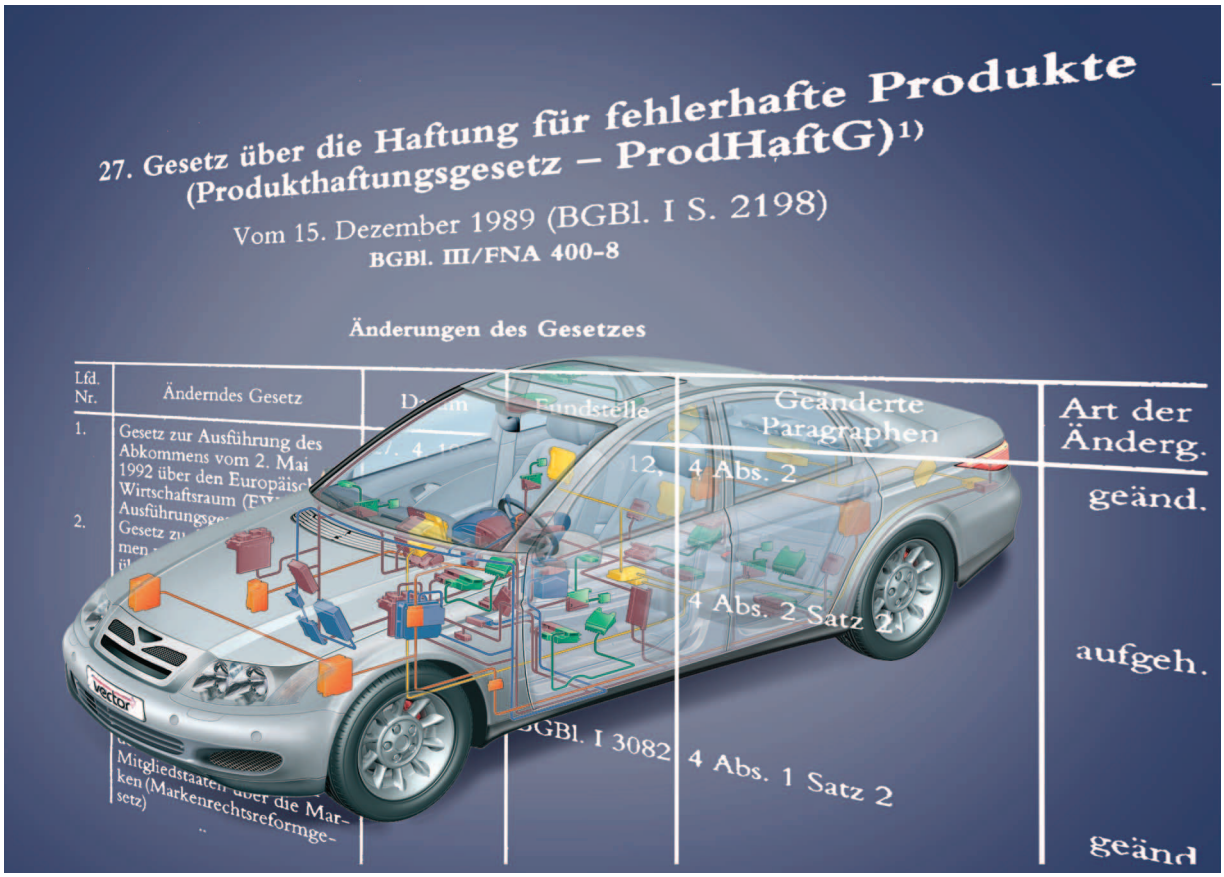
Sonderdruck
aus AEP
Automotive
Engineering Partners
(2004) Heft 5

AUTOMOTIVE ENGINEERING PARTNERS

Sonderdruck der Vector Consulting GmbH

SICHERHEITSGERECHTE ENTWICKLUNGSPROZESSE

SICHERHEITSGERECHTE ENTWICKLUNGSPROZESSE ALLES NEU GEREGELT?



