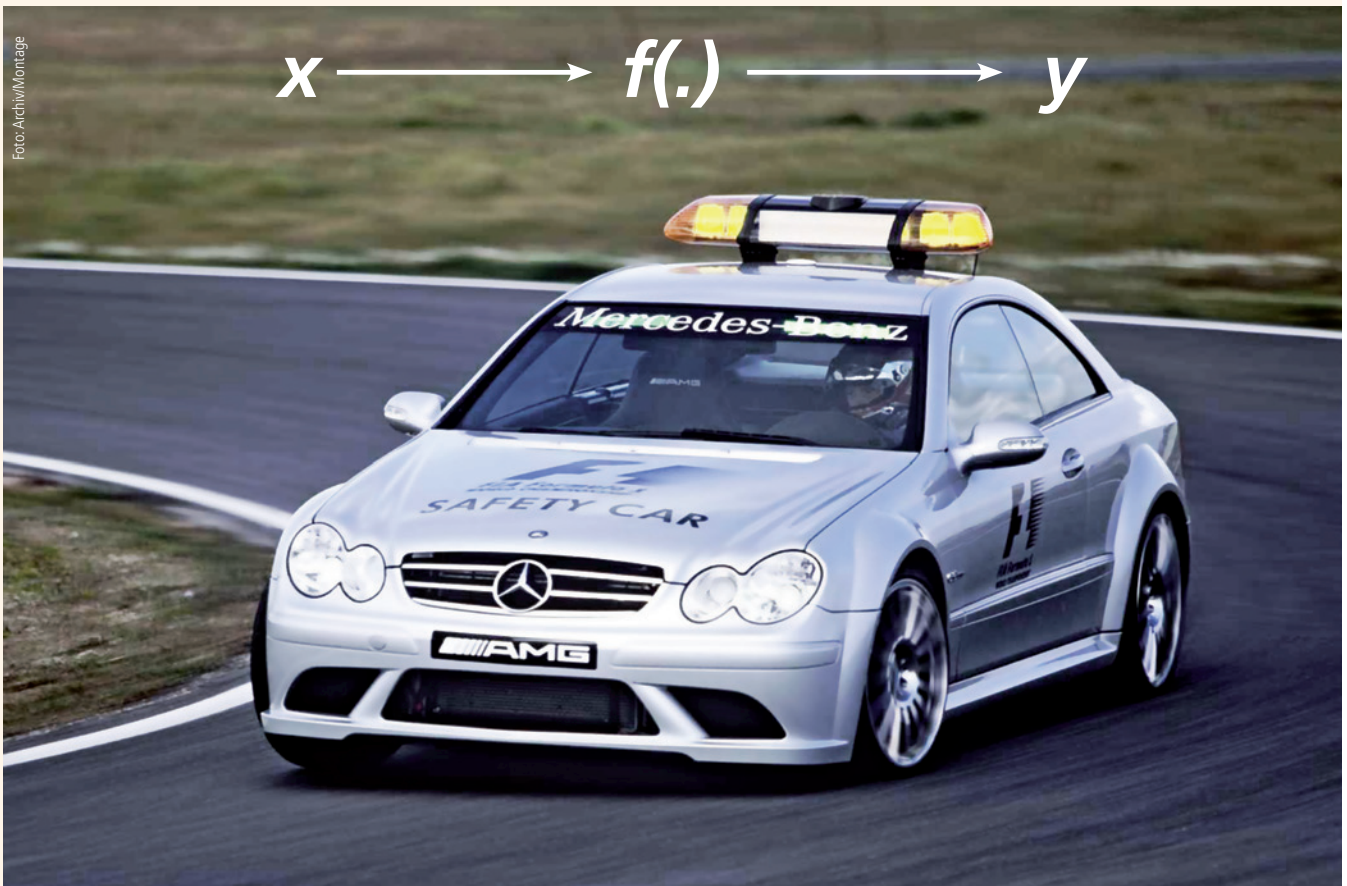


# Sicherheit hat ihren Preis

Funktionale Sicherheit: Dieses Schlagwort treibt Software-Entwicklern, Ingenieuren und den Rechtsabteilungen der Unternehmen den Schweiß auf die Stirn. Es gibt aber Wege, das hochsensible Thema in den Griff zu bekommen.



