Sicherheitsgerechte Entwicklungsprozesse – alles neu geregelt?

Dr.-Ing. Klaus-Jürgen Amsler, Dr.-Ing. Joachim Fetzer, Dr.-Ing. Dieter Lederer,
RA Dr. Meinhard Erben
Vector Consulting GmbH, Stuttgart

Einleitung

Mit der Zunahme softwarebasierter Funktionen im Kraftfahrzeug verbindet sich auch eine Zunahme von Softwarefehlern in Steuergeräten, die zu Ausfällen der Automobilelektronik führen. Bereits heute liegt der Anteil der Pannen, die durch Elektronikfehler verursacht werrden, bei ca. 50%. Es wird ein Anstieg auf ca. 63% im Jahr 2013 prognostiziert [1]. Die Ursache für Elektronikausfälle sind zum überwiegenden Teil Softwarefehler [1]. Unter diesen Randbedingungen bedeutet der vermehrte Einzug von Software auch in sicherheitskritische Bereiche [2], dass die Anwendung von Sicherheitsnormen wie z.B. der IEC 61508 [3] bei der Produktentwicklung eine immer größere Bedeutung u.a. für die Gewährleistung der Produktsicherheit erhält. Denn die Konsequenzen im Schadensfall können gravierend sein:

- Personen- und Sachschäden nebst Folgeschäden sowie punitive damages in den USA, und/oder
- weltweite Rückrufaktionen.

Die Folge für die betroffenen Automobilhersteller oder –zulieferer ist zumindest ein großer Imageschaden. Im Extremfall kann ein mittelständisches Unternehmen von der Insolvenz bedroht sein.
Diese Problematik hat sich seit dem TREAD Act (Transportation Recall Enhancement Accountability and Documentation Act) noch weiter verschärft. Im Jahr 2000 war eine weltweite Rückrufaktion von Bridgestone der Auslöser für die Einführung des TREAD Act durch die NHTSA (National Highway Traffic Safety Administration). Unfälle mit über 700 Verletzten und weltweit 203 Toten wurden auf schadhafte Reifen von Bridgestone zurückgeführt. Daraufhin rief Bridgestone 14,4 Mio. Reifen zurück. Für das Unternehmen bedeutete dies Kosten in Höhe von 1,3 Mrd. USD. Eine zweite Rückrufaktion 2001 von 13 Mio. Reifen verursachte weitere Kosten von 2,1 Mrd. USD [4].

Nicht nur die Unternehmen sind vom TREAD Act betroffen, sondern auch die verantwortlichen Mitarbeiter werden in die Haftung genommen. Bei Verstoß gegen die Berichtspflichten an die NHTSA nach dem TREAD Act drohen drastische Bußen durch die NHTSA:

- Bis zu 15 Mio. USD für das Unternehmen sowie
- bis zu 500.000 USD oder Gefängnis bis zu 15 Jahren für verantwortliche Mitarbeiter.
- Einfuhrverbot für Produkte in die USA.

Das Thema Produktsicherheit ist also auch vor diesem Hintergrund äußerst brisant, und zwar auch in juristischer Sicht, auch wenn viele Beteiligte das in Europa bisher nicht oder nur kaum wahrgenommen haben bzw. nicht wahrhaben möchten.
Damit stellt sich die Frage nach den Möglichkeiten, Produktsicherheit zu gewährleisten. Gibt es Konsequenzen für den Entwicklungsprozess? Muss alles neu geregelt werden – oder kann man auf Bewährtem aufbauen?

