

INTEGRATION VON FUNKTIONALER SICHERHEIT IM ENTWICKLUNGSPROZESS

Die neue Sicherheitsnorm ISO 26262 zwingt die Hersteller elektronischer Fahrzeugsysteme, sämtliche Entwicklungsprozesse auf das Thema Sicherheit auszurichten. Allerdings sind die „Safety-Aktivitäten“ oft von den „normalen“ Tätigkeiten der Entwickler komplett isoliert. Die Sicherheitsvorgaben fließen deswegen erst spät in den Entwicklungsprozess ein. Kostspielige und zeitintensive Änderungsschleifen werden notwendig. Berner & Mattner stellt eine neue Methodik vor, die Sicherheitsaktivitäten werkzeuggestützt mit der klassischen Systementwicklung verzahnt und Sicherheitsanforderungen frühzeitig ins Systemdesign einbezieht. In Kundenprojekten konnten den Aussagen der Autoren zufolge deutliche Effizienzsteigerungen erzielt werden.



AUTOREN



DR.-ING. BERNHARD KAISER
ist Teamleiter Automotive Competence
Center Safety & Systems Engineering
bei Berner & Mattner Systemtechnik
GmbH in Berlin.



JÜRGEN MEYER
ist Bereichsleiter Automotive
bei Berner & Mattner
Systemtechnik GmbH
in München.

GEMÄSS ISO 26 26 2

Das auf den jeweils neuesten Stand von Wissenschaft und Technik referenzierende Produkthaftungsgesetz in Verbindung mit dem neuen Automotive-Standard ISO 26262 fordert von Fahrzeugherstellern die Einhaltung sämtlicher vorgeschriebener „Safety-Aktivitäten“ über den gesamten Produktlebenszyklus. Dabei müssen alle Arbeitsprodukte lückenlos nachgewiesen werden können – von der Gefährdungsanalyse über das Sicherheitskonzept bis zur Umsetzung und dem Test der daraus resultierenden Sicherheitsanforderungen – begleitet von einer Vielzahl von Reviews, Sicherheitsanalysen und Assessments. Um diesen Nachweis im Haftungsfall auch nach Jahren zu ermöglichen, ist insbesondere die „Traceability“, also die eindeutige Verfolgbarkeit zwischen entdeckten Fehlermöglichkeiten, zugeordneten Sicherheitsanforderungen, betroffenen Systemelementen den verifizierenden Testfällen nötig, die sich bei der Komplexität heutiger Produkte nur noch werkzeuggestützt beherrschen lässt.

Dies stellt heute viele Unternehmen vor Probleme, da die Sicherheitsaktivitäten oft noch weitgehend losgelöst vom sonstigen Produktentwicklungsprozess ablaufen. Gefährdungs- und Sicherheitsanalysen beziehen sich häufig auf veraltete Annahmen über die Funktionsweise und Architektur des Systems, weil die damit betrauten Personenkreise oft verschieden sind.

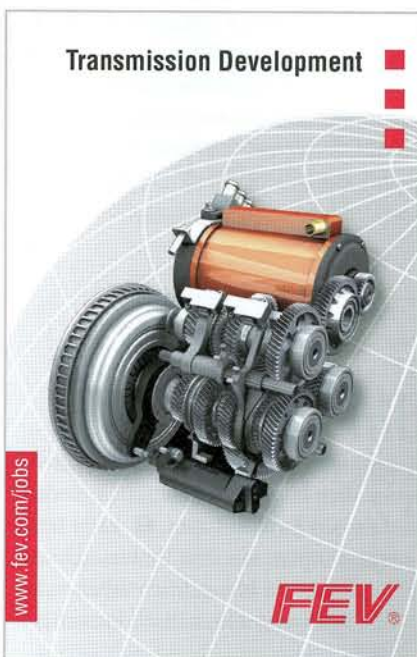
MANKO

Sicherheitskonzepte entstehen unabhängig vom parallel fortschreitenden Systemdesign, sodass die Sicherheitsanforderungen zu spät in die Entwicklung einfließen. Damit fallen kostspielige Nachentwicklungszyklen an, um die Sicherheitsaspekte nachträglich zu integrieren – samt den dadurch erforderlichen zusätzlichen Tests und Reviews.