**E**in zu geringer Bremsdruck, irrtümlich abgeschaltete Airbags, plötzlich schließende elektrische Heckklappen: Vor Zwischenfällen dieser Art ist kein Automobilhersteller gefeit. Selbst in den einschlägigen Normen (z.B. IEC 61 508) ist anerkannt, dass ab einer gewissen Komplexität Steuerungsabläufe nicht mehr fehlerfrei programmiert werden können. Untersuchungen von IBM, HP und der NASA rechnen mit einem bis drei Fehlern pro 1 000 Programmzeilen. Und die Automobilindustrie gibt mehr oder weniger offen zu, dass sie bei den oft verschachtelten Regel-

algorithmen gar nicht alle Einzelfälle testen und somit eine hundertprozentig korrekte Funktion nicht garantieren kann.

Dr. Simon Burton von der Vector Consulting Services GmbH, die sich auf die Optimierung von Produktentwicklungsprozessen spezialisiert hat, plädiert dafür, zunächst „Handlungsfelder zu identifizieren, die einen zielführenden Einstieg in die funktionale Sicherheit ermöglichen“. Er sieht drei solcher Felder:

■ **Systemorientierung:** Funktionale Sicherheit wird nicht allein durch isolierte Maßnahmen auf Komponentenebene erreicht. Vor

**Selbst das Safety-Car ist vor Rechenfehlern nicht gefeit.**

dem Systementwurf und der eigentlichen Komponentenentwicklung muss eine ausführliche Gefahren- und Risikoanalyse vorge-schaltet sein. Der Einfluss einzelner Komponenten auf die System-sicherheit sollte hinreichend analysiert, dokumentiert und für alle Beteiligten einsichtig sein, damit die Verantwortungen und Aufgaben verstanden und klar abgegrenzt sind. Auch die Systemverantwortung zwischen OEM und Lieferanten gilt es vorab zu regeln.

■ **Risikobasierte Entwicklung:** Aus der erforderlichen Gefahren- und Risikoanalyse lassen sich ge-

zielt Sicherheitsanforderungen ableiten, die in der Produktentwicklung durchgängig angewendet werden müssen. Die bisherige Praxis mit Tests in den Spätphasen der Entwicklung ist nicht ausreichend und aufgrund der langen Korrekturzeiten oder gar Rückrufaktionen viel zu teuer.

■ Sicherstellen der grundlegenden Prozessfähigkeiten: Ohne systematisch verknüpfte Prozessketten und deren konsequente Anwendung lässt sich eine sicherheitsgerechte Entwicklung kaum durchhalten und ist bei Problemen nicht nachvollziehbar. Die Mitarbeiter müssen Sicherheitsprozesse zunächst verstehen und erkennen, dass die funktionale Sicherheit ein ganz wesentlicher Bestandteil eines Produkts ist – wie sein Funktionsumfang oder die Kosten.

**Neben den technischen Aspekten** hält Burton parallel organisatorische Veränderungen für erforderlich: „Die Umsetzung der Prinzipien der funktionalen Sicherheit bedeutet einen tiefen Eingriff in eine Organisation. Es braucht dazu ein Veränderungsprojekt mit konkreten Zielen und einer Roadmap für deren Umsetzung. Gefordert sind hierarchieübergreifende Kommunikation und eine gezielte Aus- und Weiterbildung der Mitarbeiter.“

In der Praxis lauern aber Tücken. Noch längst nicht alle Automobilhersteller und Zulieferer sehen einen sicherheitsorientierten Entwicklungsprozess als Standard – sondern bisweilen eher als Extrabelastung. Ein deutscher Elektronikzulieferer beziffert seine Mehrkosten für Prozesse, bei denen die Prinzipien der funktionalen Sicherheit angewendet werden, auf plus/minus zehn Prozent.

