qualitätsvorausplanung beschrieben, bestimmen die Musterphasen weitgehend die Entwicklungsaktivitäten in der Automobilindustrie.

Diese Abbildung (Spirale) zeigt den sequenziellen Ablauf und die entsprechenden Iterationen in Form einer Spirale.

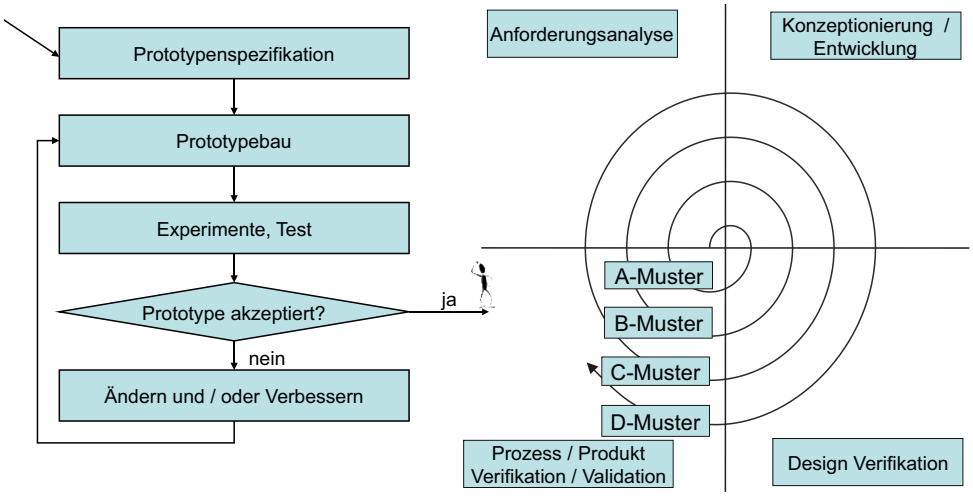

Bild 2.9 Spiralmodell für den Prototypenzyklus

Die traditionellen Musternamen wie A-, B-, C- und D-Muster sind heute nur noch in wenigen Firmenstandards (zum Beispiel Daimler) referenziert. In den APQP-Standards der AIAG und des VDAs ist alles auf das Erstmuster referenziert. Die Musterstände für die verschiedenen Kunden orientieren sich meist an den Bedürfnissen der Fahrzeugentwicklung.

Phasen der Spirale:

Prototypen Spezifikation

Dies ist natürlich nur der Traum eines jeden Prozessentwicklers, dass tatsächlich am Anfang der Produktentwicklung die Spezifikation steht. Die Realität ist, es gibt eine Realisierungsidee, die für eine Serienentwicklung aufgebaut werden soll. Besonders bei der klassischen Mechanik gibt es oftmals bereits Versuchsmuster, die nun um wesentliche Funktionen ergänzt oder für neuere Systeme elektrifiziert werden sollen.

Somit wird in der ersten Iteration auch meist nur eine Spezifikation auf hoher Abstraktionsebene spezifiziert. Das A-Muster war in der früheren Automobiltechnik meist ein Passmuster, welches sogar aus Holz sein konnte, da es in erster Linie um die Verbaubarkeit im Auto ging. Heute bei moderneren Systemen ist hier schon die gesamte äußere Schnittstelle gemeint sein, so dass man bereits die CAN-Kommunikation bei der ersten Musterlieferung auf das Zielfahrzeug anpassen muss.

Prototypenbau

Da die Muster auch wirklich zum Kunden geliefert werden, müssen diese natürlich auch gebaut werden. Hier wird natürlich in der ersten Iteration viel Handarbeit notwendig sein, in den weiteren Iterationen wird die Automatisierung kontinuierlich erhöht. Das D-Muster, meist mit dem Erstmuster vergleichbar, muss dann auf der Serienproduktionsanlage gebaut werden.

Experimentieren Test / Akzeptanz

Danach wird das Muster gemäß den gegebenen Anforderungen getestet. Zuerst unter Laborbedingungen, dann aber beim Kunden oft bereits in der Fahrzeugumgebung, um hier das dynamische Verhalten sowie das Zusammenspiel mit den anderen Komponenten zu erfahren.