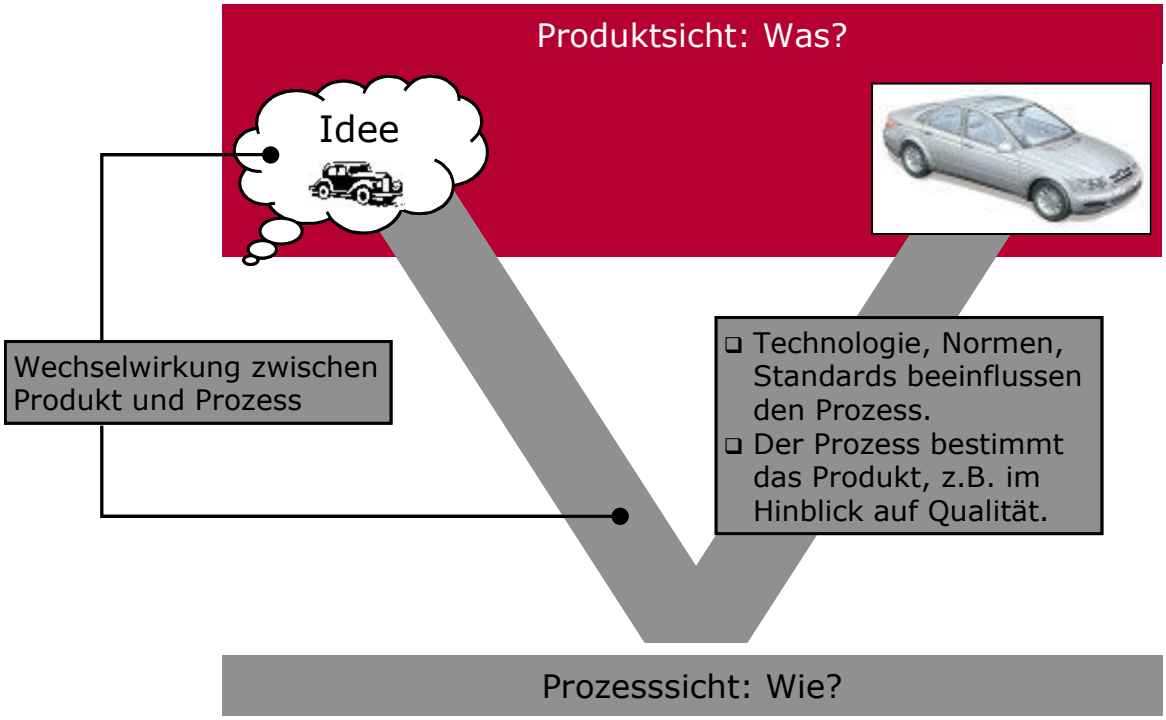

Bild 1: Wechselwirkung von Produkt und Prozess.

In diesem Beitrag wird erläutert, was unter einem ‚sicherheitsgerechten' Entwicklungsprozess zu verstehen ist. Grundvoraussetzungen, die für die Implementierung eines solchen Prozesses erfüllt sein müssen, werden sowohl aus juristischer als auch aus technischer Sicht beschrieben. Zuletzt wird das Vorgehen skizziert, wie ein solcher Prozess zu implementieren ist. Dabei handelt es sich um einen Ansatz, der, ausgehend von einem bestehenden Prozessumfeld, schrittweise zu einem sicherheitsgerechten *und* effizienten Entwicklungsprozess führt.

1 Die Wechselwirkung von Produkt und Prozess

1.1 Automotive-Systems-Engineering – die Verbindung von Produkt- und Prozesssicht

Die Entwicklung eines Produktes kann nie losgelöst vom angewendeten Entwicklungsprozess gesehen werden.

Die funktionalen und nichtfunktionalen Anforderungen an das Produkt bestimmen den anzuwendenden Entwicklungsprozess (Bild 1). Dies wird deutlich, wenn man die Wandlung der Unternehmen in der Automobilindustrie von rein mechanisch orientierten hin zu mechatronisch bzw. softwareorientierten Unternehmen in den letzten zwei Jahrzehnten betrachtet. Umgekehrt bestimmt der Entwicklungsprozess das Produkt z.B. im Hinblick auf Qualität, Funktionalität oder Kosten.

Automotive-Systems-Engineering [5] adressiert genau diesen Umstand der wechselseitigen Abhängigkeit zwischen Produkt und Prozess und integriert die Produkt- und Prozesssicht in einem fraktalen Ansatz. Selbstähnlichkeiten finden sich auf allen Systemebenen des Produkts und analog dazu auf allen Ebenen des Entwicklungsprozesses (Bild 2).

