Unfallpotenziale durch verbesserte Steuergeräte reduzieren

Von Werner Damm

Ob im Auto, im Flugzeug oder im Zug: In zunehmendem Maße werden Steuer- und Regelungsaufgaben durch Software realisiert. In diesen Bereichen nimmt der Softwareanteil exponentiell zu; ebenso wächst die Komplexität der Steuerungssoftware. Um diese zu beherrschen, werden modellbasierte Prozesse eingeführt, für die das Informatik-Institut OFFIS Werkzeuge entwickelt, die frühzeitig Fehler erkennen können.

Beim Rückwärtsfahren ein unbeabsichtigter "Satz nach hinten" - ausgelöst durch fehlerhafte Elektronik: Hier setzen die Oldenburger InformatikerInnen an. Ziel ihrer Arbeit ist es, die an sich hilfreiche Elektronik (die in Form von Steuergeräten verpackt ist) so zu verbessern, dass diese nicht selbst Verursacher von Unfällen wird.

Number of Accidents are reduced by Electronic Control Units

Today, cars, trains and aircrafts all share a critical dependency on software hidden in so-called electronic control units. Both the exponential growth of control software and the rapidly increasing complexity of its functions in safety-critical applications call for rigorous validation methods supported by model-based processes, such as developed at OFFIS.

Sie sitzen in Ihrem neuen Wagen mit Automatikgetriebe, wollen beim Supermarkt rückwärts einparken - und der Wagen macht einen Satz nach hinten - unkontrolliert, sozusagen aus eigenem Antrieb. Zum Glück ist nichts passiert, aber wenn .... Nicht auszudenken, wenn etwa hinter Ihrem Wagen ein Kind gerade in diesem Augenblick vorbeigelaufen wäre. Nicht auszudenken, was passiert, wenn der Airbag ausgelöst würde, obwohl ein Kindersitz auf dem Beifahrersitz montiert ist, oder wenn Ihr Fahrzeug in hohen Geschwindigkeitsbereichen unkontrollierte Ausbrechreaktionen zeigen würde.

Solche und ähnliche Unfallpotenziale erinnern uns daran, dass unser "liebstes Kind" schon längst vollgestopft ist mit Elekronik, dass schon längst dem Fahrer mittels dieser Elektronik "unter die Arme gegriffen wird", um z. B. in Schleudersituationen besser zu reagieren, als es Autofahrer "normalerweise" tun.

Diese Elektronik ist verpackt in Form von sogenannten *Steuergeräten* - und davon gibt es - je nach Klasse und Ausstattungsgrad - viele: von etwa 20 in einfachen Fahrzeugen bis hin zu 60 in Oberklassefahrzeugen mit voller Ausstattung. Zwar wird in Zukunft nicht unbedingt die Anzahl dieser Steuergeräte wachsen, wohl aber deren Komplexität. Noch entscheidender ist, dass in zunehmendem Maße die Rollen zwischen Fahrer und Steuergeräten sich von einer heute noch vorhandenen Führerschaft des Fahrers zu einer Führerschaft des Fahrzeuges verschieben können. Die Technologie dazu - etwa zum autonomen Fahren - ist schon sehr weit gediehen, die technologische Basis mit voll elektronischen Bremsen und Lenksystemen schon vor der Markteinführung.

Wenn denn nun also die Elektronik derart stark in das Fahrverhalten eingreift, wie können wir uns absichern, dass sie "richtig" arbeitet, wie insbesondere vermeiden, dass die Elektronik selbst Verursacher von Unfällen wird?

Die Automobil- und Zulieferindustrie trifft eine Vielzahl von qualitätssichernden Maßnahmen, um mögliche Fehlverhalten von Steuergeräten nach dem Stand der Technik während Vorentwicklung, Entwicklung und