In einigen Jahren dürften auch automobilspezifische Entwurf-

tools bereitstehen. Sie sollen den Ingenieuren bei einem Hauptproblem helfen: der Deckungsgleichheit von textbasierten Lastenheftanforderungen und entworfenen Systemarchitekturen. Das sei auch bitter nötig, enthielten doch Lastenhefte nicht selten 40000 Einzelanforderungen, zu denen pro Quartal 300 bis 500 Änderungen anfielen, berichtet ein Spezialist für „Automotive Standards“ eines deutschen Zulieferers.

**Besonders die späten Änderungen** können fatale Folgen für die funktionale Sicherheit haben. Das müssten die OEM noch lernen, wie ein OEM-Insider offen zugibt. Er plädiert dafür, den bisher praktizierten Entwicklungsprozess mit vielen isolierten, teilweise parallelen Projekten und einer späten Systemintegration zu verlassen: „Dadurch entstehen zwar lokale Optima, aber nur suboptimale Qualität im Gesamtsystem und ein hoher Entwicklungsaufwand.“ Beispielsweise wird so deutlich zu früh auf Umsetzungsdetails übergegangen. Und Sicherheitsaspekte werden meist erst nachträglich implementiert.

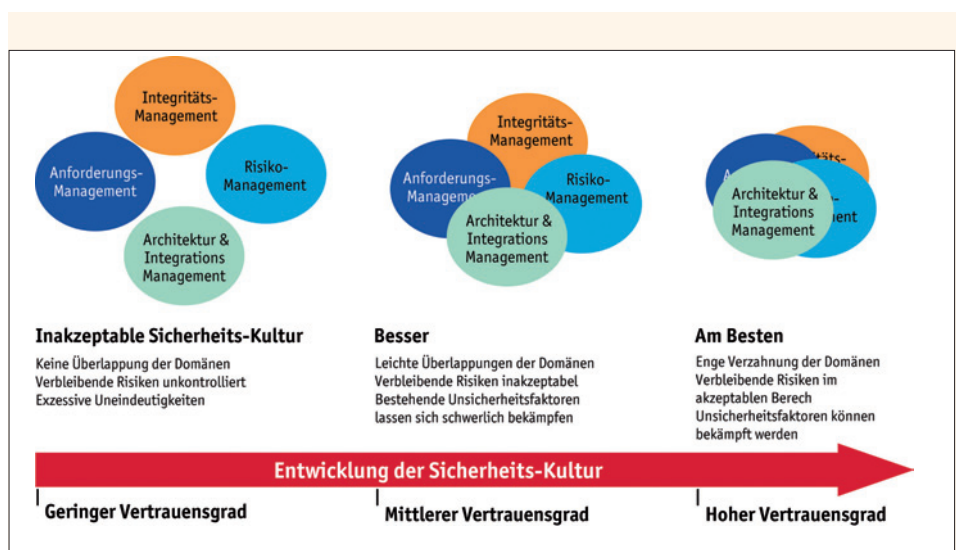
Zielführend sei es, wenn sich die OEM zunächst auf die überge-

ordnete, abstrahierte Funktionsarchitektur (logische Signale und abstrakte Softwarearchitektur) des Fahrzeugs konzentrieren würden. Das bedeute zwar einen gewissen Mehraufwand. Aber die Funktionsarchitektur aus einem Guss begünstige die Wiederverwendbarkeit von einzelnen Komponenten als Baukastensystem. Denn die Spezifikation sei fahrzeugunabhängig und funktionsorientiert. Außerdem reduziere sich der Variantenaufwand.

Auf Basis der Funktionsarchitektur kann der OEM gemeinsam mit den Zulieferern auch relativ schnell die technische Architektur (Hardware, Telegramme und die variantenabhängige Software) des Fahrzeugs spezifizieren und die gegenseitigen Verantwortungen bei der Entwicklung und Integration sauber darstellen.

Auch die Nutzerarchitektur mit ihren Fahrerschnittstellen wird aus der Funktionsarchitektur abgeleitet. Mit diesem Top-Down-Ansatz könnte der Entwicklungsaufwand um bis zu 20 Prozent verringert werden. Das würde auch die Akzeptanz sicherheitsrelevanter Systementwicklung beträchtlich erhöhen.

Hartmut Hammer



Der Sicherheitsgedanke muss im Unternehmen flächendeckend verankert sein.

Abb.: Vector Informatik