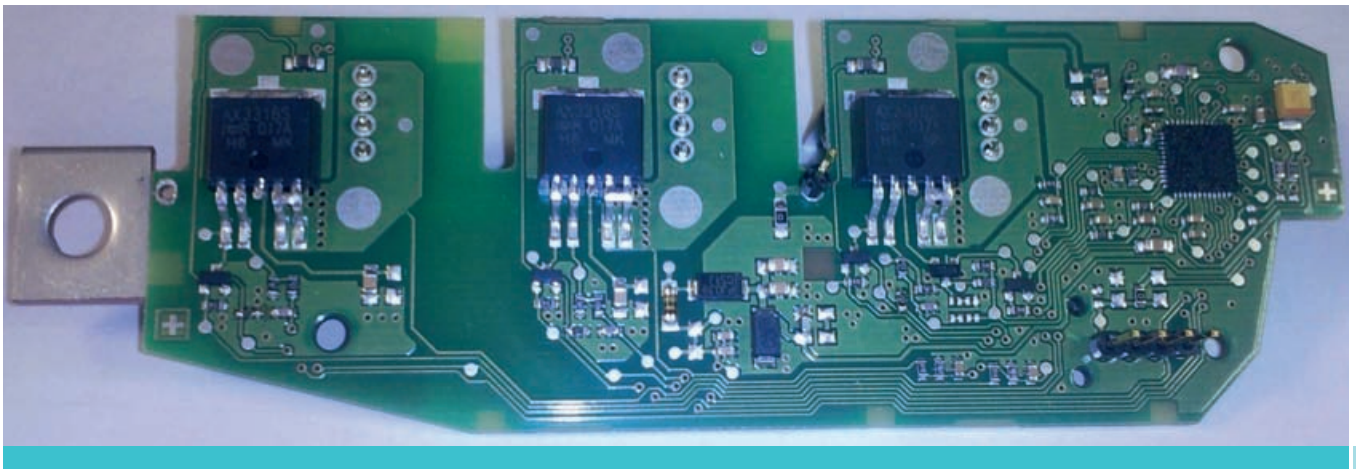
Robuste eingebettete Systeme

Die Entwicklung intelligenter Automobile leistet einen entscheidenden Beitrag zur Energieeffizienz, zur weiteren Steigerung der Verkehrssicherheit und zur Aufrechterhaltung des Verkehrsflusses bei steigender Verkehrsdichte. Die Implementierung intelligenten Verhaltens erfordert die Erhebung, Verarbeitung und Übertragung einer großen Menge an Informationen im laufenden Betrieb des Fahrzeugs. Dazu sind leistungsfähige elektronische Systeme erforderlich, die in das Gesamtsystem Automobil integriert sind, so genannte eingebettete Systeme.

Für unsere Gesellschaft ist Mobilität ein wichtiger Faktor der Lebensqualität. Das Automobil – Synonym für Mobilität – wird in den nächsten zehn Jahren einen grundlegenden Wandel erfahren:

- Der klassische Verbrennungsmotor steht vor der Ablösung durch intelligente, hybride oder rein elektrische Antriebe, um Anforderungen der Umweltverträglichkeit zu erfüllen. Die Aufgabe der intelligenten Steuerung dieser Antriebe ist es, im Spannungsfeld zwischen Reichweite, Batterielebensdauer und Umweltbelastung optimale Abwägungen zu treffen.
- Passive Sicherheitssysteme zur Minderung von Unfallfolgen werden zunehmend durch aktive Systeme ergänzt, die in der Lage sind, kritische Situationen zu erkennen und Fahrer bei der Unfallvermeidung zu unterstützen. Dazu ist es erforderlich, durch bildgebende Verfahren gewonnene Informationen äußerst schnell aufzubereiten und automatisch bezüglich der Verkehrssituation zu bewerten.
- Dem wegen wachsenden Verkehrsaufkommens drohenden Verkehrskollaps soll durch eine bessere Koordination des Verkehrsflusses begegnet werden. Zu diesem Zweck werden Automobile die Fähigkeit



01

Beispiel eines eingebetteten Systems im Automobil: LIN (Local Interconnect Network) Modul zur Kommunikation mit intelligenten Sensoren und Aktuatoren.

erhalten, sich untereinander und mit der Verkehrsinfrastruktur, z.B. mit intelligenten Ampeln, zu vernetzen, Informationen auszutauschen und sie zu bewerten, um durch kooperatives Verhalten Verzögerungen und Risiken zu reduzieren.

Alle diese Aufgaben der Steuerung, Regelung und Informationsverarbeitung werden durch so genannte *eingebettete Systeme* übernommen. Darunter versteht man aus Hardware- und Softwarekomponenten bestehende elektronische Systeme, die feste Aufgaben innerhalb größerer technischer Systeme übernehmen, in diesem Falle innerhalb des Automobils.

1. Rahmenbedingungen

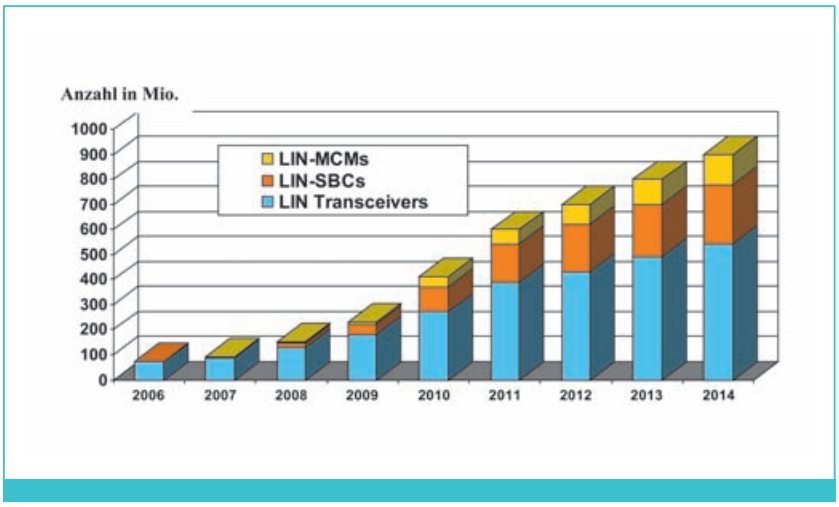
Bereits heute haben eingebettete Systeme entscheidenden Anteil an vielen Aspekten von Automobilen. In einem typischen Mittelklassemodell finden sich leicht über 50 solcher Steuergeräte; in der Oberklasse können es bis zu 100 sein. Ihr Anteil am Wert eines Fahrzeugs beträgt bis zu 30 Prozent. Sie übernehmen Aufgaben auf den Gebieten Sicherheit (Airbagsteuerung, ABS, ESP), Komfort (Klimaautomatik, Navigation), Kommunikation (Radio, Multimedia, Telefon) und Energieeffizienz (Motorsteuerung). Aber auch Fensterheber und Zentralverriegelung, Beleuchtungssystem und Blinker sowie durch Regensensoren gesteuerte Scheibenwischer sind ohne eingebettete Systeme nicht (mehr) denkbar.