Die Hoffnung beruht für alle Parteien natürlich darauf, dass man mit dem ersten Schuss bereits alle Anforderungen kennt und das entsprechende Muster mit einem positiven Prüfergebnis zurückkommt. In der Realität sieht man, dass der Prototypentest ein wesentlicher Input für die Anforderungsanalyse ist. Dies wurde auch als eine Methode neben der Simulation in die ISO 26262 übernommen.

Änderung oder Ergänzungen

Hier wird nun die Spezifikation geändert und die geänderte Spezifikation leitet einen neuen Entwicklungszyklus ein.

Toyota hat hier mit DRBFM (Design Review Based on Failure Mode) bereits recht früh eine gute Methodik entwickelt, die eine neue Iteration einleitet. Ob eine Spezifikation vollständig oder doch noch fehlerbehaftet ist, lässt sich nicht gut prüfen (frei nach Popper; verifizieren ist so lange positiv, bis ich einen Gegenbeweis finde). Ein Änderungsmanagement basierend auf der Spezifikation kann nur effektiv sein, wenn man weiß, dass die Spezifikation korrekt ist und eindeutig auch für das Produkt gilt. Pessimisten sagen, es geht gar nicht. Daher hat DRBFM hier den Vergleich auf Basis von Eigenschaften beschrieben. In einem multidisziplinären Team werden die Eigenschaften und die funktionellen Abhängigkeiten (Architektur) verglichen. Der positive wie auch negative Einfluss auf das Produkt wird in einem Designreview analysiert und bewertet bevor die Änderungsvorschläge für das Produkt übernommen werden. Diese Methode kann sehr gut für moderne Architektur-Entwicklungen abgeleitet werden. Das Ergebnis der DRBFM fließt erst nach der Einflussanalyse in die Spezifikation ein und wird als Änderung für das Produkt akzeptiert.

Diese Aspekte sind ebenfalls in den Change-Management-Prozess und die Anforderungen aus der ISO 26262 eingeflossen.

2.5 Management der Funktionalen Sicherheit im Automobil- und Sicherheitslebenszyklus

Die IEC 61508 war wohl die erste Norm, die einen Sicherheitslebenszyklus beschrieb. Die weitgehend parallel entwickelte ISO/IEC 12207 beschrieb einen Software-Lebenszyklus. Mitte der 90er Jahre hat man wohl erkannt, dass sich Anforderungen an ein Produkt über den gesamten Gebrauchszeitraum auf das Design des Produktes auswirken können. Leider hat man in all den Phasen schon die Erfahrung gemacht, dass bestimmte Fehler dazu führten, dass Menschen beim Umgang mit den Produkten gefährdet werden können. Wie wir in der ISO/IEC 12207 sehen, ergibt sich auch der Bedarf, bestimmte Fehlerbilder des Produktes über alle Phasen des Produktlebenszyklus zu betrachten. Diese stellen weitere Anforderungen an das Design eines Produktes. Auch die APQP-Standards haben die frühen Entwicklungsphasen der Entwicklung betrachtet. Die Begriffe der System-FMEA sowie später Entwurfs- oder Konzept-FMEA sind in die Standards eingeflossen. Produktwartung und Ersatzteilmanagement wurden bereits wesentlich früher von den APQP- Standards betrachtet. Auch die Idee der Dokumentenarchivierung über den Lieferzeitraum wurde bereits früh in den Standards adressiert. Der Bedarf entstand aus der Produkthaftung.

In der IEC 61508 diente der Lebenszyklus dazu, von der Produktidee bis hin zum Ende des Produktlebens, Phasen zu definieren, in denen die einzelnen Sicherheitsaktivitäten eingebettet werden konnten. Mit diesem Lebenszyklus stellte man bereits eine Basis, um auch tatsächlich Anforderungen an ein Produkt in einem gewissen Bezug vollständig beschreiben zu können.

Die Sicherheitsbetrachtung bei einer Produktidee ist bereits von immenser Wichtigkeit. Es spielen hier nicht nur sicherheitstechnische Aspekte eine Rolle, sondern im Wesentlichen wirtschaftliche. Die Geschichte hat uns gelehrt, dass man auch mit einer schlechten Idee Erfolg haben kann. Leider sind oft schlechte Ideen nur wegen der Angst des Versagens weiter verfolgt worden, und die potentiellen Gefährdungen sind erst aufgetreten, als es keine Möglichkeit der Abwendung dieser Schäden mehr gab. Für Unternehmen kann das Einstellen einer Entwicklung oft einen größeren Schaden bedeuten, als die Kompensation der Schäden, die das Produkt später bei der Nutzung verursachen kann.