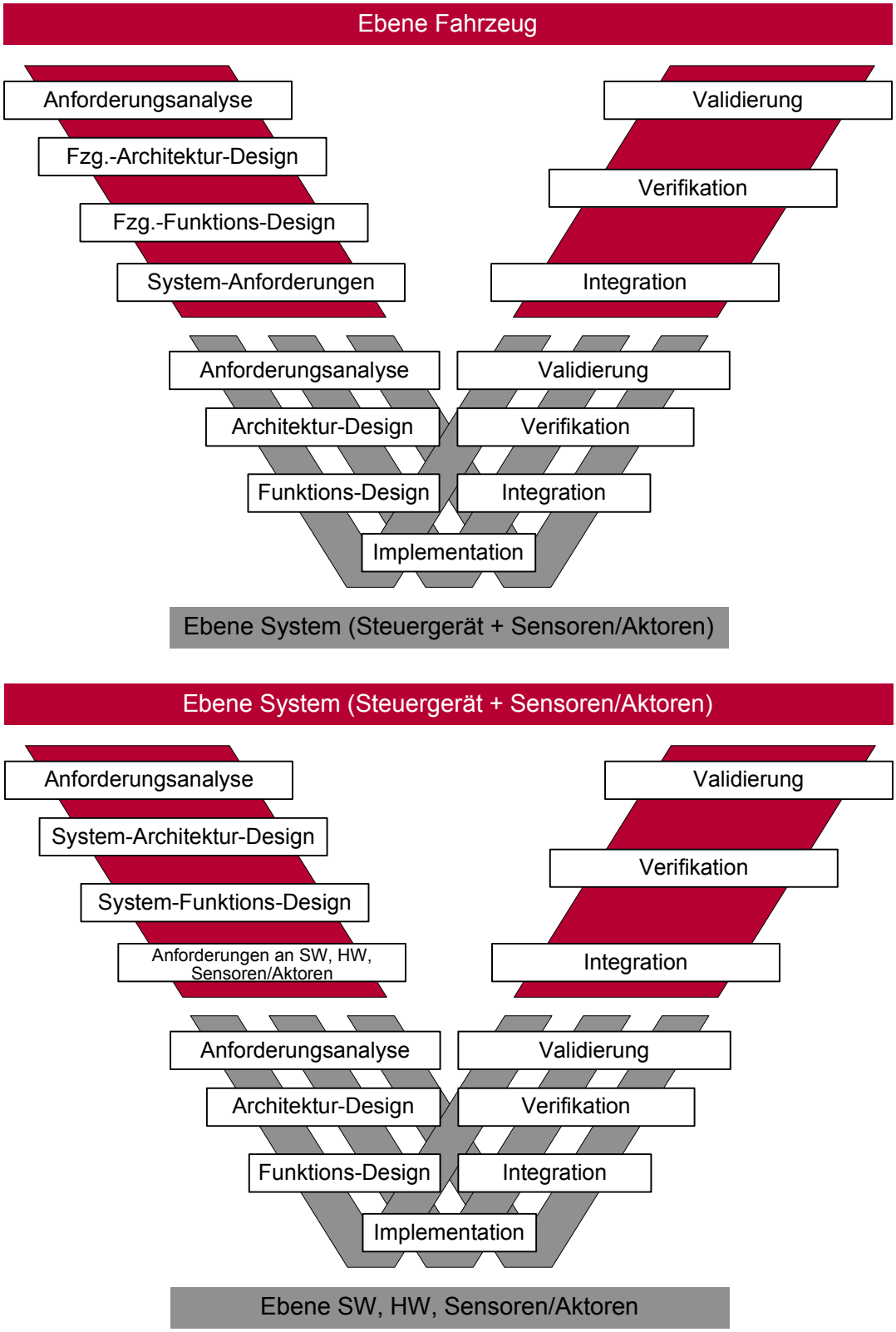

Bild 2: Entwicklungsprozess im V-Modell auf den verschiedenen Systemebenen des Produkts und der Produktentwicklung.

Das bedeutet für einen sicherheitsgerechten Entwicklungsprozess, dass auf jeder Systemebene Produkte entstehen, die dem Anspruch an die Produktsicherheit genügen müssen, d.h. fehlerfrei sein müssen. Dabei stellt sich die Frage, insbesondere aus juristischer Sicht, was überhaupt als Fehler anzusehen ist.

1.2 Fehlerarten

Der Jurist unterscheidet zwischen drei Fehlerarten, dem Herstellungsfehler, dem Instruktionsfehler und dem Überwachungsfehler.

- Herstellungsfehler, dieser gliedert sich in zwei Unterpunkte:
  - Ein Konstruktionsfehler ist ein Fehler, der jedem Produkt einer Serie anhaftet, weil bei der Konstruktion des Produkts nicht die erforderliche Sorgfalt aufgewendet worden ist. Softwarefehler sind Konstruktionsfehler, d.h. sie treten unter den gleichen Bedingungen immer auf.
  - Fabrikationsfehler gibt es nur bei einzelnen Produktexemplaren einer Serie. Sie entstehen, weil in der Produktion nicht mit ausreichender Präzision und Sorgfalt gearbeitet und der Fehler bei der Qualitätskontrolle nicht entdeckt wurde („Montagsautos“).

    Diese Fehlerart ist besonders problematisch, weil durch sie Rückrufaktionen ausgelöst werden können, bei denen im Extremfall alle Autos zurückgerufen werden müssen.
- Instruktionsfehler: Das Produkt selbst ist fehlerfrei, aber die Gebrauchsanweisung ist mangelhaft, oder der Hersteller warnt den Benutzer nicht hinreichend vor Gefahren bei der Anwendung des Produkts. Gewarnt werden muss auch vor nicht gänzlich fernliegenden Fehlanwendungen.
- Überwachungsfehler: Der Hersteller hat eine Produktbeobachtungspflicht bis hin zu Warn- oder Rückrufpflichten.

Damit zeigt sich die Wechselwirkung von Produkt und Prozess auch bei der Betrachtung der Fehlerarten. Nur ein fehlerfreier Herstellungsprozess, der Konstruktion und Fabrikation umfasst, bietet die Gewähr dafür, dass das Ergebnis des Herstellungsprozesses, also das fertige Produkt, selbst fehlerfrei ist. Im Folgenden wird der Frage nachgegangen, unter welchen Voraussetzungen der Hersteller für Fehler haftet.

2 Haftung des Herstellers

Der Hersteller kann aufgrund vertraglicher oder gesetzlicher Haftung in Anspruch genommen werden.

2.1 Vertragliche Haftung

Die vertragliche Haftung knüpft an das wirtschaftliche Nutzungs- und Äquivalenzinteresse des Erwerbers an. Ein Produkt ist fehlerhaft im Sinne vertraglicher Haftung, wenn es in seiner Funktionsfähigkeit nicht dem entspricht, was der Erwerber aufgrund des abgeschlossenen Vertrags berechtigter Weise erwarten darf.

2.2 Gesetzliche Haftung

Die gesetzliche Haftung hat als Schutzzweck das Integritätsinteresse jedes Benutzers und jedes Dritten. Dabei wird zwischen Produkt- und Produzentenhaftung unterschieden:

- Produkthaftung:
  Ein in den Verkehr gebrachtes Produkt muss diejenige Sicherheit für Leben,

Gesundheit und Sachwerte bieten, die die Allgemeinheit berechtigter Weise erwarten darf. D.h. die Produkthaftung knüpft an die Sicherheit des Produkts an.

- Produzentenhaftung:
  Die Produzentenhaftung knüpft daran an, dass das hergestellte Produkt nicht die nach der Verkehrsanschauung erforderliche Beschaffenheit aufweist und deshalb gefährlicher ist als ein gleichartiges Produkt.