Verstärkt erfolgt auch die Produktdifferenzierung unterschiedlicher Modelle oder Marken durch eingebettete Systeme. Die Möglichkeiten, die schon sehr ausgereifte Mechanik weiter zu verbessern, sind begrenzt und kostspielig. Häufig ergibt sich durch die elektronische Steuerung, z.B. von Motoren und Automatikgetrieben, ein wesentlich größeres Verbesserungspotential. Aufgrund von Plattformstrategien und Kooperationen der Fahrzeughersteller ist es auch nicht selten, dass der gleiche Antriebsstrang in verschiedenen Modellen hier um 20 Kilowatt stärker, dort um einige Zehntelliter sparsamer ausgelegt ist. Diese Differenzierung wird durch unterschiedliche Programmierung der eingebetteten Steuerung erreicht.

SUMMARY

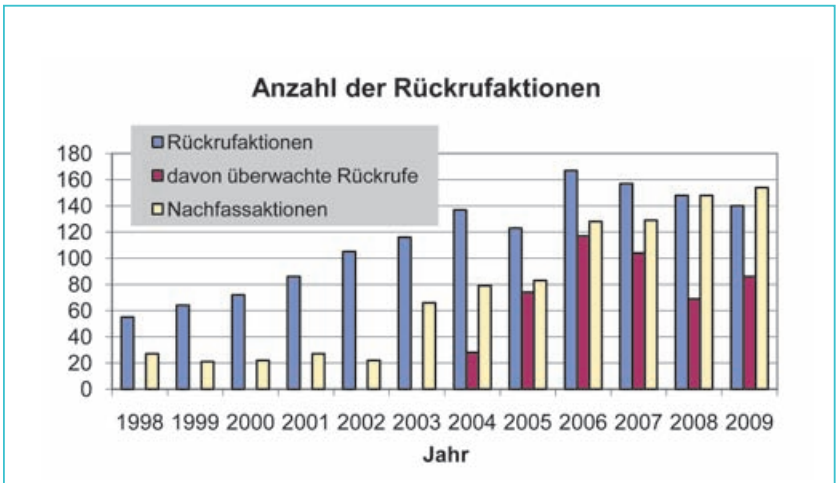
In Fahrzeugen werden zahlreiche sicherheitskritische Aufgaben, deren Ausfall oder Fehlfunktion vermieden werden muss, von eingebetteten Systemen übernommen. Diese werden im Automobil unter ungünstigen Bedingungen wie z.B. hohen Temperaturen betrieben, die den Alterungsprozess der Systeme beschleunigen können. Zudem erfordern gerade die neuen intelligenten Funktionen vermehrt die Nutzung hoch integrierter Schaltungen, die für Umgebungseinflüsse und Alterung besonders anfällig sind. Das Institut für Technische Informatik erforscht Systemarchitekturen und Entwurfsmethoden, die es erlauben, solche Systeme robust auszulegen, so dass ihre Funktionalität selbst unter ungünstigen Bedingungen und bei Auftreten interner Fehler und Defekte noch gewährleistet werden kann.

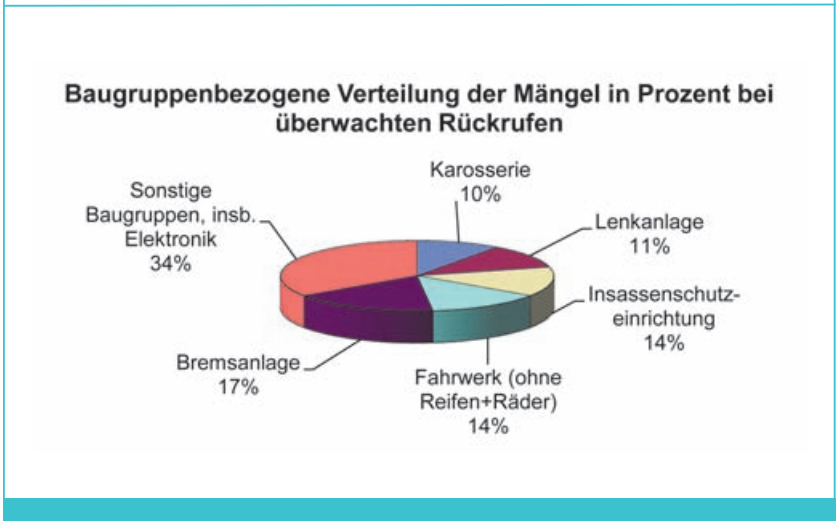
Within this decade, intelligent cars will make essential contributions to increasing energy efficiency, advancing transportation safety, and avoiding traffic congestion. Intelligence stems from capturing, processing, and transmitting large amounts of information while the car is being used. This requires high-performance electronic systems to be integrated into the automobile, known as embedded systems. Since such systems perform many safety-critical tasks, any malfunction or failure is a potential risk that must be avoided. However, operating conditions are harsh. For example, high temperatures pertinent in the engine compartment accelerate the aging process that integrated circuits are subject to. Moreover, implementing intelligence requires use of highly miniaturized devices which are especially prone to enviromental influences and aging. The Institute of Computer Architecture and Computer Engineering (Institut für Technische Informatik, ITI) researches system architectures and design methods for robust embedded systems that maintain essential functionality even under stress, occurrence of internal errors, and emergence of defects in the field.