Ein Hauptproblem dabei ist, dass Safety Manager und FMEA-Moderatoren (FMEA Failure Mode and Effects Analysis) oftmals eine unterschiedliche Sprache sprechen und andere Werkzeuge benutzen als die System- und Software-Entwickler. So bleiben die heute oft schon vorhandenen toolbasierten Architekturmodelle ungenutzt für eine systematische Untersuchung von Fehlerfortpflanzung

von einer Systemkomponente zur anderen. Umgekehrt erstellen die Safety Manager ihre Sicherheitsanforderungen weder sprachlich noch toolmäßig so, dass sie sich automatisiert in die normalen Anforderungs-Spezifikationen importieren und verlinken ließen. Obwohl also Safety Manager, FMEA-Moderatoren und Entwickler jeweils für sich gute Arbeit leisten, scheitert die Effizienz an der fehlenden Durchgängigkeit. Die aktuelle Herausforderung für die Unternehmen liegt darin, Parallelprozesse zu vermeiden und von Anfang an die FuSi-Aktivitäten (Aktivitäten im Bereich Funktionaler Sicher-

– ANZEIGE –



heit (FuSi)) in den Entwicklungsprozess zu integrieren.

DER NEUE WEG: GANZHEITLICH, HIERARCHISCH, MODELLBASIERT

In mehreren Projekten haben Spezialisten von Berner & Mattner eine Entwicklungsmethode erarbeitet, die ein hierarchisches Modellieren von Systemarchitektur und Fehlernetzen, die Zuordnung der Sicherheitsmechanismen und eine systematische Anforderungsverfolgung samt Nachweis der Testabdeckung vereint. Diese Methodologie besteht aus der geschickten toolintegrierten Kombination grundsätzlich bekannter

und bewährter Ansätze. Die Methodologie stellt per se eine Vorgehensanweisung ohne zwingenden Bezug auf konkrete Werkzeuge dar, sie wurde jedoch in Serienentwicklungsprozessen bei mehreren Automotive-Zulieferern unter Verwendung von verbreiteten Standardwerkzeugen wie „Doors“, „APIS IQ-FMEA“ und „Enterprise Architect“ pilotiert. Eine Übertragung auf andere marktgängige Tools ist mit geringem Aufwand möglich.

Ein weiterer Vorteil des Ansatzes ist, dass die entstehenden Modelle und Konzeptbausteine modular und wiederverwendbar sind und damit effizient für Produktvarianten und künftige Entwicklungen herangezogen werden können.