In Bezug auf den Herstellungsprozess bestehen Ansprüche aus der Produzentenhaftung, wenn der Hersteller gegen eine ihm bei der Herstellung obliegende Verkehrssicherungspflicht verstößt, also wenn er eine Pflicht im *organisatorischen Bereich* verletzt. Die Produzentenhaftung bezieht sich damit auch auf den Konstruktions- oder Entwicklungsprozess beim Hersteller, während die Produkthaftung sich auf das Ergebnis des Entwicklungsprozesses bezieht, also auf das fertige Produkt.

Für den Entwurf eines sicherheitsgerechten Entwicklungsprozesses werden im Folgenden die Anforderungen aus der Produzentenhaftung näher betrachtet. Welche Organisations- und Sorgfaltspflichten muss der Hersteller beachten?

2.3 Organisations- und Sorgfaltspflichten des Herstellers

Der Hersteller muss seinen Betrieb so einrichten, dass Fehler der genannten Fehlerarten aus Abschnitt 1.2 möglichst ausgeschaltet oder durch Kontrollen entdeckt werden. Dazu gehört nach der Rechtsprechung auch das Prüfen der Produkte von Zulieferern auf Fehlerfreiheit, sofern der Zulieferer aufgrund besonderer fachlicher Erfahrung und Einrichtung diese Prüfung nicht bereits selbst vorgenommen hat. Generell gilt: Je höherwertiger das Rechtsgut (bis hin zu Leib oder Leben), desto höher sind die Anforderungen, die an den Hersteller in Bezug auf den Herstellungsprozess gestellt werden.

Bei der Erstellung Software basierter Systeme gilt zwar die Besonderheit, dass es nahezu unmöglich ist, das System und insbesondere die Software fehlerfrei zu erstellen. Dieser Umstand wirkt sich aber nicht nur zu Gunsten des Herstellers aus, sondern auch in die andere Richtung: Einerseits kann man dem Hersteller kaum bei jedem Fehler Fahrlässigkeit unterstellen, was Voraussetzung für Ansprüche aus Produzentenhaftung ist. Andererseits muss der Hersteller deshalb umso mehr und umso akribischer alle ihm obliegenden Organisations- und Sorgfaltspflichten beachten. Insbesondere muss der Hersteller konstruktive und analytische Qualitätssicherungsmaßnahmen umsetzen, z.B. das Software basierte System intensiv testen, um schwere Schäden für Leib oder Leben möglichst auszuschließen.

Bei der Entwicklung von Embedded Systems für Kraftfahrzeuganwendungen treffen den Hersteller ganz besondere Sorgfaltspflichten, weil es sich um komplexe mechatronische Systeme handelt: Das Projektmanagement umfasst dabei – im Sinne des Simultaneous Engineering – die gleichzeitige und abgestimmte Umsetzung von Mechanik-, Hardware- und Softwareanforderungen in entsprechenden Entwicklungsumgebungen mit konsistenten Design-, Implementierungs-, Test-, Integrations- und Simulationskonzepten. Das stellt besonders hohe Anforderungen an den Entwicklungsprozess und seine Teilprozesse, z.B. an das übergreifende Konfigurationsmanagement.

Wer Dritte Komponenten, wie z.B. Software, erstellen lässt, die er selbst als Teil eines Produkts verwendet, ist nicht nur verpflichtet, den Dritten sorgfältig auszuwählen, sondern er muss diesen auch in besonderem Maße durch konkrete Vereinbarungen zur Einhaltung äußerster Sorgfalt verpflichten, am Besten unter

Hinweis auf existierende Normen wie IEC 61508 und/oder Prozessreifemodelle wie CMMI, SPICE, etc.

Nach der Rechtsprechung muss der Hersteller prinzipiell bei Konstruktion, Fabrikation und Instruktion den aktuellen Stand von Wissenschaft und Technik einhalten, soweit dieser objektiv erkennbar und ermittelbar ist, außerdem alle anerkannten Regeln des Fachs, also technische Normen, DIN-Vorschriften, VDE-Bestimmungen, etc. Die Frage, ob die in IEC 61508 enthaltenen Regeln vom Hersteller einzuhalten sind, ist deshalb aus juristischer Sicht eindeutig zu bejahen.

Im Folgenden wird näher dargestellt, warum die Einhaltung von analytischen und konstruktiven Qualitätssicherungsmaßnahmen aus juristischer Sicht so eminent wichtig ist.

2.4 Beweislastumkehr

Beweisfragen spielen bei Produkt- und Produzentenhaftung eine zentrale Rolle. Entgegen den sonst gültigen Beweislastregeln gelten im Falle der Produzentenhaftung für den Geschädigten Beweislasterleichterungen bis hin zur Beweislastumkehr.

- Der Geschädigte braucht (nur) darzulegen, dass das Produkt objektiv einen Sicherheitsmangel aufwies, d.h. dass der Fehler hätte vermieden werden können. Dabei sind Anscheins- und Indizienbeweise zulässig, ein sog. Vollbeweis ist nicht notwendig.
- Der Hersteller kann und muss dann beweisen, dass er für den Fehler nicht einzustehen hat, weil er die im Verkehr erforderliche Sorgfalt hinsichtlich der Konstruktion und Herstellung des Produkts beachtet hat.

Diese Beweislastumkehrregeln sind plausibel und haben einen hohen Gerechtigkeitsgehalt: Dem Geschädigten ist es kaum bis gar nicht möglich, dem Hersteller eine Pflichtverletzung nachzuweisen, weil viele der zu beweisenden Tatsachen in der Sphäre des Herstellers liegen. Diese Sphäre ist dem Geschädigten als Außenstehendem aber regelmäßig nicht zugänglich.