02

Bedeutung eingebetteter Systeme am Beispiel des prognostizierten Wachstums im Bereich LIN (Local Interconnect Network).





03

Anzahl von Rückrufen und deren produktbezogene Aufteilung (Quelle: KBA Bericht 2009).

Automobilhersteller und Zulieferer stehen aufgrund der zunehmenden Durchdringung des Automobils durch eingebettete Systeme vor der Herausforderung, die Risiken bezüglich der Betriebssicherheit ihrer Produkte zu beherrschen. Während Verbraucher offensichtlich bereit sind zu akzeptieren, dass ihre Mobiltelefone und Laptops von Zeit zu Zeit „abstürzen“, erfordern Fehlfunktionen der Automobilelektronik kostspielige Rückrufaktionen, um die Sicherheit im Straßenverkehr zu garantieren. Es ist letztlich im Interesse aller Beteiligten, dass Fehler bereits beim Entwurf eingebetteter Systeme ausgeschlossen werden, um Kosten und Risiken gering zu halten. Dabei muss zwischen zwei Arten von Fehlern, logischen und physikalischen, unterschieden werden.

2. Fehler in eingebetteten Systemen

Logische Fehler oder *Entwurfsfehler* entstehen im Entwurfsprozess eingebetteter Systeme. Schon die Spezifikation, die die gewünschte Funktionalität festlegt, kann fehlerhaft sein. In allen weiteren Entwurfsphasen, bei der Implementierung von Hardwarekomponenten ebenso wie bei der Softwareprogrammierung, können Fehler nie gänzlich ausgeschlossen werden. Es mag so erscheinen, dass diese vor allem durch das Versagen der in der Entwicklung Tätigen entstehen. Tatsächlich besteht aber eine grundlegende Erkenntnis der Berechenbarkeitstheorie darin, dass es kein allgemein gültiges Verfahren gibt, mit dem die Frage zu beantworten wäre, ob beispielsweise ein Softwareprogramm richtig funktioniert.

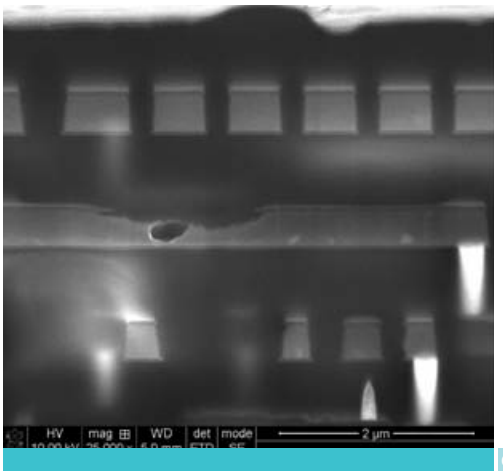
Natürlich lassen sich Entwicklungsingenieure von einer solchen Aussage nicht entmutigen. Im Speziellen, also für eingegrenzte Probleme, ist es unter Einsatz guter Ideen und großer Arbeitskraft durchaus möglich, durch Anwendungen teilweise automatisierter Beweistechniken eine mathematisch fundierte Überprüfung sicherheitskritischer Eigenschaften durchzuführen. In anderen Fällen kann mit Hilfe umfangreicher Simulationen und Tests das Vorhandensein logischer Fehler mit hinreichend großer Wahrscheinlichkeit ausgeschlossen werden.

Eine neue Herausforderung zeichnet sich momentan auf dem Gebiet der *physikalischen Fehler* ab. Traditionell wird für die Fertigung eingebetteter Systeme im Auto-

mobilbereich auf sehr robuste, langjährig erprobte Technologien zurückgegriffen. Dies gilt z.B. für Gehäuse, die die empfindliche Elektronik vor Schmutz und Feuchtigkeit schützen, insbesondere aber auch für die integrierten mikroelektronischen Schaltungen („Chips"), die in solchen Geräten eingesetzt werden und dabei hohen Beanspruchungen, etwa durch Umgebungstemperatur und Vibrationen, ausgesetzt sind. Durch großzügig ausgelegte Strukturen konnten bislang solche Einflüsse toleriert werden.

Allerdings erfordert der Trend, immer mehr und immer komplexere Funktionalität in eingebettete Systeme zu „verpacken", deren zunehmende Miniaturisierung bei gleichzeitig geringerer Stromaufnahme. Schon heute findet sich kaum Platz im Automobil, um noch weitere Steuergeräte unterzubringen. Deshalb ist es erforderlich, mehr Funktionalität in weniger Geräten zu integrieren. In Verbindung mit der Notwendigkeit höchster Rechenleistung für intelligente Funktionen im Automobil der Zukunft ist absehbar, dass auch der Automobilsektor verstärkt auf höchstintegrierte Schaltungen zurückgreifen muss, in denen einzelne Bauelemente wie Leiterbahnen und Transistoren nur noch wenige hundert Atomdurchmesser breit sind. Noch fragiler sind die in Transistoren erforderlichen Isolationsschichten, welche lediglich eine Dicke von wenigen Dutzend Atomen aufweisen und dadurch zunehmend die Ausbildung von Leckströmen sowie die Entstehung von Durchbrucheffekten und Leitbahnfehlern begünstigen.