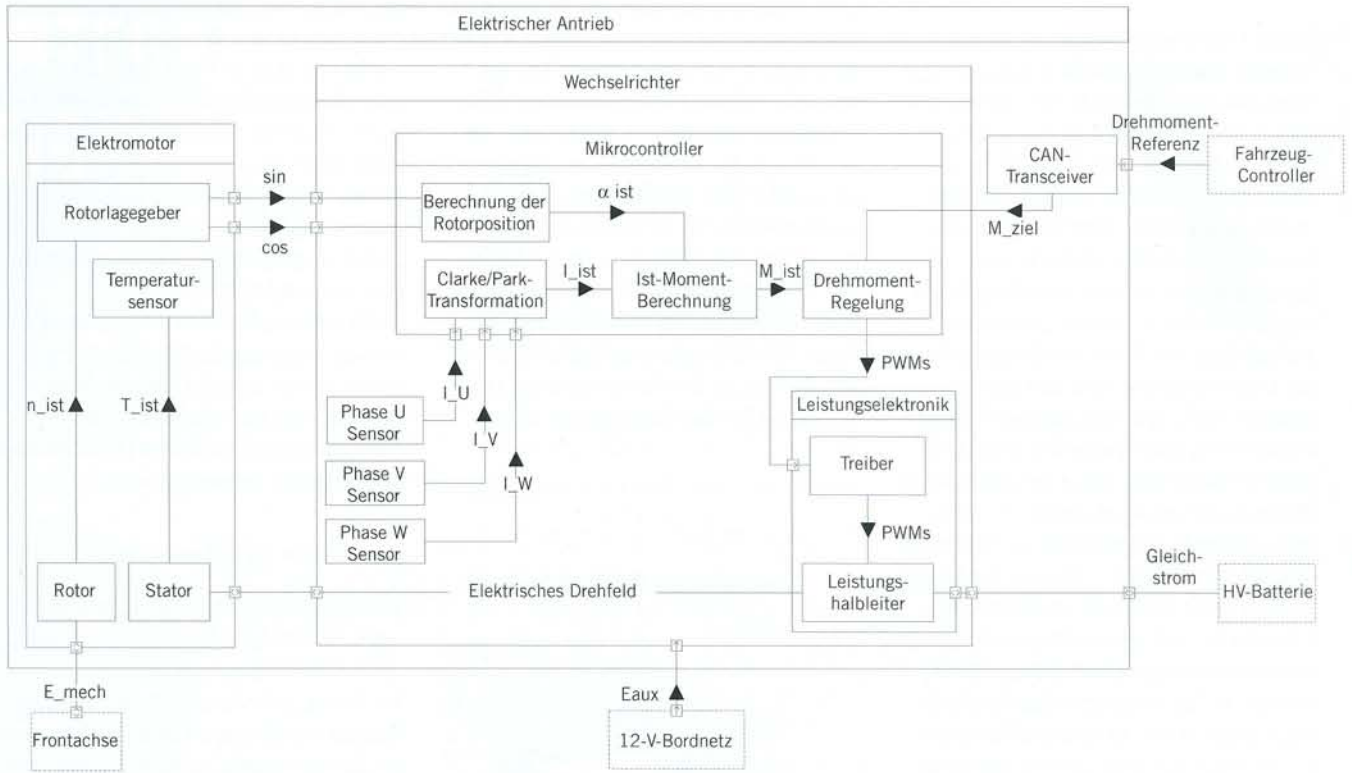
START DER SYSTEMENTWICKLUNG

Wie in jedem reifen Entwicklungsprozess steht am Anfang eine sorgfältig strukturierte Anforderungsspezifikation in einem Werkzeug, zum Beispiel Doors. Mit den Kunden wurde eine Struktur erarbeitet, die die Anforderungen, Annahmen und Constraints nach Funktionsbereichen strukturiert und als unterste Gliederungsebene sogenannte „Features“ definiert, die eine schlagwortartige Funktionsbezeichnung darstellen, wie etwa „Regelung des Motorstroms“.

Dieses Vorgehen erlaubt es, frühzeitig und mit geringem Aufwand eine erste Verlinkung dieser überschaubaren Anzahl von Features auf das Systemarchitekturmodell vorzunehmen, das parallel in einem Modellierungswerkzeug entsteht, ①. Dabei wird von der geplanten Systemarchitektur zunächst ein sehr einfaches Modell entwickelt, das dann iterativ über die Definition von Subsystemen und tabellarisch erfassten externen Signalen/Inputs sowie über das dynamische Verhalten des Systems verfeinert und mehrfach überarbeitet wird.

Entscheidend an der Systemmodellierung ist ihr hierarchischer Aufbau, der zum Zweck der späteren Sicherheitsmodellierung noch eine Ebene über die Systemgrenze hinausgeführt wird, die als Kontextdiagramm das System in seiner Interaktion mit Nachbarsystemen zeigt. Wichtig auf allen Ebenen ist es, frühzeitig die Schnittstellen zwischen den Komponenten vollständig zu erfassen, denn entlang dieser Schnittstellen pflanzen sich in der Sicht der FuSi-Experten auch die Fehler

ibd [Block] Elektrischer Antrieb [Extended]



1 Systemarchitektur als SysML „Inner Block Diagram“

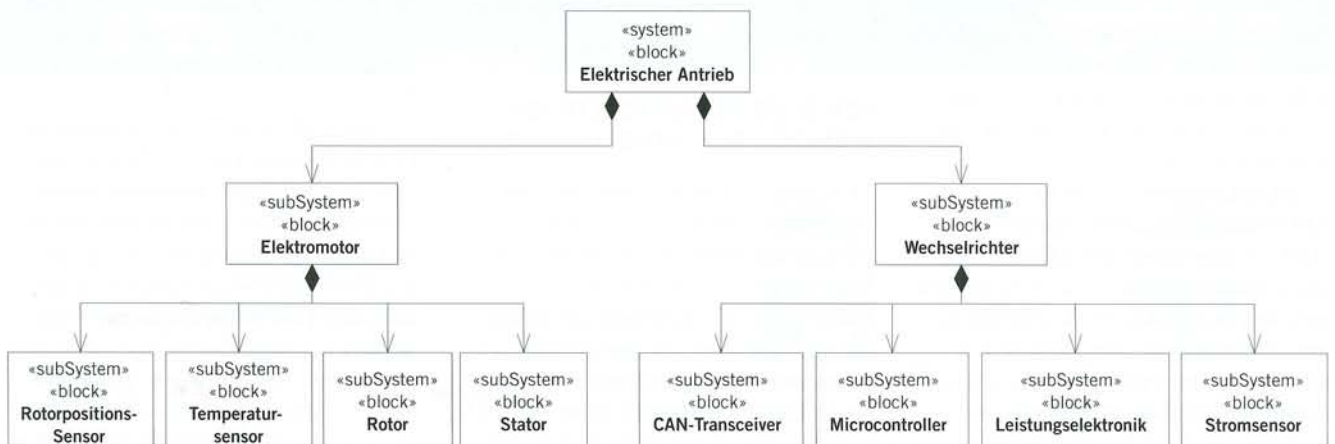
lerauswirkungen fort. So kann etwa ein zu niedrig gemessener Drehzahlsensorwert im nachfolgenden Regler zu einem überhöhten Stelleingriff führen, der sich dann an der Außengrenze des Systems als Selbstbeschleuniger des Antriebs auswirkt, was als sicherheitskritischer Vorfall (Hazard) einzustufen wäre.