Der Hersteller wird den Entlastungsbeweis nur führen können, wenn er darstellen und notfalls beweisen kann, dass er bei der Konstruktion und Herstellung des Produkts alle im Verkehr erforderlichen Sorgfaltspflichten beachtet hat und zwar in Bezug auf alle Umstände, die in seinem Betrieb liegen.

2.5 Was ist aus juristischer Sicht zu tun?

Der Hersteller muss die in Abschnitt 2.3 genannten organisatorischen Pflichten erfüllen und er muss die Erfüllung dieser Pflichten später auch nachweisen können. Dies umfasst, dass er ein effektives Vertrags- und Projektmanagement aufsetzt und dieses dann auch anwendet. Dazu gehören als Minimalanforderungen:

- Strukturierte Entwicklungsprozesse (mit Phaseneinteilung),
- Klare, vollständige, eindeutige und verständliche Spezifikationen einschließlich Test- und Abnahmekriterien,
- Anforderungs- und Änderungsmanagement-Verfahren,
- Qualitätssicherungsmaßnahmen.

Das sind aus juristischer Sicht alles altbewährte Grundregeln, d.h. man kann und soll geradezu auf Bewährtem aufbauen.

3 Sicherheitstechnische Anforderungen

Die Anforderungen an den Entwicklungsprozess, auch aus sicherheitstechnischer Perspektive, werden durch den Stand der Technik beschrieben, wie bereits in Abschnitt 2.3 ausgeführt wurde. Was der Stand der Technik beinhaltet, schreibt das internationale und das deutsche Normenwerk vor. Im Bereich der sicherheitstechnischen Anforderungen wurde im Jahr 2002 die internationale Sicherheitsgrundnorm IEC 61508 in das deutsche Normenwerk übernommen und als DIN EN 61508 veröffentlicht. Im VDE-Vorschriftenwerk wurde sie als VDE 0803 klassifiziert.

Bereits bestehende Sicherheitsnormen wie z.B. DIN V VDE 0801 [6], DIN V 19250 [7], DIN V 19251 [8] sollen vom DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE) zum 01.08.2004 zurückgezogen werden. Damit bildet die DIN EN 61508 die Grundlage für den Stand der Technik im Bereich softwarebasierter sicherheitsbezogener Systeme. Welche Konsequenzen ergeben sich nun hieraus für den Entwicklungsprozess?

3.1 Anforderungen aus der IEC 61508

- Die IEC 61508 formuliert zwei Kategorien von Anforderungen: organisatorische und technische.

Die organisatorischen Anforderungen beziehen sich auf Festlegungen zum Entwicklungsprozess (Sicherheitslebenszyklus), zur funktionalen Sicherheit (Management und Beurteilung) und zum Dokumentenmanagement. Neu im Vergleich zu bisherigen Sicherheitsnormen ist die konsequente Prozessorientierung, die sich im definierten Sicherheitslebenszyklus zeigt (Bild 3). Speziell für die Realisierung der Software sicherheitsbezogener Systeme (Punkt 9 in Bild 3) können verschiedene Lebenszyklus-Modelle verwendet werden [9], so z.B. auch das V-Modell (Bild 2).
Technische Anforderungen beziehen sich im Wesentlichen auf die Sicherheitsintegrität der Hardware, d.h. auf die Anforderungen an die Hardwarearchitektur und die Wahrscheinlichkeit zufälliger Hardwareausfälle sowie auf die systematische Sicherheitsintegrität zur Vermeidung und Beherrschung von Ausfällen. Die Sicherheitsintegrität ist auf Software anzuwenden und besteht in der Implementierung empfohlener Verfahren und Techniken in jeder Phase des Software Sicherheitslebenszyklus (siehe V-Modell in Bild 2).

Die organisatorischen und technischen Anforderungen der IEC 61508 lassen sich gemäß dem Ansatz des Automotive-Systems-Engineering [5] den drei Ebenen

- Engineering-Prozess
- Management-Prozess und
- Prozess-Management,

zuordnen (Bild 4).

Speziell zur Ebene Management-Prozess gehören u.a. die Aktivitäten Anforderungsmanagement, Projektmanagement, Konfigurationsmanagement und Qualitätsmanagement. Auf dieser Ebene lassen sich die Anforderungen der IEC 61508 auf die Aktivitäten zum Planen, Steuern und Verfolgen des Engineering abbilden (Bild 5). Die in den Bildern 4 und 5 gezeigten Zuordnungen haben Konsequenzen auf die Anforderungen an einen Entwicklungsprozess hinsichtlich der Konformität zu IEC 61508.