Diese Strukturen sind für mehrere Mechanismen der Fehlerentstehung anfällig. Schon bei der Fertigung von Chips mittels eines photolithographischen Verfahrens treten Abweichungen auf, die mit zunehmender Miniaturisierung immer mehr ins Gewicht fallen. Im Betrieb unter harschen Umgebungsbedingungen können durch hohe Stromstärken, hohe Temperaturen, Spannungsspitzen und Einschläge natürlicher Umgebungsstrahlung zusätzliche vorübergehende oder dauerhafte Fehler entstehen. Heute werden defektbehaftete Chips nach der Fertigung in immer aufwändigeren Testverfahren identifiziert und aussortiert. Um trotz steigenden Fehleraufkommens weiterhin eine wirtschaftlich vertretbare Fertigungsausbeute zu erzielen, wird es in Zukunft erforderlich sein, Fehler zu tolerieren. Dies kann z.B. durch den Einbau von „Ersatzteilen" für defekte Elemente geschehen. Solche Verfahren werden bereits in Speicherchips oder redundant ausgelegten CPU-Cores (Cell Processor) angewandt. Darüber hinaus müssen wir auch lernen, mit Fehlern umzugehen, die während des Betriebs auftreten, wobei die Sicherheit des Fahrzeugs stets gewährleistet sein muss und Reparaturaufwand nach Möglichkeit zu vermeiden ist oder nur in relativ großen zeitlichen Abständen, beispielsweise bei der Kfz-Service-Inspektion, erfolgen darf.



04

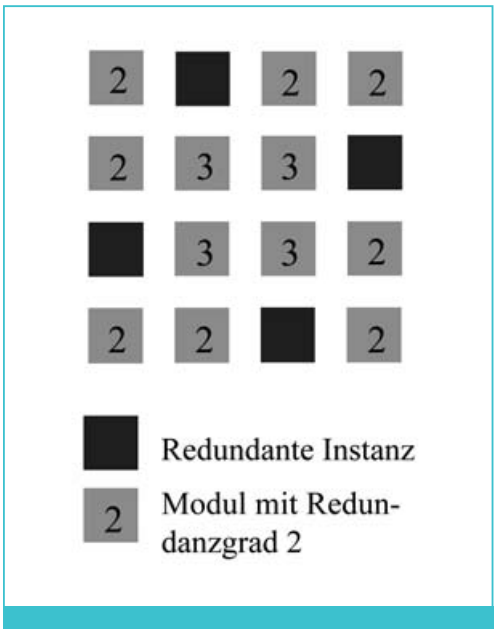
Leitbahnfehler, sichtbar gemacht durch physikalische Analytik.

In diesen Zusammenhang passt eine Schlagzeile, die vor einiger Zeit durch die Presse ging: „Oldtimer sterben aus! – Elektroniktod statt Rosttod?" Gemeint ist, dass die Lebensdauer von Fahrzeugen mehr und mehr durch die Elektronik begrenzt wird. Für ein verrostetes Blechteil oder eine defekte mechanische Komponente kann, wenn Originalersatzteile nicht mehr verfügbar sind, immer noch maßgefertigter Ersatz hergestellt werden. Letzteres ist für elektronische Komponenten aufgrund des enormen Aufwands für Entwicklung und Fertigung und wegen der Außerdienststellung der ursprünglich eingesetzten Fertigungstechnologien nicht mehr möglich. Umso wichtiger wird es, eine gute Bevorratung mit elektronischen Ersatzteilen zu gewährleisten. Jedoch ist zu bedenken, dass elektronische Komponenten bereits dann altern, wenn sie nur gelagert werden, wenn auch weniger schnell als im Betrieb.

Physikalische Fehler können also während der Fertigung, im Betrieb und selbst während der Lagerung entstehen. Ökonomische Gründe und Sicherheitsanforderungen machen es notwendig, eingebettete Systeme so zu entwerfen, dass die Systemfunktionalität auch bei begrenztem Auftreten solcher Fehler noch gewährleistet ist.

3. Robuste Auslegung eingebetteter Systeme

Eine klassische Technik hierfür ist die *n*-fache modulare Redundanz. Hierbei wird jedes Systemmodul mehrfach (*n* mal) eingebaut. Ein zusätzliches Entscheidungsmodul vergleicht die Ausgaben der *n* Instanzen und



05

Verbesserte redundante Anordnung.

wählt die von einer Mehrheit der Module vorgeschlagene Ausgabe aus. Bei dreifacher Redundanz kann somit eine Instanz ausfallen. Für die Flugtüchtigkeit unverzichtbare Rechensysteme in Flugzeugen sind sogar fünffach redundant ausgelegt; damit können zwei Ausfälle toleriert werden. Trotz durchaus erfolgreicher Anwendungen weist diese Technik Schwachpunkte auf. In einem Verkehrsflugzeug im Wert von einigen hundert Millionen Euro mögen die Kosten redundanter elektronischer Systeme von untergeordneter Bedeutung sein. Der Automobilsektor ist hingegen stark kostengetrieben, und in Verhandlungen über die Lieferung eingebetteter Systeme geht es bei den Stückpreisen oft um Centbeträge. Es ist kaum realisierbar, jedes Modul mehrfach einzubauen. Zudem besteht bei der Integration redundanter Instanzen auf dem gleichen Chip die Gefahr, dass ein Fehler gleich mehrere Instanzen betrifft. Und schließlich ist in jedem Fall das Entscheidungsmodul ein kritisches Element, das besonders robust ausgelegt werden muss, da sein Ausfall nicht kompensiert werden kann.

Es gibt eine Vielzahl anderer Ansätze, eingebettete Systeme so zu gestalten, dass die Unzuverlässigkeit einzelner Teile toleriert werden kann. So können z.B. die Komponenten beim Einschalten bzw. im Betrieb einem gezielten Test unterzogen werden, wodurch fehlerbehaftete Komponenten genau identifiziert und bezüglich des Gesamtsystems isoliert werden können. Damit kann eine höhere Verlässlichkeit gesichert werden als durch die bloße Annahme, dass eine Mehrzahl von Modulen schon richtig arbeiten wird. Dieser Test kann mit Verfahren des Selbsttestens oder durch gegenseitiges Testen effizient implementiert werden. Solche Arbeiten sind schon seit längerem Gegenstand der Forschung am Institut für Technische Informatik [4].

