



SPICE

CMMI

ISO 26262

IEC 61508

SCHLÜSSELFAKTOREN FÜR EINEN
ERFOLGREICHEN PROJEKTABSCHLUSS

Funktionale Sicherheit – Das Gesamtsystem ‚Fahrzeug‘

Funktionale Sicherheit ist im Fokus der der Automobilindustrie. Der Safety Standard IEC 61508 und die spezifische Anpassung ISO CD 26262 für die Automobilindustrie kombiniert mit Reifegradmodellen wie CMMI oder SPICE helfen bei der systematischen und nachweisbaren Umsetzung. Speziell wegen Anforderungen aus der Produkthaftung riet jedoch Dr. Dieter Lederer, Geschäftsführer der Vector Consulting GmbH anlässlich des Vector Forums „Funktionale Sicherheit“ zu zügigem Handeln, denn wer die Systemrisiken einzuschätzen weiß, wird auch keine Probleme bekommen.

Funktionale Sicherheit (FS) ist Teil der Gesamtsicherheit, der von der korrekten Funktion eines sicherheitsrelevanten Systems abhängt. Nehmen wir beispielsweise das Bremssystem. Der Fahrer betätigt die Bremse und das System bremst – in jeder Situation und unter allen Umständen. Wesentlich ist, dass hier das gesamte System, vom Bremspedal bis zur Wirkung auf die Räder betrachtet wird. Es genügt nicht, das Pedal oder die Umsetzung auf die Räder einzeln abzusichern. FS ist eine Systemeigenschaft und

involviert alle Komponenten, die zur korrekten Funktion beitragen. Durch den hohen Grad der Vernetzung von Funktionen im Fahrzeug untereinander ist jedoch nicht nur die einzelne Funktion betroffen, sondern auch weitere Systeme, die dem Geräteverbund im Fahrzeug angehören und mit dieser Einzelfunktion in Relation stehen. Dies schließt auch nichtelektrische Merkmale mit ein. In unserem Beispiel könnte das eine Display-Anzeige sein, die auf Störungen im System Bremse hinweist.



Was ist ein System?

Wie ist ein System definiert? „Oft haben Zulieferer und OEM eine unterschiedliche Auffassung, über die Definition des Systembegriffs“, so erläutert Dr. Stefan Kriebel, Abteilungsleiter Softwareentwicklung Fahrdynamik bei der BMW AG, ein mögliches Defizit in der Kommunikation zwischen beiden Partnern. Zum einen gibt es den Systembegriff mit Bezug zur Gesamtfahrzeugebene, der insbesondere für die E/E-Vernetzung relevant ist, aber auch für die Funktionsentwicklung aufgrund ihrer zunehmenden Vernetzung an Bedeutung gewinnt. Zum anderen wird der Systembegriff auch für die Komponentenentwicklung verwendet, wobei ein in sich geschlossenes (Regel-)System betrachtet wird, welches meist auch exklusiv auf einem Steuergerät beheimatet ist. Funktions- und Steuergeräte-Entwicklung wurden bisher vorwiegend abhängig voneinander betrieben, was die Vernetzung von Funktionen, als auch von Komponenten sehr aufwändig macht. „Für komplexe Dienstleistungen auf der Systemebene muss zukünftig auf Seiten der Zulieferer nicht nur das zu entwickelnde System betrachtet werden, sondern auch dessen Vernetzung, auf einer Ebene, die deutlich über dem bisherigen Systembegriff der Komponente hinausgeht“, so Dr. Kriebel. Jedoch nimmt er die Fahrzeughersteller nicht aus der Pflicht, denn ihnen gelingt es nach seinen Worten noch nicht ausreichend, die Vernetzung des Systems ‚Fahrzeug‘ hinsichtlich der Anforderungen an FS frühzeitig im Entwicklungsprozess zu beschreiben und damit einen wesentlichen Beitrag zur effizienteren Entwicklung von FS-relevanten Systemen beizusteuern. Die Stärken von

OEM und Lieferant können in einer guten Zusammenarbeit, z. B. durch eine frühzeitige und gemeinsame Gefahren- und Risikoanalyse genutzt werden. **Bild 1** zeigt, dass beide Seiten ihre eigene spezielle Expertise einbringen müssen, damit eine risikobasierte Entwicklung hin zu nachvollziehbarer FS möglich ist.