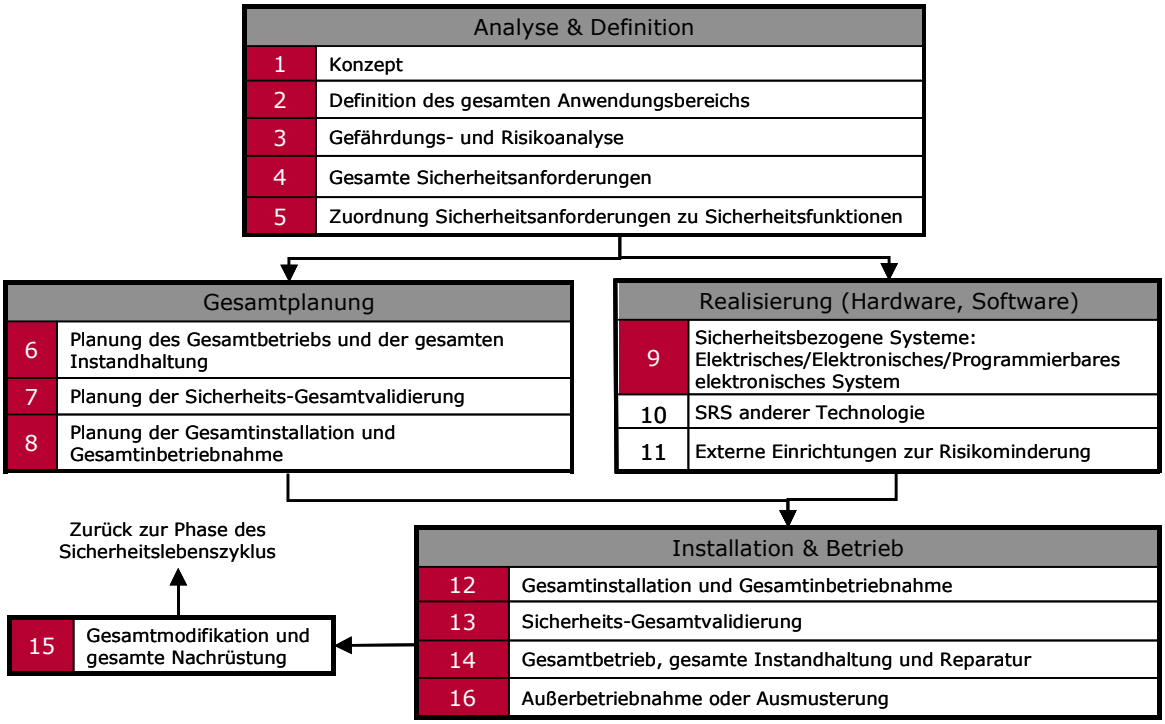

Bild 3: Sicherheitslebenszyklus nach IEC 61508.

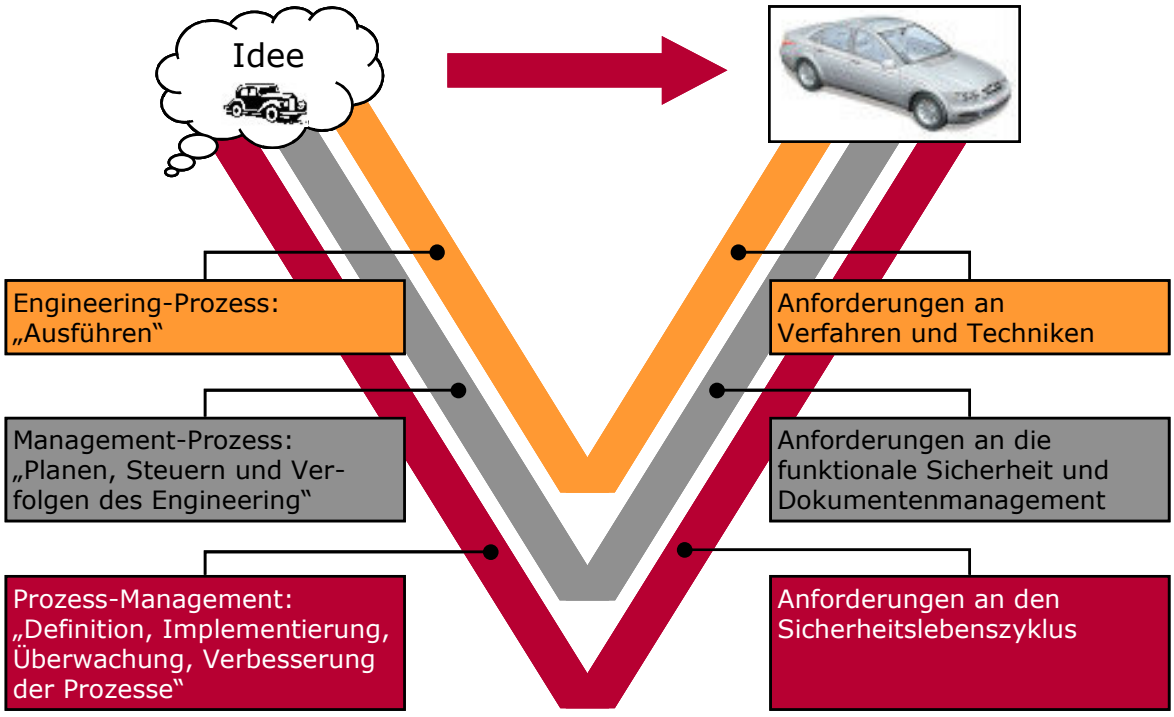

Bild 4:Zuordnung der Anforderungen aus der IEC 61508 zu den Prozessebenen des Automotive-Systems-Engineering.