Die Produkt- und Produzentenhaftung wirkt auch bei Elektronik und Software

Mit dem vermehrten Einzug von Software auch in sicherheitskritische Bereiche wie Lenkung und Bremsen gewinnt das Thema Produktsicherheit bei Kraftfahrzeugen zunehmend an Brisanz. Wie lässt sich Produktsicherheit gewährleisten, und welche Konsequenzen hat dies für den Entwicklungsprozess? Muss seit der Gesetzesverschärfung im Juni 2004 alles neu geregelt werden – oder kann auf Bewährtem aufgebaut werden? In diesem Beitrag von Vector Consulting und Kanzlei Erben wird erläutert, was unter einem sicherheitsgerechten Entwicklungsprozess für die Elektronik zu verstehen ist.

Neben kostspieligen Rückrufaktionen bei schadhaften Fahrzeugen, die zudem das Herstellerimage belasten, entstehen für Automobilhersteller, Zulieferer und Dienstleister erhebliche finanzielle Risiken vor allem aus Sicht der Produkt- und Produzentenhaftung. Der folgende Beitrag beschreibt die Implementierung eines sicherheitsgerechten Entwicklungsprozesses speziell für Elektronik angesichts der heutigen juristischen und technischen Rahmenbedingungen. Dieser Ansatz geht von einem bestehenden Prozessumfeld aus, das schrittweise in einen sicherheitsgerechten und effizienten Entwicklungsprozess überführt wird.

JURISTISCHE RAHMENBEDINGUNGEN

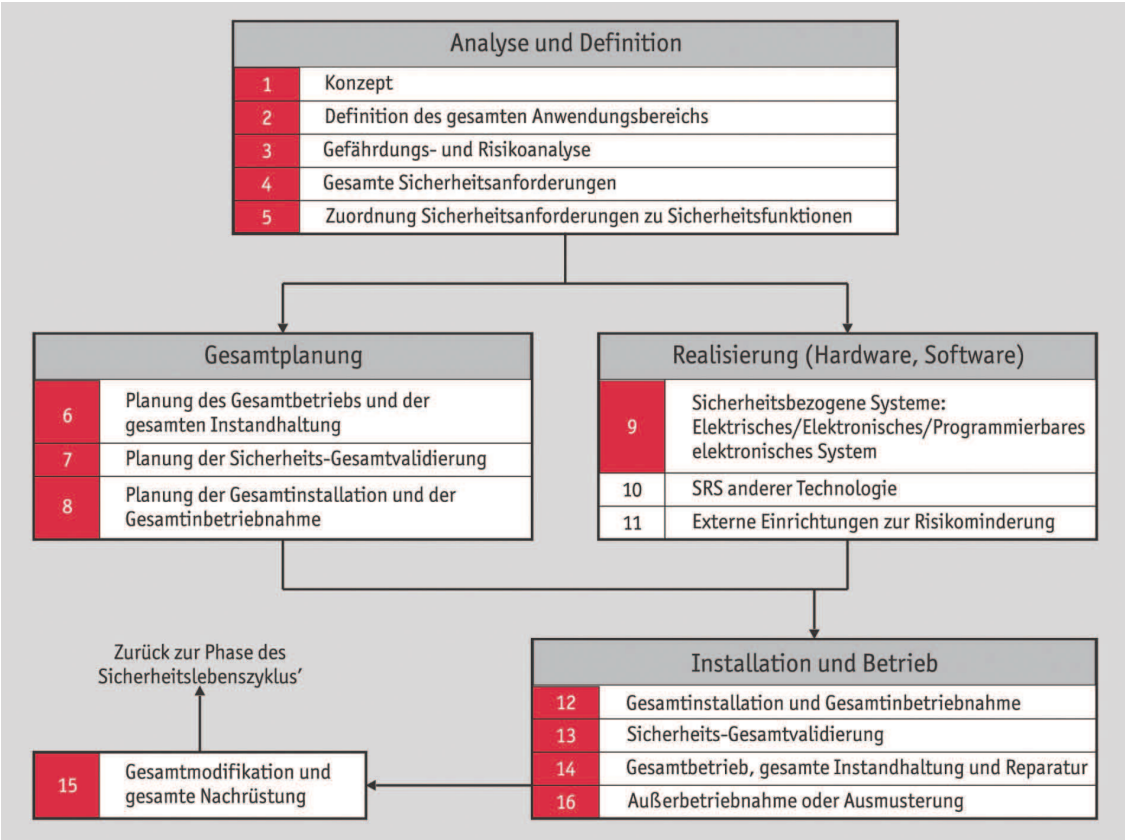
Der US-amerikanische Tread Act [1] nimmt Unternehmen und verantwortliche Mitarbeiter mit erheblichen Sanktionsdrohungen in die Pflicht, über alle Maßnahmen, die durch fehlerhafte Teile verursacht wurden, umfassend und proaktiv zu berichten. Dementsprechende Produktbeobachtungspflichten hat die Europäische Union in die bestehende Produktsicherheitsrichtlinie (2001/95/EG) aufgenommen, die im Juni 2004 in deutsches Recht umgesetzt wurde.