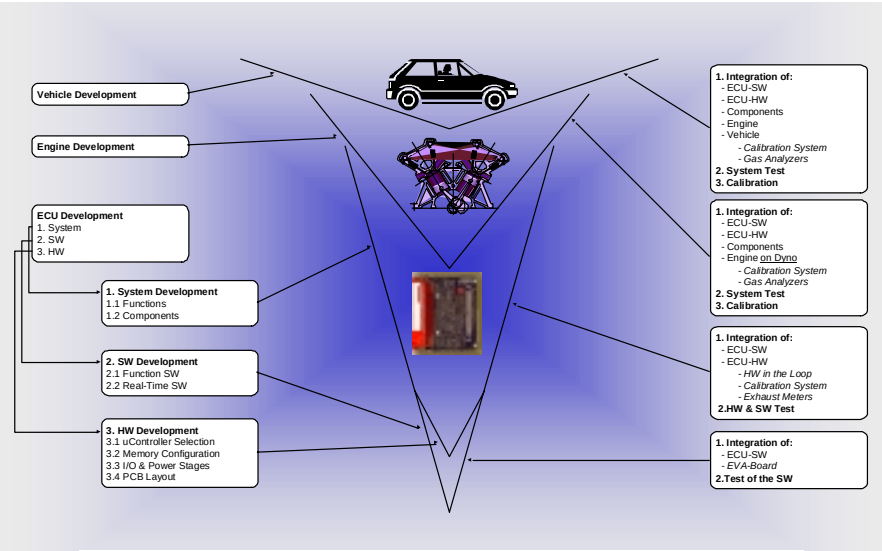
Produktion zu erkennen und zu eliminieren. Diesen Stand der Technik selbst voranzutreiben, insbesondere mit dazu beizutragen, dass Steuergeräte fehlerfrei arbeiten, ist ein vorrangiges Ziel der Forschungs- und Entwicklungsaktiväten im F&E Bereich Eingebettete Systeme von OFFIS (Oldenburger Forschungs- und Entwicklungs-Institut für Informatik-Werkzeuge und -Systeme; An-Institut der Universität Oldenburg). Als Teil der Verbesserungen wird von Seiten der Automobilindustrie zunehmend ein *modellbasierter* Entwurfsprozess für die Entwicklung von Steuergeräten eingesetzt. Dabei wird - im Vorfeld der eigentlichen Entwicklung des Steuergerätes - ein *Modell* der Steuerung erstellt, welches dann vielfältigen qualitätssichernden Schritten unterzogen werden kann. Im V-basierten Entwurfsprozess werden solche Modelle sowohl für die Systementwicklung wie auch für die Softwarespezifikation verwendet. Zur Unterstützung der Systementwicklung bieten kommerzielle Case Tools wie z.B. das STATEMATE System der Firma I-Logix die Möglichkeit, Teilkomponenten sowie den Informationsfluss zwischen Teilkomponenten und weiteren Fahrzeugkomponenten festzulegen (z.B. Sensoren zur Erfassung der Fahrzeugbeschleunigung sowie Aktuatoren zum Entriegeln einer Tür). Diese *Strukturansicht* wird ergänzt durch eine *Verhaltensansicht*, in der ausführbare Spezifikationen für die Teilfunktionen angegeben werden. Hierzu werden in STATEMATE eine auf David Harel's StateCharts aufbauende, automatenbasierte Realzeitprogrammiersprache eingesetzt.

Der entscheidende Vorteil eines solchen modellbasierten Prozesses liegt darin, dass damit bereits in einer frühen Phase eine vollständige Verhaltesspezifikation des Steuergerätes vorliegt. Dies erlaubt es dem Entwickler, durch animierte Simulation die gewünschten Funktionen abzusichern, automatisch für im Testfahrzeug integrierte leistungsfähige Rechernersysteme aus den Modellen Codes zu erzeugen und damit sogar während des Fahrbetriebs das nur als Modell beschriebene Steuergerät vollständig zu integrieren, oder aber sogar vollständige Steuergerätenetzwerke zu modellieren und deren Zusammenspiel auf Modellebene durch Simulation abzusichern. Im letzten Fall spricht man oft von *virtual integration V*, da - im Gegensatz zum "klassischen" V-Diagramm - hier nur eine virtuelle Integration von Steuergeräten auf Modellebene erfolgt.