DER AUTOMATISIERTE EXPORT

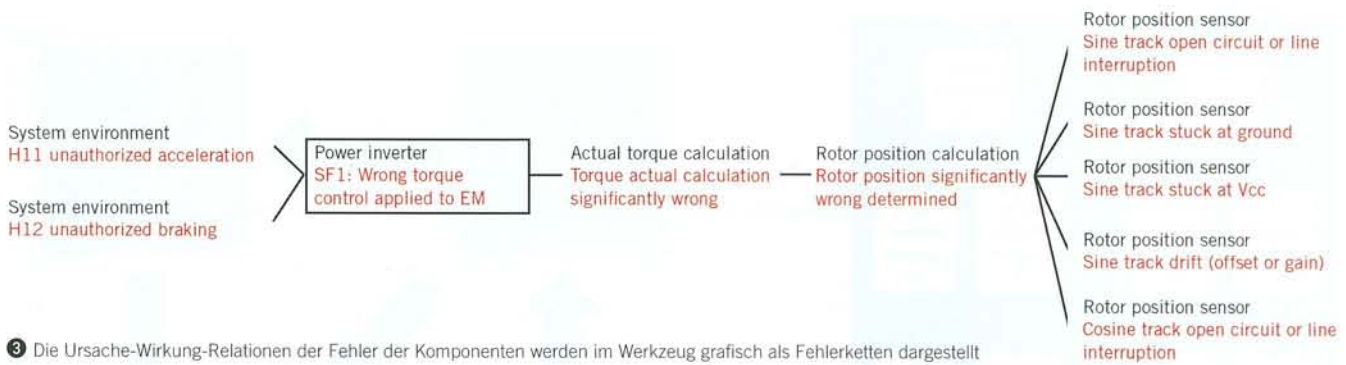
Aufgrund der Äquivalenzbeziehung zwischen dem hierarchischen Systemmodell und dessen Strukturbaum, 2, kann letzterer mit Skripten aus dem Systemarchitekturmodell in ein hierarchisch arbeitendes FMEA-Werkzeug automatisch importiert

werden. So profitieren die FuSi- und FMEA-Experten schon von der nun vorhandenen Datenstruktur, während die Funktionsentwickler die Anforderungen und die Systemarchitektur iterativ verfeinern. Mehr noch: Durch die Verlinkung zwischen Doors und dem Modellierungstool können die beabsichtigten Funktionen einer jeden Kompo-

bdd



2 Repräsentation der Architektur als Strukturbaum



3 Die Ursache-Wirkung-Relationen der Fehler der Komponenten werden im Werkzeug grafisch als Fehlerketten dargestellt

nente auf allen Hierarchieebenen ebenfalls automatisch in die FMEA übernommen werden, was eine enorme Aufwandsreduktion und eine bisher nicht gekannte Konsistenz ermöglicht.

Nun können die geforderten Sicherheitsanalysen, beginnend mit der Gefährdungsanalyse und Risikobewertung, in dem FuSi-Werkzeug (Werkzeug für Funktionale Sicherheit) durchgeführt werden. Dazu werden zu den beabsichtigten Funktionen je Komponente die möglichen Fehlfunktionen angetragen, systematisiert durch eine der „HAZOP-Technik“ entlehnte Schlüsselwortmethode (bei kontinuierlichen Signalen, beispielsweise „zu viel“, „zu wenig“, bei Ereignissen „zu spät“, „unerwartet“ etc.). HAZOP (englisch: HAZard and OPerability) dient der Überprüfung der Sicherheit und Funktionsfähigkeit technischer Systeme. Die Ursache-Wirkung-Relationen der Fehler der Komponenten werden im Werkzeug grafisch als Fehlerketten dargestellt, 3. Dafür werden anhand der bekannten Schnittstellen und der durch die Architektur vorgegebenen Verschaltung automatisch Vorgaben durch das Tool gegeben, da sich Fehler nur über diese Pfade zwischen Nachbar-komponenten oder zwischen Komponenten und ihren Über-Komponenten fortpflanzen können.