Ein ergänzender Ansatz besteht darin, redundante Instanzen als Ersatz für mehrere andere Module vorzusehen, während sie bei *n*-fach modularer Redundanz nur je einem einzelnen Modul zugeordnet sind. Bei geschickter Anordnung kann dabei ein hoher Redundanzgrad bei vergleichbar geringerem Zusatzaufwand erzielt werden. Ein Beispiel ist in **05** dargestellt. Redundante Instanzen sind mit dunklen Quadraten dargestellt. Jedes andere Modul hat genau eine redundante Instanz in direkter Nachbarschaft. Der Redundanzgrad, wenn eine zwei horizontale oder vertikale Schritte entfernte redundante Instanz für ein fehlerhaftes Modul einspringen kann, ist jeweils mit Zahlen dargestellt. Jedes Modul hat wenigstens zwei redundante Instanzen in Reichweite von zwei Schritten, vergleichbar mit dem dreifach modularen Ansatz. Während letzterer ein Verhältnis redundanter Instanzen zu den restlichen Modulen von 2:1 (200 Prozent Zusatzkosten) aufweist, ist dieses mit 4:12 (33 Prozent Zusatzkosten) für die in **05** gezeigte Lösung deutlich günstiger.

Als Ergebnis unserer Untersuchungen können wir für beliebige Anordnungen und Nachbarschaftsbeziehungen von Modulen eine Platzierung redundanter Instanzen bestimmen, die einen vorgegebenen Redundanzgrad mit minimalem Zusatzaufwand erreicht oder aber bei vorgegebenem Aufwand den Redundanzgrad maximiert.

Bei genauem Hinsehen wird jedoch deutlich, dass der geringere Kostenaufwand in unserem Beispiel dadurch erkauft wird, dass eine redundante Instanz im ungünstigen Fall die Aufgaben mehrerer fehlerbehafteter Module übernehmen muss. Ist das der Fall, so kann es sein, dass die Leistungsfähigkeit der redundanten Instanz überstrapaziert wird und deshalb die Leistung des Gesamtsystems zurückgeht. Um dies zu vermeiden, kann die redundante Instanz mit einer höheren Frequenz betrieben werden, was allerdings den Energieverbrauch steigert. Performanzverlust oder erhöhte Energieaufnahme können in vielen Fällen bis zu einem gewissen Grad akzeptabel sein, sofern die sicherheitsrelevante Funktionalität aufrecht erhalten wird.

Diese Überlegungen sollen verdeutlichen, dass viele Kriterien abzuwägen sind, um die Funktion eines eingebetteten Systems auch unter ungünstigen Umständen, die zum Auftreten von Fehlern führen, aufrecht zu erhalten. Gelingt dies, so spricht man in der Praxis häufig davon, das entworfene System sei robust. Robustheit ist dabei ein qualitativer Begriff. Wir streben an, diesen Begriff quantitativ zu erfassen, also „messbar“ zu machen, so dass die

Robustheit während des Entwurfs eingebetteter Systeme gezielt optimiert werden kann.

4. Quantitativer Robustheitsbegriff

In vielen technischen Zusammenhängen und auch in alltäglichen Lebenssituationen wird der Begriff Robustheit gebraucht, ohne dass es eine formale oder gar quantifizierbare Definition gäbe. Das kann zu Verwirrung oder begrifflicher Redundanz führen, wie zum Beispiel in der nicht selten gehörten Aussage „Robust ist, wenn die Mean Time To Failure hoch ist“. Hier wird Robustheit implizit mit Zuverlässigkeit identifiziert.

Ein Beispiel aus dem Alltag zeigt dagegen, dass Robustheit und Zuverlässigkeit verwandte, aber zu unterscheidende Eigenschaften sind: Leidet ein Mensch bei den für uns normalen Lebensbedingungen lediglich einmal im Jahr an einer leichten Erkrankung, etwa einer Erkältung, kann man zu Recht sagen, dass der Körper zuverlässig arbeitet und die Person mit einer verlässlichen Gesundheit ausgestattet ist. Doch genügt das, um jemandem eine robuste Gesundheit zu bescheinigen? Nein; im üblichen Sprachgebrauch erfreut sich eine Person einer robusten Gesundheit, wenn sie auch unter ungewöhnlichen Bedingungen, etwa bei fortwährender Arbeit im Freien bei schlechtem Wetter, bei Aufenthalt in extremen Klimazonen oder unter schlechten hygienischen Umständen, nicht ernsthaft erkrankt.

Diese Auffassung von Robustheit spiegelt sich auch in folgender enzyklopädischer Definition wider: „Robustheit (lat. robustus, von robur: Hart-, Eichenholz) ist die Fähigkeit eines Systems, seine Funktion auch bei Schwankungen der Umgebungsbedingungen aufrecht zu erhalten. Meist ist es sinnvoll anzugeben, wogegen das System robust ist (z.B. gegen Änderung der Umgebungstemperatur oder gegen Fehlbedienung)“ [1]. Auf verschiedenen mathematisch-technischen Gebieten, etwa der Regelungstechnik, der Algorithmik und der Statistik, gibt es spezialisierte Varianten dieses qualitativen Robustheitsbegriffes.

Übertragen auf das Gebiet der Automobilelektronik und Elektromobilität, in dem die zunächst angestrebten Anwendungen des Projekts ROBUST liegen, bedeutet dies: Ein Fahrzeug, das während der üblichen erwarteten Lebensdauer von etwa 13 Jahren bei normaler Nutzung ohne größere Reparaturen funktioniert, ist zuverlässig. Robustheit hingegen liegt vor, wenn das Fahrzeug auch unter verschärften Bedingungen oder aber für eine über das Übliche hinausgehende Zeit die erwarteten Eigenschaften aufweist.