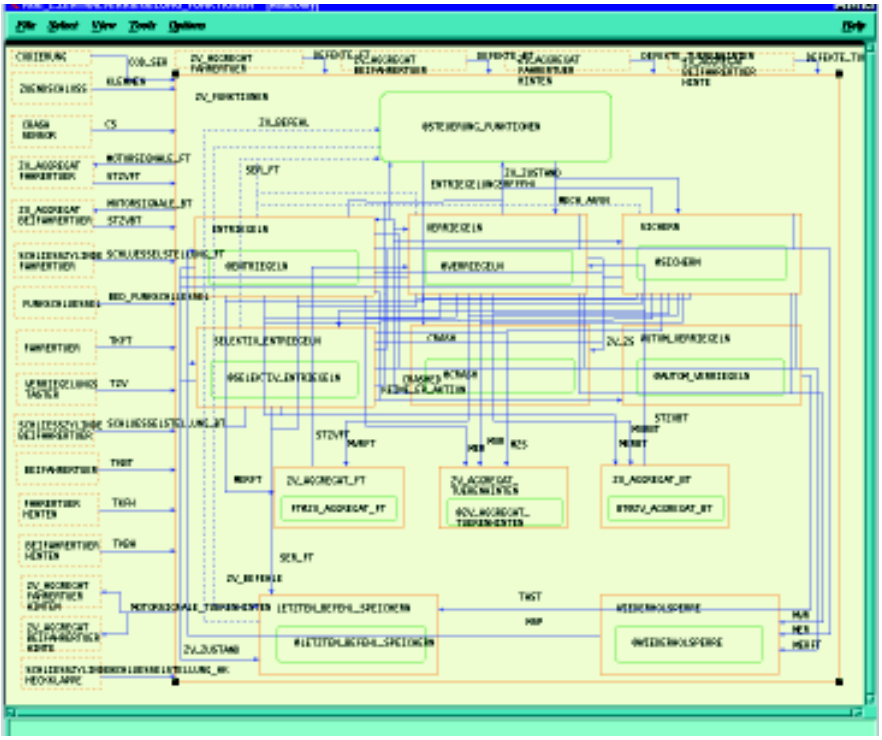
Diese Ausführungen machen erkennbar, welche signifikanten Qualitätsverbesserungen bereits durch einen solchen modellbasierten Prozess erzielbar sind. Dennoch können nach wie vor auch in einem solchen Prozess Fehler übersehen werden, da selbst vergleichsweise einfache Steuergeräte wie die im Bild gezeigte Zentralverriegelung eine extrem hohe Zahl von Zuständen annehmen können. Würde man etwa die Zentralverriegelung unmittelbar als Hardwareschaltung realisieren, also sowohl die dort verwendeten Daten wie auch sämtliche Zustände durch Bits repräsentieren, so würde ein endlicher Automat mit 300 Zustandsbits benötigt, der damit im Prinzip 2^{300} Zustände annehmen kann (dies entspricht größenordnungsmäßig einer 1 gefolgt von 90 Nullen). Dass in einem solchen System trotz umfangreicher Simulation noch Fehler versteckt sein können, ist naheliegend, und auch die oben dargestellten Probefahrten reichen nicht notwendigerweise aus, um die Vielzahl dieser Systemzustände sämtlich nachfahren zu können.

Während somit eine *Simulation* immer nur einzelne Verhalten eines Steuergerätes nachfahren kann, zielt eine (formale) *Verifikation* auf eine (mathematisch) *vollständige* Analyse eines Systems. Unter den vielfältigen Ansätzen haben sich - nicht zuletzt Dank bahnbrechender Arbeiten von Ed Clarke von der Carnegie Mellon Universität - sogenannte Modellprüfungsverfahren als vielversprechend herausgestellt. Mittels *symbolischer* Repräsentationen des Zustandsraums, die also auf eine explizite Aufzählung aller Zustände verzichten und statt dessen auf einer effizienten Kodierung der pro Zustandsbits geforderten Übergangsfunktionen arbeiten, konnten Größenordnungen erreicht werden, die etwa im Bereich von 300 Zustandsbits liegen. Diese "Laborergebnisse" in die industrielle Praxis zu bringen, also formale Verifikationstechniken in industrielle Entwurfsprozesse zu integrieren, stellte eine lockende Herausforderung für OFFIS dar. Die dabei zu lösenden Fragestellungen reichen von der Grundlagenforschung über die Entwicklung einer komplexen Softwarearchitektur bis hin zur detaillierten Kenntnis der Anwendungsdomäne, insbesondere der dort eingesetzten Entwurfsprozesse. Aus Sicht der Grundlagenforschung seien beispielhaft folgende Fragestellungen genannt:

- Wie kann mit realen Applikationen umgegangen werden, welche die beherschbare Zustandszahl überschreiten?
- Kann man etwa Steuergerätenetzwerke dadurch verifizieren, dass jeweils nur bestimmte "abstraktere Sichten" der einzelnen Steuergeräte für die Verifikation herangezogen werden, etwa solche, die gerade für die Kommunikation relevant sind?
- Kann man solche Abstraktionen automatisch erzeugen?
- Wie können die Realzeitaspekte in der Verifikation berücksichtigt werden?
- Wie können die für regelungstechnische



Im Luftfahrt- und Automobilbereich kommen oft Varianten eines V-basierten Entwurfsprozesses zum Einsatz. Das obige Schaubild zeigt dies für den Automobilbereich, in dem drei Konstruktionsprozesse - dargestellt durch drei ineinander verschachtelte Vs – synchronisiert werden müssen. Die in diesem Artikel vorgestellten Validationstechniken betreffen die Entwicklung von Steuergeräten, welche ihrerseits unterteilt werden in die Systementwicklung, die Softwareentwicklung, und die Hardwareentwicklung. Mit dem absteigenden Ast des V´s verbunden sind Entwurfsschritte, in denen die durch das Steuergerät zu realisierende Funktion zergliedert wird in Teilfunktionen. Dieser Prozeß der funktionalen Dekomposition wird bis zu Basis-Softwareeinheiten durchgeführt, welche dann in einer Implementierungsphase als Code für den in der Hardwareentwicklung ausgewählten Mikrocontroller realisiert werden. Im aufsteigenden Teil des V´s werden zunächst SW-Module zu ablauffähigen Tasks integriert, und dann in die (parallel entwickelte) Steuergeräte Hardware integriert. Anschließend erfolgt die Integration sowohl mit den zu regelnden Komponenten – im Bild etwa die Integration von Motorsteuerung und Motor – sowie mit anderen Steuergeräten. Das untere V enthält in der Mitte ein Steuergerät (englisch: electronic control unit, ECU).



In einem modellbasierten Entwurfsprozess wird im Rahmen des Systementwurfs eine Aufgliederung der Gesamtfunktion des Steuergerätes in Teilfunktionen vorgenommen. Im Bild handelt es sich um ein Modell einer Zentralverriegelung, welche die Teilfunktionen *Entriegeln, Verriegeln, Sichern, Automatisch Verriegeln, Selektiv Entriegeln und Crash* sowie weitere Funktionen wie etwa eine Wiederholsperre beinhaltet. Die *Crash Funktion* entriegelt im Falle eines Unfalls automatisch alle Türen. Wann welche Teilfunktion zu aktivieren ist, wird durch den grün umrandeten Controller festgelegt. Ebenfalls erkennbar sind die mit dem Steuergerät verbundenen anderen Teilsysteme des Fahrzeuges.

Anwendungen typischen dynamischen Aspekte einer automatischen Analyse zugänglich gemacht werden?
Solche Grundlagenfragen wurden - teilweise in Kooperation mit Wissenschaftlern des Technion (Orna Grumberg) und des Weizmann Instituts (David Harel und Amir Pnueli) in Israel - behandelt.
Vergleichbar zur Komplexität der Grundlagenfragen sind die Herausforderungen in der softwaretechnischen Umsetzung. Beispielhaft sein auch hier zu behandelnde Themenfelder genannt:

- die Integration eines kommerziellen Entwicklungswerkzeuges Statemate, d.h. die Umsetzung der dort angeboten vielfältigen Möglichkeiten zur Modellierung von Steuergeräten in eine sich zunehmend als allgemeine Integrationsplattform erweisende Zwischenrepräsentation, welche die Vielzahl der Konstrukte von Statemate auf ihre semantische Essenz reduziert;
- die Entwicklung und Konzeption umfassender Analyse und Optimierungswerkzeuge auf der Zwischenrepräsentation;
- das Herunterbrechen aller Berechnungen auf Bitebene in die von Modellprüfern akzeptierten symbolischen Formate;
- die Integration der aus der Grundlagenforschung entwickelten Techniken der Systemverifikation und Abstraktion;
- sowie schließlich die Integration aller Teilkomponenten unter einer einheitlichen Benutzerführung.