Hier betrachten wir bereits einen wesentlichen Aspekt der Produkthaftung, den wohl der Gesetzgeber bereits im 19. Jahrhundert gesehen hat. Er hat uns im §823 aufgefordert, Gefährdungen durch Produkte, soweit es Wissenschaft und Technik

erlauben, zu vermeiden. Sollte es zu einer Schädigung kommen, so ist der Vertreiber („Inverkehrbringer") des Produktes schadensersatzpflichtig.

Um hier nicht zu weit in die Rechtsprechung abzudriften, zurück zum Produktlebenszyklus beziehungsweise zum Sicherheitslebenszyklus. Eine Funktion kann bereits, wenn sie wie beabsichtigt funktioniert, zu einer Gefährdung führen. Dies wird heute im deutschen Sprachraum allgemein als Gebrauchssicherheit bezeichnet. Wie im Kapitel 3.1 (Sicherheit, Risiko etc.) beschrieben, ist dieser Aspekt nicht in der ISO 26262 adressiert. Jedoch hofft man gerne, dass man im Laufe der Produktentwicklung doch noch etwas findet, welches dieses Risiko zu beherrschen hilft oder man wird die Funktion soweit einschränken, dass kein Risiko besteht. Da muss man hoffen, dass die ISO 26262 hier eine Hilfestellung leisten kann. Die ISO 26262 kann nur die Gefährdung, die auf Basis von Fehlfunktionen des Produktes entsteht, beherrschen helfen. Gute Ingenieure werden auch bei gefahrbringenden Funktionen einen Sicherheitsmechanismus für die ein oder andere Anwendung finden, aber wenn dieser nicht gefunden wird, bedeutet das, das Produkt hat keine Chance auf dem Markt zur Etablierung. Versuche bei komplexen Produkten, die in hohen Stückzahlen produziert werden, solche Fehler als hinreichend unwahrscheinlich zu deklarieren, kann eine Herausforderung werden. Formal handelt es sich um systematische Fehler, diese gemäß ISO 26262 zu quantifizieren ist in der Norm nicht vorgesehen. Die Eigenschaften solcher komplexen Produkte, ihre möglichen Fehler, so wie die mögliche Varianz ihrer Verwendung kann nur sehr schwer beurteilt werden. Das Produkt mag zwar noch auf den Markt kommen können, wenn es aber die erste Gefährdung gibt, dann kann man das Produkt nur noch vom Markt nehmen. Dies führte in der Vergangenheit sogar schon dazu, dass Fahrzeuge vom Hersteller zurückgekauft werden mussten.

Daher ist es bereits einer der ersten Schritte, um überhaupt in den Anwendungsbereich der ISO 26262 einzutreten, die Gebrauchssicherheit des Produkts nachzuweisen. Um späteren Produkthaftungsaspekten zuvorzukommen, ist es sinnvoll, dies auch hinreichend zu dokumentieren, sodass durch bestimmte Veränderungen während der weiteren Entwicklung nicht doch die Gebrauchssicherheit wieder in Frage gestellt werden kann. Es entspricht weitgehend dem Wesen eines Ingenieurs, seine Idee nicht beim ersten Fehlschlag zu verwerfen, sondern durch geeignete Modifikationen doch zum Ziel führen zu können.

Um auch kurz einen Blick auf das Ende des Produktlebenszyklus zu haben, einige Aspekte zum Produktlebenszyklus selbst. Unter dem Gesichtspunkt der Gefährdung ist die öffentliche Diskussion zu den Mobiltelefonen ein gutes Stichwort. Klar wird durch die schnellen und kurzen Lebenszyklen von Elektronik jede Menge hochwertiger Elektroschrott produziert. Dies wäre durch die Sicherheitsbrille betrachtet nicht weiter kritisch, wenn nicht bereits die Komponenten selber nicht nur teure, sondern