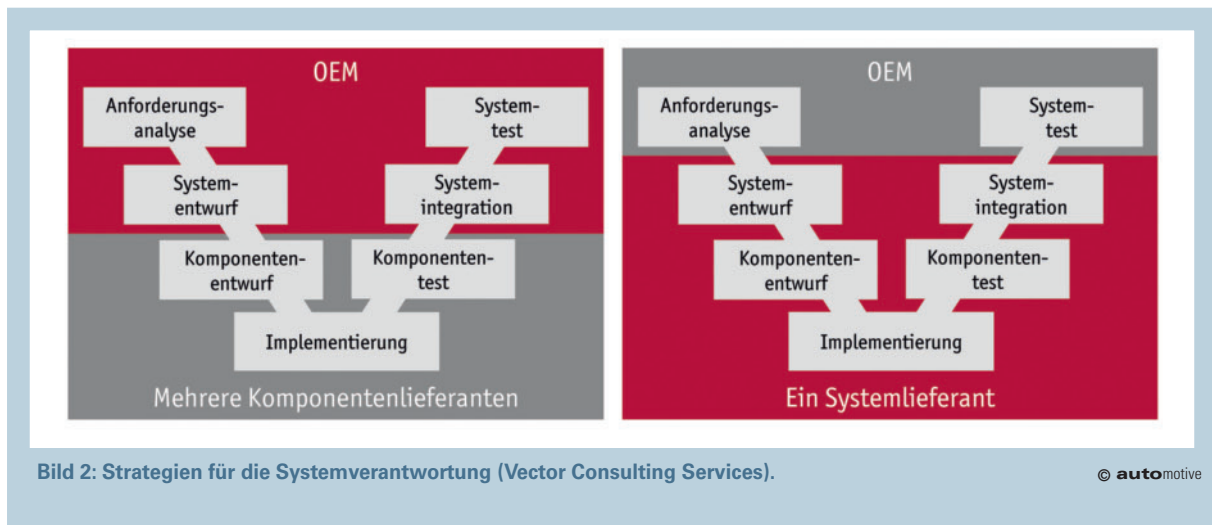
Allerdings wird in den Unternehmen die Umsetzung von FS-Aufgaben oftmals von dediziert eingesetzten Personen ausgeübt. Funktionale Sicherheit wird dann nur als „Add-on“ an den existierenden Entwicklungsprozess angehängt und am Ende ins Gesamtsystem hinein integriert. Daraus ergibt sich allerdings eine nur suboptimale Qualität im Gesamtsystem. Kritisch ist dieses lokale Vorgehen, weil damit FS nicht durchgängig aus System-sicht nachweisbar ist. Zudem entstehen ineffiziente Lösungen, da sicherheitsrelevante Aspekte unterschiedlich umgesetzt werden. Jürgen Belz, Leiter der Abteilung Prozesse, Methoden und Tools bei der Hella KGaA Hueck & Co., beziffert diesen Mehraufwand auf 8 bis 12% des Gesamtumfangs. Seiner Erfahrung nach hält sich deshalb, neben den Vorbehalten durch zusätzliche Risiken und Pflichten, auch das Management bedeckt. Meist gelingt es erst durch externe Beratung, die Führungsetagen von der Notwendigkeit einer durchgängigen FS-Kultur zu überzeugen.