Ein sicherheitsgerechter Entwicklungsprozess zeichnet sich dadurch aus, dass auf jeder Systemebene, zum Beispiel Fahrzeug, Steuergerät und Software, Produkte entstehen, die dem Anspruch an die Produktsicherheit genügen, das heißt fehlerfrei sind. Fehlerfrei bedeutet im juristischen Sinn im Wesentlichen ohne Konstruktions- und Fabrikationsfehler. Softwarefehler sind regelmäßig Konstruktionsfehler, weil sie unter den gleichen Bedingungen immer auftreten, während ein mangelhafter Herstellungsprozess mit nachlässiger Qualitätssicherung zu Fabrikationsfehlern führen kann.

Die gesetzliche Haftung schützt den einzelnen Anwender, aber auch jeden Dritten. Dabei wird zwischen Produkthaftung und Produzentenhaftung unterschieden:

– Die Produkthaftung bezieht sich auf das Ergebnis des Herstellungsprozesses, also auf das fertige Produkt.

– Die Produzentenhaftung greift ein, wenn der Hersteller während der Entwicklung und Herstellung fahrlässig seine Organisations- und Sorgfaltspflichten verletzt.



Sicherheitslebenszyklus nach IEC 61508

Die folgenden Ausführungen konzentrieren sich auf den Entwicklungs- und Herstellungsprozess und damit in juristischer Sicht auf die (drohende) Produzentenhaftung: Welche Pflichten treffen den Hersteller bei der Entwicklung und Herstellung?

ORGANISATIONS- UND SORGFALTSPFLICHTEN DES HERSTELLERS

Ein Hersteller muss seinen Betrieb so ein-

AUTOREN

Dr.-Ing. Klaus-Jürgen Amsler ist Senior Consultant bei der Vector Consulting GmbH in Stuttgart.

Dr.-Ing. Joachim Fetzer ist Geschäftsführer der Vector Consulting GmbH in Stuttgart.

RA Dr. Meinhard Erben ist Rechtsanwalt für IT-Recht in Stuttgart.

richten, dass Konstruktions- und Fabrikationsfehler – auch bei Zulieferteilen – möglichst ausgeschaltet oder durch Kontrollen entdeckt werden. Da es (nahezu) unmöglich ist, softwarebasierte Systeme fehlerfrei zu entwickeln, ist der Hersteller verpflichtet, alle ihm obliegenden Organisations- und Sorgfaltspflichten umso akribischer zu beachten, das heißt das softwarebasierte System so intensiv zu testen, dass schwere Schäden für Leib oder Leben möglichst ausgeschlossen werden.