auch teilweise umweltunverträgliche Stoffe beinhalten würden. Hier ist in erster Linie Blei zu nennen. So gibt uns der Gesetzgeber bereits klare Regeln, wie wir hier zu verfahren haben. Nun mag es an den Haaren herbeigezogen sein, zu sagen, dass giftiges Elektrolyt in Kondensatoren auch irgendwann zu einer Gefährdung führen kann. Auch mag es weithergeholt sein, zu sagen, dass ein Platzen eines Elektrolytkondensators eine Fehlfunktion eines E/E-Teils ist. Aber hier diskutieren wir nur darüber, ob die ISO 26262 uns noch helfen kann. Fakt ist, es gibt hier auch Potentiale für Gefährdungen, die man bei der Herstellung und der Entwicklung eines Produktes beachten sollte, wenn man nicht in Konflikt mit der Produkthaftung kommen möchte. Ein prägnanteres Beispiel für das Ende eines Teilproduktes sollte hier jedoch auch noch betrachtet werden. Meist ist es ja so, dass wir ein Auto nicht nur während der Garantiezeit fahren. Autos, die heute älter als 25 Jahre sind, werden ja wieder als Oldtimer beliebter als das Fahrzeug mit den neuesten Errungenschaften der Technik. Zum Glück gab es vor 25 Jahren noch nicht so viel Elektronik im Fahrzeug, dies wird sich aber nun von Jahr zu Jahr ändern.

Es muss auch auf die Wartung des Fahrzeugs, insbesondere die Komponenten und Systeme, welche zum Beispiel einem Verschleiß unterworfen sind, geachtet werden. Opel hat ja mal mit einer lebenslangen Garantie, sprich 15 Jahren und 160.000 Kilometern, geworben. Aber dies hat man doch schnell wieder aufgegeben. Wir haben gelernt, dass die NASA über Ebay 8086er Rechner gekauft hat, um Alt-Systeme warten zu können. Jeder kann sich vorstellen, wie aufwendig es ist, Programmteile die in FORTRAN geschrieben wurden, heute noch modifizieren oder warten zu können. Dies ist am Beispiel WINDOWS und den Fortschritten unserer Computer praktisch nicht darstellbar. Wir werden später sehen, dass eine Prognose für elektrische Bauelemente über ihr Ausfallverhalten über mehr als 10 Jahre sehr schwierig ist. Im Bereich der Nutzfahrzeuge wird oft schon von einer Lebensdauer von 20 Jahren gesprochen. Bei einem 8086 hat man zwar schon intermittierende Fehler wahrgenommen, aber dass man tatsächlich schon Maßnahmen systematisch bei der Integration vorgenommen hat, kann wohl bezweifelt werden. Die Wartbarkeit auch unter Sicherheitsaspekten tatsächlich sicherzustellen, wird noch eine Herausforderung für die Automobilindustrie darstellen.

2.5.1 Sicherheitslebenszyklus für die Automobilentwicklung

In der ISO 26262 ist der Sicherheitslebenszyklus im Teil 2 Kapitel 5 „Overall Safety Management“ beschrieben. Der Sicherheitslebenszyklus, der Produktlebenszyklus und das „Management der Funktionalen Sicherheit“ soll hier in Beziehung gesetzt werden. Das Ziel des Managements der Funktionalen Sicherheit gemäß ISO 26262

ist die Verantwortlichkeit, der handelnden Personen, Abteilungen und Organisationen, die für die einzelnen Phasen des Sicherheitslebenszyklus verantwortlich sind, zu definieren. Dies gilt für die Aktivitäten, die notwendig sind, die Funktionale Sicherheit für die Produkte, das Fahrzeugsystem oder wie die Norm sagt, das ITEM, das man als Betrachtungseinheit (Fahrzeugsystem) übersetzen könnte, sowie die Maßnahmen, die notwendig sind, um zu bestätigen, dass die Produkte gemäß der ISO 262626 entwickelt worden sind.

Weiter müssen die Aktivitäten beschrieben werden, die über den Sicherheitslebenszyklus hinaus notwendig sind, um überhaupt eine entsprechende Infrastruktur vorweisen zu können, damit der Produktlebenszyklus angewendet werden kann.

Hierzu gehört als Basis ein gelebtes und angewendetes Qualitätsmanagementsystem, weiter wird eine Sicherheitskultur gefordert, die gewährleisten soll, dass vom einzelnen Mitarbeiter bis hin zum obersten Management die Sicherheit mit der notwendigen Sorgfalt und Respekt betrachtet und die notwendigen Maßnahmen angemessen angewendet oder umgesetzt werden können.

Aber auch Themen wie „Lessons Learned“, sprich systematisch aus Fehlern lernen, ein Kompetenzmanagement, kontinuierliche Verbesserung sowie Qualifikations- und Trainingsprogramme werden hier als Voraussetzung gesehen, den Sicherheitslebenszyklus anwenden zu können.