Dies bestätigt auch Dr. Kriebel. Nach seinen Worten wäre es wichtig, dass FS-Know-how im selben Fokus steht wie das Funktions-Know-how selbst: „Wir sollten die funktionale Sicherheit und die Umsetzung deren Anforderungen zum Standard erheben und somit den dazugehörigen sicherheitsgerichteten Entwicklungsprozess als Standard leben. Für ein nicht FS-relevantes Projekt, oder für eines mit geringer FS-Einstufung, können wir die FS-Artefakte bewusst herausstreichen, die nicht benötigt werden.“

Viele Firmen sind aber noch lange nicht so weit. Simon Burton, von Vector Consulting Services sieht in der Praxis zwei Ausprägungen: „Zum einen zeigt sich bei einigen Unternehmen eine erschreckende Passivität aus Mangel an Verständnis, das Produkthaftungsrisiko wird

EFFICIENCY DAY 2008

Erfahren Sie anhand von Praxisvorträgen, Benchmarks und erprobter Methodik mehr darüber, wie Sie Ihre Produkte, Entwicklungsprozesse und die zugehörige Engineering-Infrastruktur optimieren und wie Sie passende Ansätze erfolgreich umsetzen können. efficiencyday - Effiziente Entwicklung elektronischer Systeme am 16. Oktober 2008 in Fellbach/Stuttgart
Das Programm finden Sie auch im Internet: www.hanser.de/efficiencyday



unterschätzt, eine Veränderung als nicht notwendig erachtet. Es ging ja bisher auch ohne durchgängige Entwicklungsprozesse für FS. Bei anderen Firmen dagegen entsteht Aktionismus aus Besorgnis. Das Thema kommt unweigerlich auf sie zu, also muss man irgend etwas tun.“ Diese Firmen stecken nach Burtons Erfahrung sehr viel Detailarbeit in Prozessdefinitionen und Methoden, und kaufen aufwändige Tools, ohne ein hinreichendes Verständnis des Gesamtkonzepts oder des Systems zu

haben. Die Konsequenz ist, dass Projekte gestresst und mit Details überfrachtet sind, während die gewählten Maßnahmen dennoch zu kurz greifen.

Dabei nimmt Burton die Zulieferer in Schutz. Sicherheitsziele würden nicht in der Systemarchitektur berücksichtigt, Annahmen über andere Systemkomponenten nicht dokumentiert oder weitergegeben. „Die Zulieferer sind nicht ausreichend über Verhalten der anderen Systeme informiert“, so der Experte.

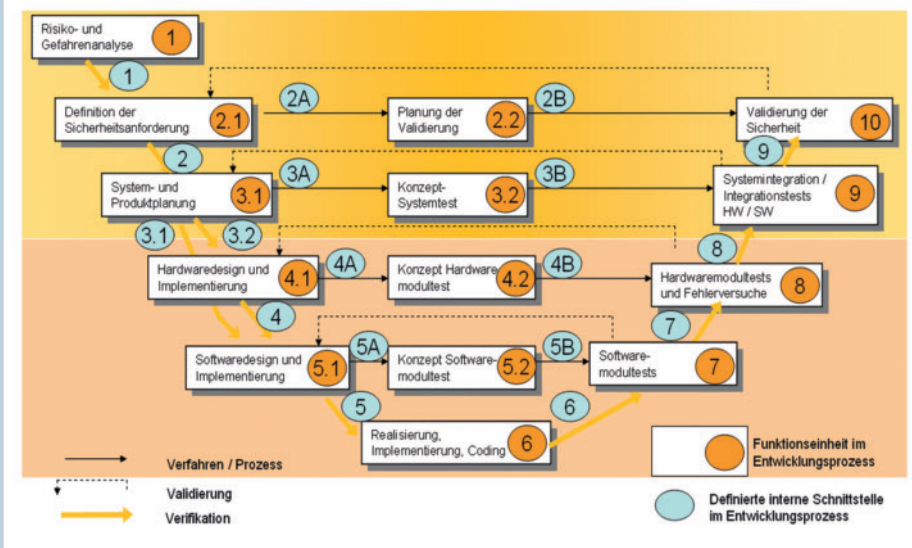


Bild 3: V-Modell nach FS-Management-Gesichtspunkten (Continental Teves).