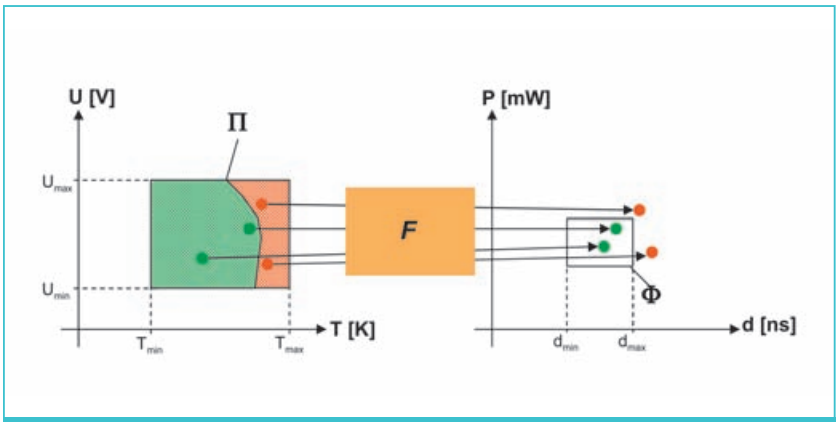
Um den Robustheitsbegriff stärker formalisieren und Robustheit quantifizieren zu können, ist es erforderlich, die erwarteten Eigenschaften genau zu erfassen. Im einfachsten Fall handelt es sich dabei lediglich um die Unterscheidung „funktioniert“ oder „funktioniert nicht“. Im Allgemeinen ist hingegen zu erwarten, dass viele weitere Eigenschaften von einem System erfüllt werden müssen, z.B. die oben angeführten Kriterien einer minimal zu garantierenden Performanz und eines maximal akzeptablen Energieverbrauchs. Handelt es sich um n Eigenschaften, so spannen diese einen n-dimensionalen Raum auf. In jeder Dimension können die zulässigen Wertebereiche der Eigenschaftsgröße spezifiziert werden. Aus dem kartesischen Produkt dieser Bereiche ergibt sich das Teilgebiet des Eigenschaftsraums, in dem das System wie gewünscht funktioniert. Durch Angabe eines nicht-orthogonalen Gebiets können auch Abhängigkeiten zwischen den Eigenschaften erfasst werden.

In Analogie zu den erwarteten Eigenschaften müssen auch die normalen Betriebsbedingungen erfasst werden. Im Automobilbereich sind diese durch so genannte „Mission Profiles“ spezifiziert, welche Ober- bzw. Untergrenzen für die als üblich angenommene Beanspruchung eines Automobils und seiner nanoelektronischen Subsysteme vorgeben. Jede dafür relevante Einflussgröße kann als eine Dimension eines m-dimensionalen Raums der Stör-

Projekt ROBUST

Das Projekt ROBUST erforscht neue Methoden und Verfahren zum Entwurf robuster eingebetteter Systeme und konzentriert sich dabei auf die besonders kritischen nanoelektronischen Komponenten. Hierzu werden erstmals Maße zur Quantifizierung der Robustheit definiert. Diese Maße werden mit Hilfe zu abstrahierender Robustheitsmodelle und unter Anwendung neuer Robustheitsanalyseverfahren für die Systemebene ermittelt. Die Robustheitsmaße werden eingesetzt, um beim Entwurf statische und dynamische Optimierungen der Robustheit gezielt durchzuführen und zu bewerten. Als Ergebnisse entstehen neue Methoden und prototypische Werkzeuge, welche im Rahmen eines Top-Down-Systementwurfs nanoelektronischer Systeme die Robustheit bereits in frühen Entwurfsphasen berücksichtigen. Die Methoden und Prototypen werden durch Anwendung auf ein Demonstrator-Design evaluiert und den industriellen Projektpartnern für weiterführende Arbeiten zur Integration in ihren Entwurfsprozess zur Verfügung gestellt.

Neben dem Institut für Technische Informatik sind Arbeitsgruppen aus Frankfurt, Hannover, Karlsruhe, München und Oldenburg an ROBUST beteiligt. Das Projekt wird als Clusterforschungsprojekt vom Bundesministerium für Bildung und Forschung gefördert und durch die im edacentrum e.V. engagierten Unternehmen kofinanziert.

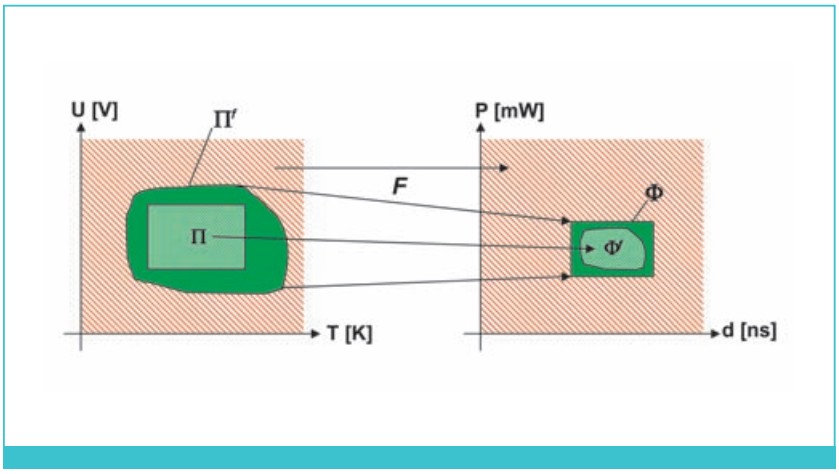


06

Abbildung der Störeinflüsse (links) in den Eigenschaftsraum (rechts) durch ein nicht-robustes System F.

einflüsse erfasst werden. Durch Angabe eines Teilgebiets dieses Raumes wird ein Mission Profile festgelegt.

06 zeigt auf der linken Seite als Beispiel für Störeinflüsse die Umgebungstemperatur *T* sowie eine Schwankungsbreite der Versorgungsspannung *U*. Als normal aufgefasste Werte sind durch das Gebiet Π angegeben. Auf der rechten Seite sind als einzuhaltende Eigenschaften die Leistungsaufnahme *P* sowie die Verzögerung (Latenz) *d* erfasst. Ein System *F* ist nun durch eine Abbildung charakterisiert, die angibt, wie die Störeinflüsse die Systemeigenschaften beeinflussen. Die klassische Methode zur Bestimmung dieser Abbildung ist der Test von Systemprototypen unter verschiedenen Umgebungsbedingungen. Im Projekt ROBUST wird angestrebt, durch Analyse- und Simulationsverfahren eine entsprechende Bewertung bereits in frühen Entwurfsphasen zu ermöglichen.