Grundsätzlich geht man in der ISO 26262 davon aus, dass Produkte in einer Projektstruktur entwickelt werden.

Hier wird die Möglichkeit gegeben, dass Bereiche oder Organisationen, die Produkte bereits nach einer generellen Interpretation oder Umsetzung des Produktlebenszyklus („Project independent tailoring of the safety-lifecycle“) entwickeln. Das heißt man entwickelt eine Prozesslandschaft, die eine gültige Ableitung der ISO 26262 darstellt, aber auch auf die Infrastruktur und Produktaspekte optimiert werden kann. Alternativ dazu kann jede Produktentwicklung direkt aus dem Rahmen der ISO 26262 zum Beispiel als Projektsicherheitspläne abgeleitet werden.

Besonders in der Produktentwicklung und der Produktion kann es vorteilhaft sein, viele Aktivitäten kunden- und / oder produktneutral zu definieren. Dies hat Vorteile in der Maschinenauslastung, aber auch im Bereich der Produktentwicklung. Die internen Prozesse können auf entsprechend qualifizierte Entwicklungswerkzeuge abgestimmt werden, Varianten für verschiedene Kunden können mit geringem Änderungsaufwand angeboten werden. Auch hat die Wiederverwendung von bewährten Abläufen, Sicherheitskonzepten sowie von bewährten Produkten einen positiven Aspekt auf die Sicherheit der Produkte.

2.5.2 Sicherheitslebenszyklus gemäß ISO 26262

Der Sicherheitslebenszyklus der ISO 26262 fasst die wichtigsten Sicherheitsaktivitäten in der Konzeptphase, der Serienentwicklung und nach Serienfreigabe zusammen. Die Planung, die Koordination und der Nachweis dieser Aktivitäten über alle Phasen des Lebenszyklus ist zentrale Managementaufgabe. Die Aktivitäten der Konzeptphase, der Serienentwicklung und nach SOP werden in den Bänden 3, 4 und 7 in dieser Norm ausführlich beschrieben.

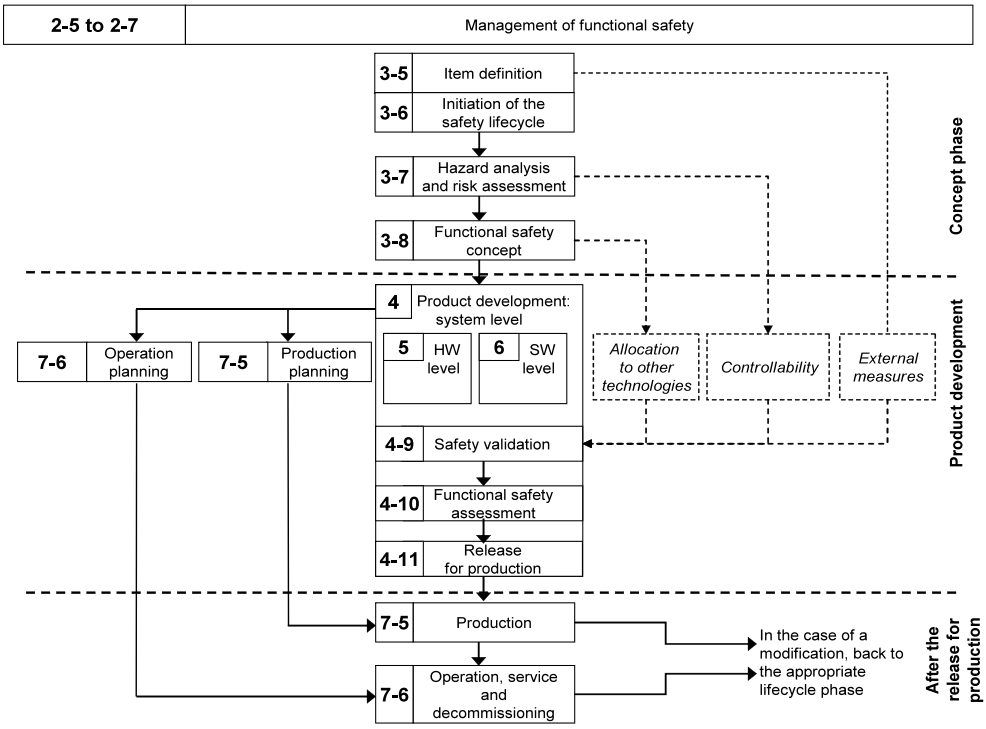

Bild 2.10 Sicherheitslebenszyklus gemäß ISO 26262 (Quelle: ISO 26262, Teil 2)