© automotive

Das Ergebnis: Die Gesamtsicherheit des Systems wird nicht ausreichend beherrscht, der Einfluss einzelner Komponenten auf die Systemsicherheit ist nicht hinreichend klar. „Wenn Anforderungen unvollständig definiert sind, ist es unmöglich, nachträglich zu demonstrieren, dass alle Sicherheitsanforderungen erfüllt wurden.“ Dabei sollte das Systemsicherheitskonzept bereits in einer frühen Phase der Entwicklung erstellt werden, denn es muss Basis der Komponentenentwicklung sein.

Wer hat die Systemverantwortung?

In der Regel haben beide Seiten, Zulieferer ebenso wie die Fahrzeughersteller, Erfahrungen mit Gefahren- und Risikoanalysen. Diese Stärken sollten gemeinsam genutzt werden. Mögliche Strategien zeigt **Bild 2**. Unterschiede zeigen sich in den Grenzen der Verantwortlichkeit. So kann das Sicherheitskonzept durchaus vom Zulieferer erstellt werden. Dieser klärt dann die Schnittstellen zum Fahrzeug mit dem OEM (Bild 2, rechte Seite). Im anderen Fall gibt der OEM das Sicherheitskonzept vor und koordiniert die Komponentenschnittstellen (linke Seite).

Sicherheitsarchitektur integrieren

Im Auto müssen freilich andere Regeln gelten als beispielsweise im Flugzeug - denn dort sitzt kein auf Notfälle trainiertes Personal am Steuer. Der Ansatz eines Sicherheits-Entwurfsprozesses ist aber adaptierbar. Mehr Aufwand in Analyse und Risikomanagement zu Beginn eines Projekts ergibt später eine deutliche Abnahme der Kosten und Zeitaufwände. Das sieht auch Peter Zimmerschitt-Halbig, verantwortlich für FS-Management beim Zulieferer Continental Teves AG, so. Er kennt aus seinem Unternehmen Steuergeräte-Entwicklungsprozesse mit über 300 Einzelaktivitäten und vielen Subprozessen. „In Summe kommt es zu einer Reduzierung der Entwicklungskosten durch FS-Management,

denn FS-Management generiert keine Mehrarbeit, sondern strukturiert die Arbeitsweise der Entwickler und trägt zur Gestaltung von Zusammenhängen der Einzelaktivitäten bei.“

Projektplanung, Requirements Engineering, Architekturentwicklung, Systemanalyse, Testmanagement und Änderungsmanagement müssen in ihrer Gesamtheit vom System über Sub-Systeme bis hin zur Komponente systematisch und durchgängig verfolgt werden (**Bild 3**). Generell erfordert die Vorgehensweise ein sauberes Spezifizieren zu Beginn des Projekts.

„Die IEC 61508 ist etabliert und als Stand der Technik aner-

kannt“, so Zimmerschitt-Halbig. „Sie ist jedoch nur bedingt direkt anwendbar und benötigt eine gewisse Interpretation.“ Daher wird die kommende ISO 26262 deutlich mehr Hilfestellung leisten, sie liegt jedoch im Moment nur als Entwurf (sog. Committee Draft) vor und dürfte nicht vor 2011 zum Standard erklärt werden.

Der anerkannte und objektive Stand der Technik ist zum Schutz vor juristischen Auseinandersetzungen aber auf jeden Fall einzuhalten. Und der wird nicht nur durch Normen vorgeschrieben, wie Rechtsanwalt Dr. Wolf Günther von der auf technische Rechtsfragen spezialisierten Kanzlei Dr. Erben erläutert. „Wer die Systemrisiken fundiert einzuschätzen weiß, wird auch keine Probleme bekommen“, erklärte Dr. Dieter Lederer, Geschäftsführer der Vector Consulting GmbH. Konsequentes Risikomanagement, Qualitätsmanagement und ein systematischer Entwicklungsprozess sind laut Dr. Lederer Schlüsselfaktoren für einen erfolgreichen Projektabschluss: „Funktionale Sicherheit ist kein ‚Hexenwerk‘. Aber es erfordert Nachdruck und Nachhaltigkeit in der Umsetzung.“ (oe)



Dr. Christof Ebert ist Geschäftsführer der Vector Consulting Services GmbH.



Dr. Dieter Lederer ist Geschäftsführer der Vector Consulting Services GmbH.