Da die oberste Architekturebene das Gesamtsystem in seiner Umgebung repräsentiert, sind die sich an dessen Grenzen auswirkenden Fehler potenzielle Gefährdungen. Diese werden, bezogen auf verschiedene Verkehrssituationen, nach den Parametern „Schwere“, „Auftrittshäufigkeit der Situation“ sowie „Beherrschbarkeit“ bewertet, um den ASIL zu erhalten. So besteht bereits eine natürliche Verlinkung zwischen der Gefährdungsanalyse und der FMEA, die das im Laufe der Ent-

wicklung immer konkreter werdende Systemdesign bis hinunter zur Bauteilebene nach neu hinzukommenden Fehlermöglichkeiten durchsucht. In gemeinsamen Workshops zwischen Entwicklern, FMEA-Moderator und den Experten für Funktionale Sicherheit werden nun technisch und wirtschaftlich machbare Gegenmaßnahmen nach den Vorgaben der ISO 26262 definiert, die der Verhinderung, Erkennung oder Beherrschung möglicher Fehler die-

nen. Die Konsistenz zwischen FMEA und Systemmodell hat sich dabei als hervorragende Verständnishilfe zwischen den Disziplinen bewährt.

RÜCKSPEISUNG IN DEN ENTWICKLUNGSPROZESS

Die Ausarbeitung der Maßnahmen zu Safety Requirements und deren Allokation auf die Systemarchitektur geschieht nach

BTC Embedded Tester®

ISO 26262 zertifizierte Testumgebung für TargetLink®



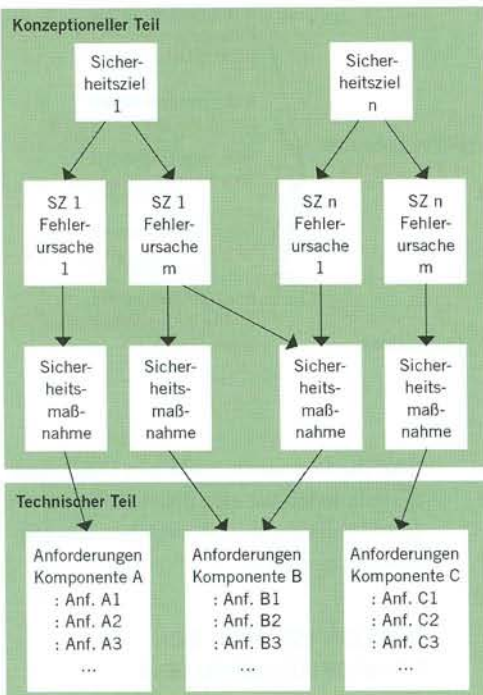
TargetLink
STRATEGIC
PARTNER

- „Fit for Purpose“ nach ISO 26262
- Anforderungs- / Modellbasiertes Testen
- Coverage-Messungen auf allen Ebenen
- Automatische Testfallgenerierung
- Automatische Back-to-Back-Tests
- Automatisierte Debug-Unterstützung

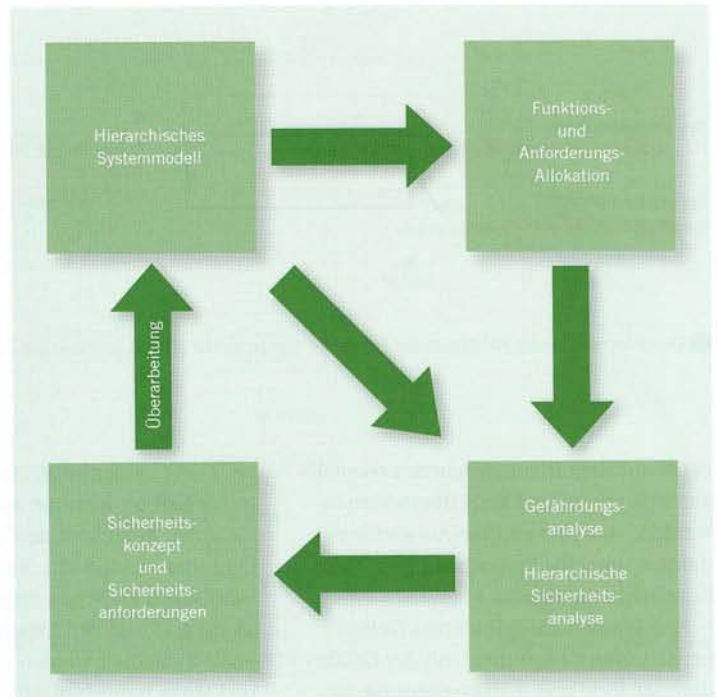
Besuchen Sie uns auf dem
VDI-Kongress „Elektronik im Kraftfahrzeug“
12. - 13. Oktober 2011 in Baden-Baden
auf dem BTC-Stand der Fachausstellung!