07

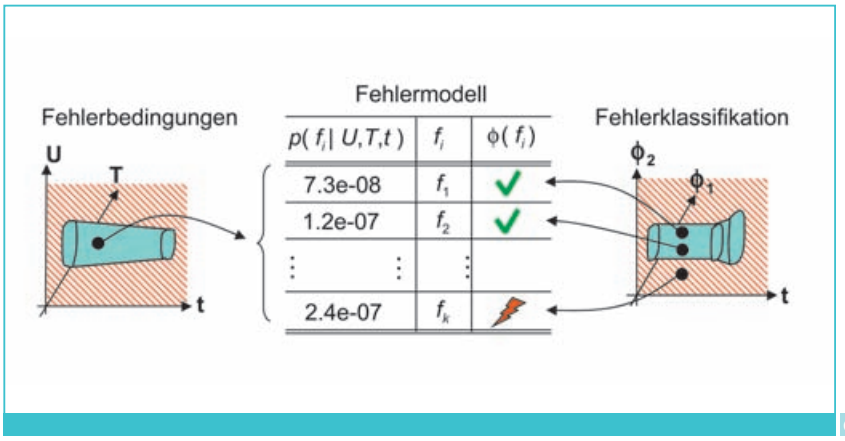
Ein robustes System F toleriert Störeinflüsse, die das Mission Profile übersteigen.

Ein System, das wie in **06** dargestellt schon für einige „Arbeitspunkte" innerhalb des Mission Profile die spezifizierten Eigenschaften verletzt, ist nicht als robust zu bezeichnen. Nur wenn im Normalbetrieb alle Eigenschaften erfüllt sind, kann durch Tolerieren von Störeinflüssen, die über das Normale hinaus gehen, Robustheit geschaffen werden, wie in **07** dargestellt: Über das Gebiet Π hinaus werden auch alle im Gebiet Π*f* liegenden Störeinflüsse in akzeptable Eigenschaften abgebildet. Alternativ lässt sich Robustheit im Eigenschaftsraum dadurch erkennen, dass bei normalen Störeinflüssen die entstehenden Eigenschaften Φ*f* einen Spielraum zu den Grenzen des Gebiets Φ aufweisen, so dass auch mit noch stärkeren Störungen umgegangen werden könnte. Nur in den rot dargestellten Gebieten führen die Störeinflüsse zu Eigenschaftsverletzungen.

Zwecks Bewertung der Robustheit wird im Handbuch für Robustheitsvalidierung [2] der Sicherheitsabstand zwischen dem Mission Profile Π und dem als Safe Operating Area bezeichneten Gebiet Π*f* herangezogen. Dieser Abstand lässt sich jedoch nur für einzelne Dimensionen bestimmen; eine Abstandsmetrik, die Größen mit unterschiedlichen physikalischen Einheiten vermischt, wäre weder wohldefiniert noch sinnvoll interpretierbar. Um dennoch die verschiedenen Aspekte mit einem gemeinsamen Robustheitsmaß quantifizieren zu können, verfolgen wir den Ansatz, Robustheit als Wahrscheinlichkeit zu definieren.

Robustheit verstehen wir als die Wahrscheinlichkeit, dass ein System auch unter ungünstigen Störeinflüssen im Rahmen der spezifizierten Eigenschaften funktioniert. Dies kann auf solche Störeinflüsse bezogen werden, die das Mission Profile überschreiten; dann ist Robustheit die bedingte Wahrscheinlichkeit, dass die Eigenschaften eingehalten werden, wenn das System außerhalb des Mission Profile betrieben wird. Diese lässt sich im linken ebenso wie im rechten Diagramm in **07** bestimmen als Quotient der Wahrscheinlichkeit des dunkelgrünen Gebiets und der Wahrscheinlichkeit des Komplements des hellgrünen Gebiets. Eine begriffliche Variante verzichtet durch Annahme eines leeren Gebiets Π auf das Mission Profile und betrachtet die Funktionswahrscheinlichkeit des Systems unter allen möglichen Störeinflüssen. In der wahrscheinlichkeitsbasierten Definition spiegelt sich die begriffliche Nähe von

Robustheit und Zuverlässigkeit wider. Jedoch setzt Robustheit erst bei Überschreiten des Rahmens des normalen Betriebs ein, innerhalb dessen Zuverlässigkeit bewertet wird. Zudem erlaubt es unser Robustheitsbegriff, die betrachteten Störeinflüsse und Eigenschaften explizit anzugeben, wodurch festgelegt wird, wogegen und bezüglich welcher Eigenschaften ein System robust sein soll. Weitere Details zu dem hier nur grob vorgestellten Ansatz sowie zu verwandten Arbeiten sind in [3] verfügbar.



08

Schematische Übersicht der Robustheitsbewertung mittels Systemfehlersimulation und bedingungsorientiertem Fehlermodell.

5. Robustheitsanalyse

Neben der Koordination eines domänenübergreifenden Robustheitsbegriffs liegt ein weiterer Schwerpunkt der Arbeiten des Instituts für Technische Informatik auf der Untersuchung von Methoden und Verfahren zur Robustheitsanalyse durch Fehlersimulation digitaler Teile eines Systems. Diese Arbeiten ergänzen sich mit jenen anderer Projektpartner, die analoge Fehlersimulationen bearbeiteten. Sie werden integriert durch die Nutzung der Systemmodellierungsbibliothek *SystemC-AMS* als gemeinsame Basis sowie durch die angestrebte integrierte Robustheitsbewertung des Gesamtsystems. An den Berührungspunkten zwischen analogen und digitalen Komponenten sind zudem die unterschiedlichen Fehlerarten der beiden Welten ineinander zu übersetzen. Beispielsweise gilt jede graduelle Abweichung von einem Sollwert als Fehler in der analogen Welt. Eine solche Abweichung löst hingegen in der digitalen Welt nur dann einen Fehler aus, wenn sie einen bestimmten Schwellenwert überschreitet.