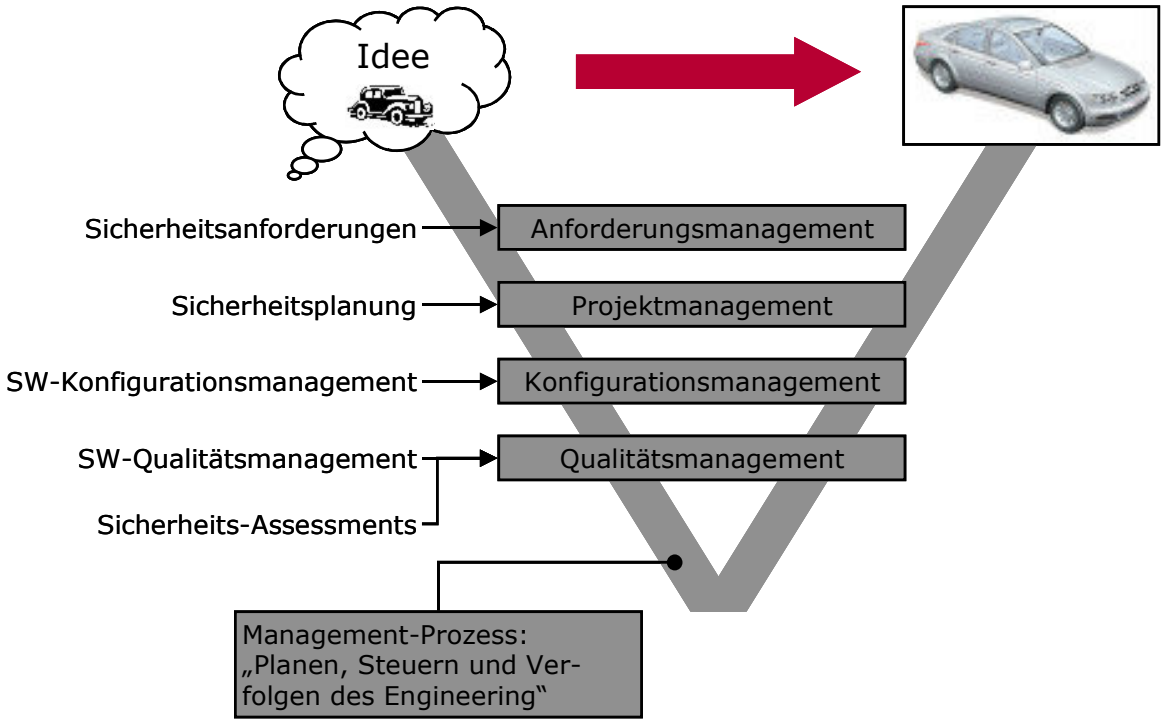

Bild 5: Zuordnung der Anforderungen aus der IEC 61508 zu den Aktivitäten der Ebene Management-Prozess.

3.2 Mindestanforderungen an den Entwicklungsprozess

Um die im Abschnitt 3.1 aufgeführten spezifischen sicherheitsrelevanten Anforderungen an das Prozess-Management erfüllen zu können, muss der Entwicklungsprozess über die folgenden grundlegenden Eigenschaften verfügen:

- Anwendung eines definierten Lifecycle-Modells,
- Anforderungsmanagement zur Sicherstellung einer kontrollierten Basis an Produktanforderungen für das Projektmanagement und die Entwicklung,
- Planung und Verfolgung aller Projektaktivitäten samt den Verantwortlichkeiten für deren Durchführung,
- Konfigurationsmanagement zur Sicherstellung der Produktintegrität während des gesamten Produkt-Lebenszyklus,
- Qualitätssicherung, um zu gewährleisten, dass vorgegebene Prozesse durchgeführt und vorgegebene Produktanforderungen umgesetzt werden.

Die aufgeführten Punkte entsprechen den in Abschnitt 2.5 definierten Minimalanforderungen aus juristischer Sicht und kennzeichnen einen Reifegrad, über den der Entwicklungsprozess mindestens verfügen muss. Unter Einbeziehung von Reifegradmodellen wie CMM [10], CMMI [11] oder SPICE [12] zeigt sich, dass ein Reifegrad der Stufe 2 (Level 2) erforderlich ist, um die genannten Mindestanforderungen erfüllen zu können. Andererseits bedeutet dies: Ein Entwicklungsprozess, der den Reifegrad Level 2 erfüllt, stellt bereits eine gute Grundlage für einen mit IEC 61508 konformen, d.h. sicherheitsgerechten, Entwicklungsprozess dar. Aus dieser Feststellung leitet sich unmittelbar der Weg zum sicherheitsgerechten Entwicklungsprozess ab.