www.btc-es.de





4 Doors-Repräsentationen des Sicherheitskonzepts



5 Integration vorhandener Techniken in ein in sich konsistentes Framework

den Vorgaben der Norm im Sicherheitskonzept. Dieses wird im Ansatz von Berner & Mattner nicht mehr als Textdokument gepflegt, sondern komplett in Doors. Der Import der Sicherheitsmaßnahmen aus dem FMEA-Tool bietet auch in dieser Richtung Automatisierungspotenziale. Doors-Attribute erlauben eine Klassifikation der Statements im Sicherheitskonzept, etwa als Annahmen, Maßnahmen, Safety-Strategien (wie etwa Asil-Dekomposition) und schließlich technischen Anforderungen, wobei nur die letzten in den weiteren Requirements-Prozess einfließen und durch Implementierungsnachweise und Testfälle abzudecken sind. Die Verwendung eines Anforderungswerkzeugs für das Sicherheitskonzept hat vielfältige Vorteile: Neben der hierarchischen Strukturierung ermöglicht das Tool die von der ISO 26262 geforderten Attribute, motiviert zu atomaren Anforderungen und erlaubt deren Integration in das Set der sonstigen Anforderungen samt nachfolgender Verlinkung zum Systemdesign und zu den Testfällen. Durch die eingangs erfolgte thematische Gruppierung der Anforderungen zu Features, die auf Modellelemente allokiert werden, ist der ASIL einer jeden Systemkomponente sofort ablesbar. Die vorgeschriebenen Reviews des Sicherheitskonzepts lassen

sich durch „Entlangklicken“ wesentlich vereinfachen; die Begründung zu Safety-Maßnahmen kann jederzeit nachvollzogen werden, was gerade im Fall von späteren Änderungen essenziell ist. Die Baseline-Funktionalität erlaubt weiterhin das geforderte Konfigurationsmanagement, 4.

Da im vorliegenden Projekt auch die Testfälle in Doors verwaltet wurden, angereichert um Attribute zum Stand der Testfallausführung und des Testergebnisses, konnten automatisiert wöchentlich Metriken und Tortendiagramme zum Stand der Absicherung der Safety Requirements erzeugt werden und das Safety Assessment somit optimal vorbereitet werden.

FAZIT UND AUSBLICK

Die beschriebene Methodik wurde bereits in mehreren Serienentwicklungsprojekten für Hybrid- und Elektroantriebe erfolgreich eingesetzt. Das einheitliche Verständnis von Entwicklern und FuSi-Experten über die Methodik und das System musste in der Anfangsphase über Workshops und vermehrte Abstimmungen in der praktischen Arbeit zunächst erarbeitet werden; bald zeigte sich jedoch, dass sich der anfängliche

Aufwand für die Modellierung schon im ersten Projekt schnell amortisiert, weil die Zusammenarbeit zunehmend reibungsloser verlief. Hinzu kommt, dass aufgrund der Modularisierung einmal erarbeitete Modellkomponenten in künftigen Entwicklungen wiederverwendet werden können.

Durch den neuen Ansatz flossen die Sicherheitsanforderungen deutlich früher als in vergleichbaren Projekten in die Entwicklung ein und konnten damit aufwandsärmer und kostengünstiger berücksichtigt werden. Die Sicherheitsanforderungen wurden als technische Spezifikation in Standardwerkzeugen wie Doors hinterlegt und konnten gemeinsam und transparent mit den technischen Spezifikationen getestet werden. Das Sicherheitskonzept lässt sich komplett und transparent mit seinen Verlinkungen zum Systemmodell abbilden, 5.



DOWNLOAD DES BEITRAGS
www.ATZonline.de



READ THE ENGLISH E-MAGAZINE
order your test issue now:
SAM-service@springer.com