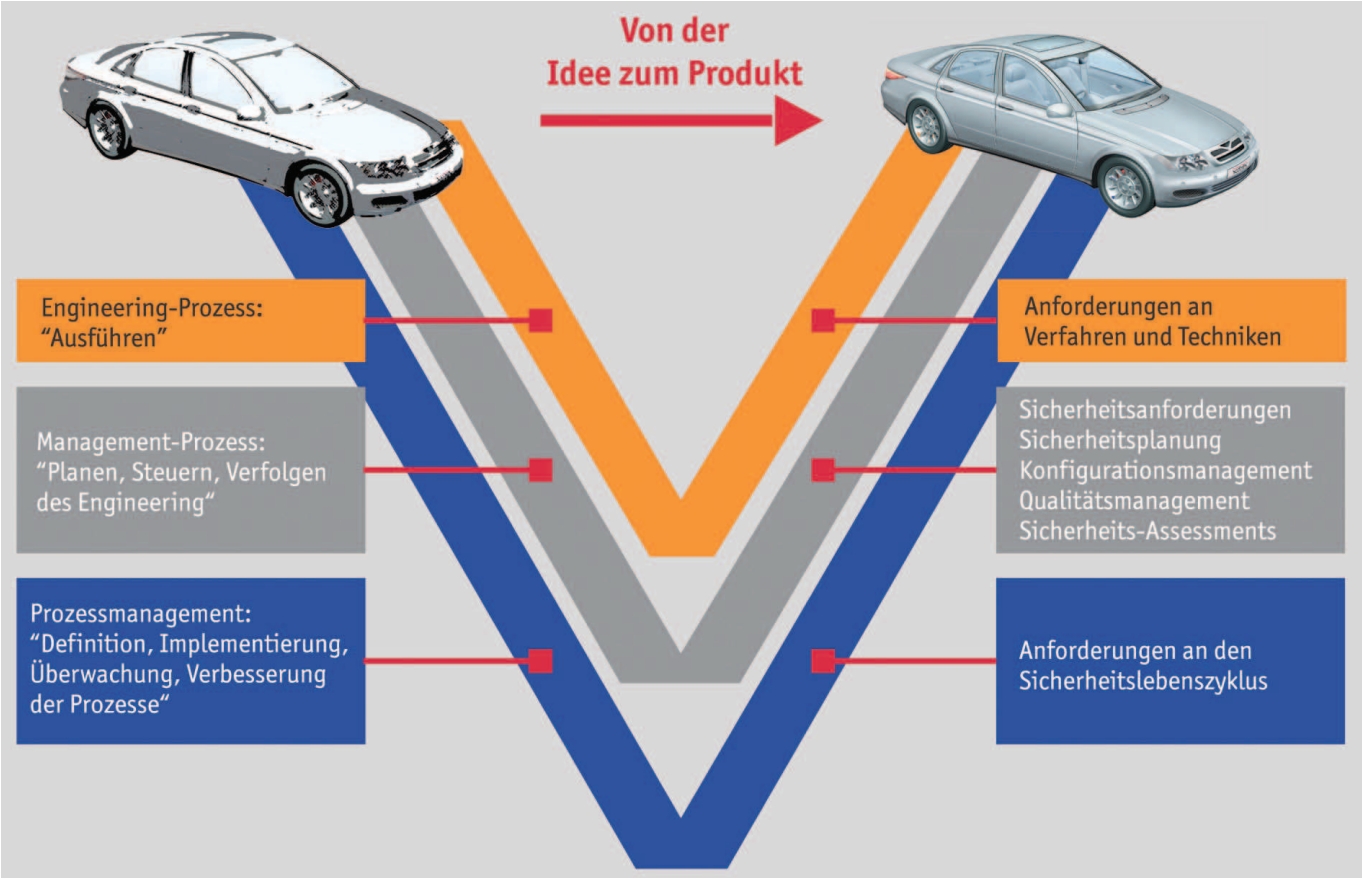
Dies trifft in besonderem Maße bei der Entwicklung von Embedded Systems für Kraftfahrzeuganwendungen zu, weil es sich hierbei um komplexe mechatronische Systeme (Mechanik, Hardware und Software) handelt [2]. Hier müssen Entwicklungsumgebungen mit konsistenten Design-, Implementierungs-, Integrations-, Test- und Simulationskonzepten eingesetzt werden.