Im Zusammenhang mit dem zuvor beschriebenen Robustheitsmodell dient die Fehlersimulation dazu, die durch das System generierten Eigenschaften Φf bei unterschiedlichen Störeinflüssen zu bewerten. Sie stellt damit letztlich die Abbildung von dem Raum der Störeinflüsse in den Eigenschaftsraum her. Allerdings kann diese Abbildung nicht in einem einzigen Schritt berechnet bzw. simuliert werden, da im Falle digitaler Systemteile ein direkter Schluss von analogen Störgrößen auf das resultierende Verhalten aufgrund der gewollten Abstraktion digitaler Modelle von analogen Details nicht möglich ist. Stattdessen wird der Zusammenhang zwischen Störungen und Eigenschaften unter Nutzung des Konzepts bedingungsorientierter Fehlermodelle als Bindeglied hergestellt (siehe **08**). Ein solches Fehlermodell basiert zunächst auf einer Menge von Fehlern, die für das digitale Modell angenommen werden. Anstelle klassischer Fehlermodelle wie dem Stuck-At-Modell, das auf niedrigen, implementierungsnahen Ebenen gängig ist, können auf der Systemebene abstraktere Fehlermodelle eingesetzt werden. Die betrachteten Simulationsverfahren werden diesbezüglich flexibel ausgelegt, so dass Fehlermodelle austauschbar sind.

Der „bedingungsorientierte“ Anteil eines Fehlermodells beschreibt, wie wahrscheinlich das Auftreten eines Fehlers bei vorgegebenem Fehlermechanismus f_i und zugehörigen Parametern wie Spannung U, Temperatur T und Alter t ist. Auf diese Weise wird eine Verbindung zum Raum der Störeinflüsse hergestellt. Die parameterabhängigen Wahrscheinlichkeiten müssen zu diesem Zweck für unterschiedliche Systemkomponenten individuell charakterisiert werden. Diese Charakterisierung wird in Zusammenarbeit mit anderen Projektpartnern vorgenommen. Hier fließen wiederum Informationen über die Stressbelastung der Komponenten im Systembetrieb ein, welche durch die Systemsimulation ermittelt werden.

Um nun die Robustheit eines Systems zu bestimmen, wird dieses zunächst mit Fehlern simuliert, wobei die Fehler bezüglich ihrer Auswirkungen klassifiziert werden. Dabei geht es vor allem darum, zu bestimmen, ob das Auftreten eines Fehlers zu einer Verletzung spezifizierter Eigenschaften Φ führt. Dieser Schritt ist aufwändig, da er systematisch für alle Fehler durchgeführt werden muss. Dies ist aber

bei gegebenem System nur einmal erforderlich. In einem zweiten Schritt werden die Fehler mit ihrer charakterisierten Auftretenswahrscheinlichkeit p bei unterschiedlichen Störeinflüssen (im Beispiel der **08**: U, T und t) bewertet. Durch Summation wird die Wahrscheinlichkeit einer Eigenschaftsverletzung bestimmt, womit wie zuvor beschrieben die Robustheit berechnet werden kann. •

Martin Radetzki und Thomas Hötzel

Literatur

[1] Wikipedia, „Robustheit“, online: http://de.wikipedia.org/wiki/Robustheit, 15.10.2010.

[2] SAE International Standard J1879, „Handbook for Robustness Validation of Semiconductor Devices in Automotive Applications“, April 2007.

[3] Radetzki, M., Bringmann, O., Nebel, W., Olbrich, M., Salfelder, F., Schlichtmann, U., „Robustheit nanoelektronischer Schaltungen und Systeme“, in: Zuverlässigkeit und Entwurf, 4. GMM/GI/ITG-Fachtagung vom 13.-15. September 2010 in Wildbad Kreuth, VDE-Verlag, 2010.

[4] Bertsche, B., Göhner, P., Jensen, U., Schinköthe, W., Wunderlich, H.-J., „Zuverlässigkeit mechatronischer Systeme“, Springer, 2009.

DIE AUTOREN

Prof. Dr.-Ing. Martin Radetzki

studierte an der Universität Oldenburg Informatik und Physik und promovierte dort im Fach Technische Informatik über die „Synthese digitaler Schaltungen aus objektorientierten Spezifikationen“. Von 2000 bis 2005 war er bei der sci-worx GmbH sowie der edacentrum GmbH in Hannover tätig. Seit 2005 leitet er die Abteilung Eingebettete Systeme am Institut für Technische Informatik der Universität Stuttgart.

Dr.-Ing. Thomas Hötzel

ist seit 2010 Geschäftsführer der Atmel Automotive GmbH und leitet dort die Entwicklung der Business Unit RF & Automotive. Er hat langjährige Erfahrung im Bereich Halbleiter-Innovationsmanagement und ist Experte für sämtliche Geschäfts- und Entwicklungsprozesse – von der strategischen Planung bis hin zur Massenproduktion. Thomas Hötzel studierte Elektroniktechnik an der Technischen Universität Braunschweig mit Schwerpunkt Multimedia. Seit 1989 war er bei Philips Semiconductors (heute NXP) tätig, danach von 2000 bis 2005 als COO bei der sci-worx GmbH Hannover, einer Tochterfirma der Infineon Technologies AG. 2005 folgte der Wechsel zur ZMD AG, Dresden, dort war er bis 2009 für die Produktentwicklung verantwortlich und als CTO Mitglied des ZMD-Vorstands. 2005 bis 2009 leitete er den Arbeitskreis IC-Design im Silicon Saxony Netzwerk, 2009 wurde er zum Mitglied des VDE/GMM-Beirats ernannt.

Kontakt

Institut für Technische Informatik, Abteilung Eingebettete Systeme
Universität Stuttgart, Pfaffenwaldring 47, 70569 Stuttgart
Tel. 0711/685-88270, Fax 0711/685-88286
E-Mail: martin.radetzki@informatik.uni-stuttgart.de, Internet: www.iti.uni-stuttgart.de