Diese Vielzahl von ineinander greifenden Ergebnissen führte zur Entwicklung einer leistungsfähigen Verifikationsumgebung für das Werkzeug Statemate, mit der Steuergeräte der Größenordnung der Zentralverriegelung unter Einsatz der Abstraktionstechniken im Minutenbereich verifiziert werden können. Erreicht wurde dieses nicht zuletzt auch Dank enger Kooperationen mit industriellen Partnern, im Automobilbereich insbesondere mit BMW, da nur eine gute Kenntnis typischer Einsatzsituationen und Modellierungsstile eine Optimierung der gesamten Werkzeugkette erlauben, wie sie für diese Leistungsklasse unverzichtbar ist.
Heute hat OFFIS in zahlreichen durch BMBF und EU oder auch unmittelbar durch die Industrie geförderten Projekten Kooperationen mit einer Vielzahl führender Automobilhersteller, so in Deutschland mit BMW und DaimlerChrysler. Aber auch im Luftfahrtbereich greifen diese Techniken; hier kooperiert OFFIS z.B. mit DASA und Aerospatial, um die Verifikationstechniken für den künftigen Airbus-Entwicklungsprozess einsetzbar zu machen. Auch im Bereich der Bahntechnik stößt die inzwischen über I-Logix angebotene Verifikationsumgebung auf positive Resonanz. So laufen zur Zeit etwa Kooperationsverhandlungen mit Adtranz.
Modellbasierte Verifikation bleibt nur ein Baustein in der Vielzahl von qualitätssichernden Maßnahmen in der Entwicklung von Steuergeräten. Inzwischen wurde eine automatische Generierung von Testvektoren aus Statematemodellen - wiederum in enger Kooperation mit BMW - prototypisch realisiert, um sowohl die Abnahme von Steuergeräten vom Zulieferer wie auch die Integration von Steuergeräten mit dem als "golden device" dienenden Referenzmodell im aufsteigenden Teil des V-Modells vornehmen zu können. Auch hier zeichnen sich weitreichende industrielle Kooperationen ab. Jeder solche Baustein trägt einen Teil dazu bei, die Sicherheit der Steuerungssysteme zu erhöhen und ist ein Schritt mehr zur Vermeidung von durch Steuergeräten verursachten Unfällen.

Der Autor

Prof. Dr. Werner Damm ist seit 1987 Hochschullehrer für Rechnerarchitektur am Fachbereich Informatik und seit 1995 Vorstandsmitglied des An-Instituts OFFIS. Er studierte Informatik und Mathematik an der Universität Bonn, und wurde dann wissenschaftlicher Assistent an der RWTH Aachen, wo er über Fragestellungen aus der Theoretischen Informatik 1981 promovierte und sich 1986 für das Fach Informatik habilitierte. In Oldenburg trug er maßgeblich zum Aufbau des F&E Bereiches Eingebettete Systeme im Institut OFFIS bei. Die dort durchgeführten Arbeiten zur Verbesserung der Qualität modellbasierter Entwurfsprozesse wurden wiederholt vom BMBF und der EU gefördert. Die am Fachbereich Informatik gesetzten Forschungsschwerpunkte im Bereich der Grundlagenforschung für Parallelrechnersysteme und Eingebettete Systeme wurden mehrfach von der DFG gefördert.

Die im Beitrag dargestellte Statemate Verifikationsumgebung ist ein gemeinsames Ergebnis der folgenden Mitarbeiter der Arbeitsgruppe des Autors: Dipl.-Inform. Tom Bienmüller, Dipl.-Inform. Henning Brinkmann, Dr. Udo Brockmeyer, Dipl-Inform. Claus Eßmann, Dr. Bernhard Josko, Dipl.-Inform. Hans Holberg, Dr. Hardi Hungar, Dipl.-Inform. Rainer Lochmann, Dipl.-Inform. Karsten Lüth, Dipl.-Inform. Rainer Schlör, Dipl.-Inform. Ingo Schinz, Dipl.-Inform. Hartmut Wittke, Dr. Gunnar Wittich.