Der hier abgebildete Sicherheitslebenszyklus der ISO 26262 verweist in seinen Elementen direkt auf die entsprechenden Kapitel der ISO 26262. Das Management der Funktionalen Sicherheit gemäß Teil 2 der Norm umfasst alle weiteren Aktivitäten von Teil 3 (Definition des Entwicklungsgegenstands, dem Fahrzeugsystem) bis zum Teil 7 Kapitel 6 (Betrieb, Service (Wartung) und Außerbetriebnahme (Entsorgung)).

Der Sicherheitslebenszyklus ist in 3 Phasen unterteilt:

- Konzept
- Produktentwicklung
- Nach Produktionsfreigabe

Hierbei ist zu beachten, dass das technische Sicherheitskonzept der Produktentwicklung zugeordnet ist. Neben den 3 Teilen zur Produktentwicklung von Systemen, EE-Hardware und Software, sind die beiden Kapitel Produktions- und Betriebsplanung (Teil 7) dargestellt. Dies sind Aktivitäten die neben den Entwicklungs-V-Zyklen gesehen werden. Weiter werden Aktivitäten dargestellt, die von der Norm nicht direkt adressiert werden, aber für eine Produktentwicklung oft notwendig sind.

Externe Maßnahmen

Darunter sind Maßnahmen zu verstehen, die nicht von der in der Systemdefinition beschriebenen Betrachtungseinheit beeinflusst werden können. Externe Risikoreduktion beinhaltet z. B. Verhalten der Verkehrsteilnehmer oder Eigenschaften der Straße. Sie wird in der Systemdefinition beschrieben. In der Gefahrenanalyse und Risikoanalyse kann von externer Risikoreduktion profitiert werden. Der Nachweis der Wirksamkeit der externen Risikoreduktion ist nicht Umfang dieser Norm.

Beherrschbarkeit (Controllability)

Die in der Gefahrenanalyse und Risikoanalyse zugrunde gelegte Beherrschbarkeit soll während der Serienentwicklung nachgewiesen werden. Geht es hier nicht um eindeutige Beherrschbarkeit der gefährdeten Personen, so wird dies in Teil 3 der ISO 26262 näher betrachtet. Hier überschneiden sich auch wieder Inhalte der Gebrauchssicherheit, da die Frage ob die Funktion so definiert ist, dass sie beim korrekten funktionieren nicht gefährlich werden kann, auch relevant sein kann.

Zuordnung zu Maßnahmen andere Technologien

Darunter sind Technologien zu verstehen, die nicht unter den Betrachtungsumfang dieser Norm fallen, z. B. Mechanik und Hydraulik. Diese werden bei der Zuordnung der Sicherheitsfunktionen herangezogen. Auch der Nachweis der Effizienz, Effektivität oder überhaupt die Anwendbarkeit dieser Maßnahmen ist nicht Umfang dieser Norm.

Im Rahmen des Managements der Funktionalen Sicherheit fordert die Norm zum Sicherheitslebenszyklus weitergehend folgende Aktivitäten:

- Zum E/E-System sind ausreichende Informationen zu jeder Phase des Sicherheitslebenszyklus zu dokumentieren, die für die wirkungsvolle Erfüllung nachfolgender Phasen und Verifikationstätigkeiten notwendig sind.
- Die Aufgaben des Managements der funktionalen Sicherheit sind die Durchführung und Dokumentation der Phasen und Aktivitäten über den gesamten Lebenszyklus sicherzustellen und eine für die funktionale Sicherheit förderliche Unternehmenskultur bereitzustellen.

Aus Sicht der Funktionalen Sicherheit steht nicht die Erfüllung der Anforderungen, die sich aus irgendwelchen Prozessmodellen ableiten. Der Sicherheitslebenszyklus muss korrekt und hinreichend abgeleitet werden. Wichtig für die Projektplanung und die zu planenden Sicherheitsaktivitäten ist, dass die Sicherheitskonzepte so umgesetzt werden, dass die Sicherheitsziele hinreichend abgesichert werden.