Für den Software-Hersteller, aber auch den Kfz-Hersteller, ist die genaue Beachtung der Normen zum Stand der Technik, wie die Norm IEC 61508 [3] oder Prozessreifemodelle wie CMMI [4] oder SPICE [5], auch aus Beweislastgründen eminent wichtig. Denn Beweisfragen spielen bei der 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 im Wesentlichen nur darzulegen, dass das Produkt objektiv einen Sicherheitsmangel aufwies, das heißt, dass der Fehler bei der Entwicklung hätte vermieden werden können. Dabei lässt die Rechtsprechung häufig den so genannten ersten Anschein als Beweis gelten. Der Hersteller kann (und muss!) dann beweisen, dass er für den Fehler nicht verantwortlich ist, weil er die im Verkehr erforderliche Sorgfalt hinsichtlich der Konstruktion und Herstellung des Produkts beachtet hat. Damit er dieses tun kann, ist die Einhaltung und Nachweisbarkeit analytischer und konstruktiver Qualitätssicherungsmaßnahmen unbedingt notwendig.

WAS IST AUS JURISTISCHER SICHT ZU TUN?

Der Hersteller muss die vorgenannten organisatorischen Pflichten erfüllen und er muss die Erfüllung dieser Pflichten später auch nachweisen können. Dies setzt voraus, dass

Zuordnung der Anforderungen aus der IEC 61508 zu den Prozessebenen des Automotive Systems Engineering



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
– Verfahren für das Anforderungs- und Änderungsmanagement
– Qualitätssicherungsmaßnahmen.

SICHERHEITSTECHNISCHE ANFORDERUNGEN

Im Bereich der sicherheitstechnischen Anforderungen wurde im Jahr 2002 die internationale Sicherheitsgrundnorm IEC 61508 [3] in das deutsche Normenwerk übernommen und als DIN EN 61508 veröffentlicht. Sie bildet damit die Grundlage für den Stand der Technik im Bereich softwarebasierter sicherheitsbezogener Systeme.

Die Norm IEC 61508 formuliert organisatorische Anforderungen mit Festlegungen zur funktionalen Sicherheit (Management und Beurteilung), zum Dokumentenmanagement und zur Definition eines Sicherheitslebenszyklus im Sinne einer konsequenten Prozessorientierung. Dortige technische Anforderungen beziehen sich im Wesentlichen auf die Sicherheitsintegrität der Hardwarearchitektur, also auf die Wahrscheinlichkeit zufälliger Hardwareausfälle sowie auf die systematische Sicherheitsintegrität zur Vermeidung und Beherrschung von Ausfällen. Letztere ist auf Software anzuwenden und besteht in der Implementierung empfohlener Verfahren und Techniken in jeder Phase des Software-Sicherheitslebenszyklus.

Bezieht man die Anforderungen der IEC 61508 auf die drei Ebenen Engineering-Prozess, Management-Prozess und Prozess-Management gemäß dem Ansatz des Automotive Systems Engineering [6], dann bildet sich ein Schwerpunkt der Anforderungen auf der Ebene des Management-Prozesses.

DER SICHERHEITSGERECHTE ENTWICKLUNGSPROZESS

Ein sicherheitsgerechter Entwicklungsprozess muss demnach bestimmte Eigenschaften in Bezug auf das Anforderungs-, Projekt-, Konfigurations- und Qualitätsmanagement besitzen. Diese Prozessbereiche werden in Reifegradmodellen wie CMM [7], CMMI [4] oder SPICE [5] beschrieben. Ein Entwicklungsprozess, der den Reifegrad „Level 2" bezogen auf diese Modelle erfüllt, stellt bereits eine gute Grundlage für einen mit der IEC 61508 konformen Entwicklungsprozess dar und erfüllt auch bereits die genannten Minimalanforderungen aus juristischer Sicht.