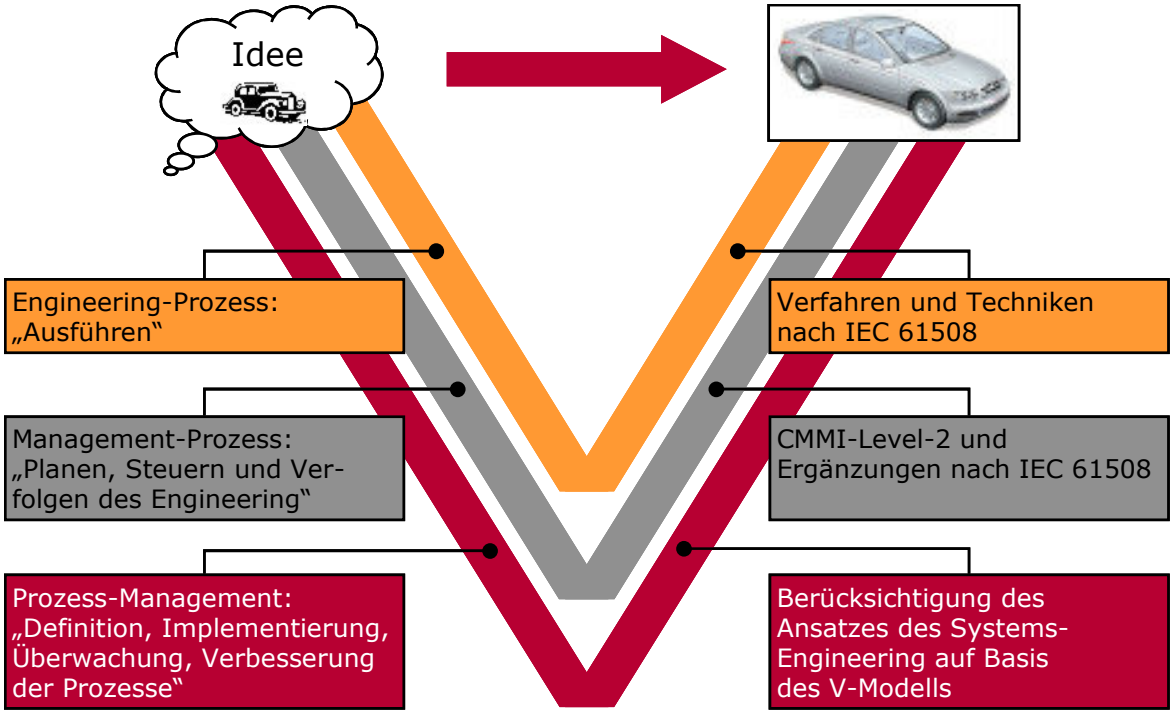

Bild 6: Sicherheitsgerechter Entwicklungsprozess.

3.3 Der sicherheitsgerechte Entwicklungsprozess

Ausgehend von einem gegebenen Prozessumfeld lässt sich die Konformität zur IEC 61508 in drei Schritten erreichen:

1. Ermittlung des Prozessreifegrads, basierend auf einem Reifegradmodell (z.B. CMMI, SPICE).
2. Durchführung von Maßnahmen zur Erlangung des Mindestreifegrades Level 2. Diese Maßnahmen können gleichzeitig zur Steigerung der Effizienz des Entwicklungsprozesses benutzt werden.
3. Berücksichtigung der spezifischen sicherheitsrelevanten Anforderungen nach IEC 61508 als ergänzende Prozessbausteine. Dazu gehören u.a.
   - Durchführung von Gefährdungs- und Risikoanalysen,
   - Analysen zur geforderten Sicherheitsintegrität,
   - Anwendung spezieller Verfahren und Techniken in Abhängigkeit von der geforderten Sicherheitsintegrität,
   - Maßnahmen zur Beurteilung der funktionalen Sicherheit.

Ausgehend vom Ansatz des Automotive-Systems-Engineering nach Bild 4 stellt die Konformität zur IEC 61508 eine Ergänzung dar (Bild 6). Die schrittweise Ausrichtung hin zum sicherheitsgerechten Entwicklungsprozess ist damit eine Maßnahme im Sinne der kontinuierlichen Prozessverbesserung.

4 Zusammenfassung

Die Einhaltung bzw. systematische Anwendung der Reifegradmodelle CMM, CMMI oder SPICE stellt eine wesentliche Grundlage dar, nicht nur die Anforderungen aus der IEC 61508 sondern auch die Mindestanforderungen aus juristischer Sicht zu erfüllen. Ein wirksames Prozess-Management ist erforderlich, um ausgehend von dieser Grundlage einen mit IEC 61508 konformen Entwicklungsprozess sukzessive zu etablieren und sich somit des Themas Produzentenhaftung zu erwehren.

Für den sicherheitsgerechten, zu IEC 61508 konformen Entwicklungsprozess muss wenig neu geregelt werden. Man kann und soll geradezu auf Bewährtem aufbauen.

Literatur

[1] Mercer Management Consulting: Automobil-Elektronik, Problemfelder, Herausforderungen und Lösungsansätze, Vorstudie, Aug. 2003

[2] „European Automotive Market for X-by-wire Technologies“, Frost & Sullivan, 2001

[3] IEC 61508 „Functional safety of electrical/electronic/programmable electronic safety-related systems”, www.iec.ch

[4] Vortrag Tread Act, Fraunhofer-Institut IPA, Jan. 2004, www.ipa.fhg.de

[5] D. Lederer, J. Fetzer, G. Heling, G. Baumann, „Automotive Systems Engineering – The Solution for Comoplex Technical Challenges?“, Proceedings 5. Internationales Stuttgarter Symposium Kraftfahrwesen und Verbrennunsmotoren, Feb. 2003, S. 593–607

[6] DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben

[7] DIN V 19250: Leittechnik – Grundlegende Sicherheitsbetrachtungen für MSR-Schutz einrichtungen

[8] DIN V 19251: Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maß-nahmen zur gesicherten Funktion

[9] ISO/IEC 12207 „Software life cycle processes”, www.iso.ch

[10] M.C. Paulk, Ch.V. Weber, and B. Curtis, “The Capability Maturity Model. Guidelines for Improving the Software Process”, Addison-Wesley, 1995

[11] CMMI: www.sei.cmu.edu

[12] SPICE: www.isospice.com