Aus dieser Feststellung leitet sich unmittelbar der Weg zum sicherheitsgerechten Entwicklungsprozess ab, der mit Maßnahmen des Prozess-Managements in drei Schritten erreicht wird:
– Ermittlung des Prozessreifegrads, basierend auf einem Reifegradmodell
– Durchführung von Maßnahmen zur Erlangung des Mindestreifegrads „Level 2" und gleichzeitig zur Steigerung der Effizienz des Entwicklungsprozesses
– Berücksichtigung der spezifischen sicherheitsrelevanten Anforderungen als ergänzende Prozessbausteine, wie zum Beispiel Durchführung von Gefährdungs- und Risikoanalysen zur Ermittlung der erforderlichen Sicherheitsintegrität oder Maßnahmen zur Beurteilung der funktionalen Sicherheit

Die schrittweise Ausrichtung hin zum sicherheitsgerechten Entwicklungsprozess kann damit als Maßnahme im Sinne der kontinuierlichen Prozessverbesserung angesehen werden.

ZUSAMMENFASSUNG

Die systematische Anwendung der Reifegradmodelle CMM, CMMI oder SPICE stellt eine wesentliche Grundlage dar, nicht nur die Anforderungen aus der internationalen Norm IEC 61508 sondern auch die Mindestanforderungen aus juristischer Sicht zu erfüllen. Ein wirksames Prozess-Management ist erforderlich, um – ausgehend von dieser Grundlage – einen mit der IEC 61508 konformen Entwicklungsprozess sukzessive zu etablieren und somit das Thema Produzentenhaftung proaktiv anzugehen.

Aus allem folgt: Für einen sicherheitsgerechten, IEC-61508-konformen Entwicklungsprozess muss wenig neu geregelt werden. Man kann und soll geradezu auf Bewährtem aufbauen – vorausgesetzt, dieses entspricht den dargestellten (Minimal-)Anforderungen.

Literatur

[1] Tread Act: www.ipa.fhg.de/Arbeitsgebiete/BereichA/210/leistungsangebote/Tread_Act/
[2] Frost & Sullivan: European Automotive Market for X-by-wire Technologies. Studie, 2001
[3] IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. www.iec.ch
[4] CMMI: www.sei.cmu.edu
[5] SPICE: www.isospice.com
[6] Lederer, D.; Fetzer, J.; Heling, G.; Baumann, G.: Automotive Systems Engineering – The Solution for Complex Technical Challenges? Proceedings, 5. Internationales Stuttgarter Symposium Kraftfahrwesen und Verbrennungsmotoren, Februar 2003, S. 593–607
[7] Paulk, M. C.; Weber, Ch. V.; Curtis, B.: The Capability Maturity Model. Guidelines for Improving the Software Process. Addison-Wesley, USA, 1995

Vector Informatik GmbH | Werkzeuge aus Software

Die Vector Informatik GmbH wurde 1988 in Stuttgart gegründet. Heute zählt man zu den führenden Herstellern von Software-Werkzeugen und -Komponenten für die Vernetzung in elektronischen Kfz-Systemen, basierend auf CAN, LIN, Most oder Flexray. Die Produkte gewährleisten beispielsweise die reibungslose Kommunikation zwischen elektronischen Komponenten in modernen Fahrzeugen. Weltweit setzen Kunden aus der Automobilindustrie, der Transport- und Steuerungstechnik auf die Lösungen und Produkte der unabhängigen und eigenständigen Vector-Gruppe, zu der auch die Vector Consulting GmbH, ebenfalls mit Sitz in Stuttgart, gehört, die 2001 gegründet wurde. Heute (Juni 2004) hat die Gruppe über 400 Mitarbeiter weltweit.

Weitere Informationen unter: www.vector-consulting.de