Formale Verifikation von ASCET Modellen im Rahmen der Entwicklung der Aktivlenkung

Prof. Dr. Werner Damm, Christoph Schulte, Hartmut Wittke, Marc Segelken
OFFIS, Oldenburg
Uwe Higgen, Dr. Michael Eckrich
BMW AG, München

Abstract: Im folgenden wird der Einsatz eines Prototypen zur formalen Verifikation von ASCET-SD-Modellen im Kontext der aktuell von BMW entwickelten Aktivlenkung [EPK+02] geschildert. Der Prototyp wurde zur Überprüfung sicherheitsrelevanter Eigenschaften der Abschaltlogik verwendet, welche ein zentraler Bestandteil der Steuerung der Aktivlenkung ist.

1 Einleitung

Der Einzug von X-by-Wire Systemen hat im Fahrzeug längst stattgefunden. So sind das ”Shift-by-Wire”, also die elektromechanische Getriebesteuerung im 7er BMW oder dessen elektromechanische Feststellbremse EMF typische Vertreter der ”By-Wire”-Technologie in einem Serienfahrzeug. Der Trend wird fortgesetzt durch die für den neuen 5er BMW entwickelte Aktivlenkung, einer Lenkung mit voller ”Steer-by-Wire”-Funktionalität, sieht man vom autonomen Fahren ab. Auch das Bremsen mit ”Brake-by-Wire” wird ohne Hydrauliksystem mit Bremskraftverstärker in Zukunft funktionieren. Verbessertes Crash Verhalten und neue Potentiale zur Reduzierung des Bremsweges sind die Ziele des Umstiegs auf diese ”By-Wire”-Technologie.

BMW hat mit ASCET-SD die gesamten Steuerungs- und Regelfunktionen für die Aktivlenkung entwickelt. Zunächst wurden die Funktionen ”offline” auf dem PC mit Matlab simuliert. Im zweiten Schritt folgte dann die Modellierung mit ASCET-SD und der Test im Fahrzeug mittels ”Online”-Simulation auf dem modularen Experimentalsystem ES1000. Im dritten Schritt werden die Funktionen mittels Target-Code-Generierung auf das Serien-Steuergerät portiert und schliesslich im Fahrversuch mit INCA appliziert.

In diesem Paper wird die Applikation des von OFFIS entwickelten Verifikationswerkzeugs [BDKW01] auf eine Komponente der Aktivlenkung-Software geschildert, welche die zentralen sicherheitsrelevanten Funktionen wahrnimmt. Das bereits für andere CASE-Tools eingesetzte Verifikationswerkzeug[1] wurde in diesem Kontext um die Unterstützung des ASCET-SD CASE-Tools erweitert.

[1] Es gibt auch eine Unterstützung für Stateflow, Scade und Statemate. Letztere wird bereits kommerziell durch OSC vertrieben.

2 Beschreibung des Verifikationswerkzeugs aus Anwendersicht

Das von OFFIS entwickelte Verifikationswerkzeug dient der Sicherung der funktionalen und realzeitmäßigen Korrektheit von ASCET-SD-Modellen. Das Hauptaugenmerk liegt auf der Einsetzbarkeit im industriellen Rahmen, was durch die Anwendung des Werkzeugs noch während dessen Entwicklung auf Teile der Aktivlenkung unterstrichen wurde. Der hohe Automatisierungsgrad im Verifikations- und Fehlerdiagnoseprozeß motiviert die Anwendung des Verifikationswerkzeugs bereits in der Systemkonzeptionsphase und kann somit den gesamten Entwicklungsprozess begleitend eingesetzt werden.

Neben dem in ASCET-SD entworfenen Modell wird eine (sicherheitsrelevante) Eigenschaft als Eingabe für das vollständig grafisch zu benutzende Verifikationswerkzeug benötigt. Zusammen mit dem übersetzen (Teil-) Modell wird diese dem Modelchecker[Gro96] zur Bearbeitung übergeben. Nur wenn das ASCET Modell die Anforderung unter allen möglichen Randbedingungen erfüllt, wird diese vom Modelchecker als gültig erkannt. Der Wahrheitswert dieser Aussage ist mathematisch abgesichert, da der Modelchecker automatisch einen formalen Nachweis bzw. Widerlegung dieser Eigenschaft durchführt. Keine Art von Testen kann dies erreichen, da ein Test aus Komplexitätsgründen nicht vollständig sein kann und jeder einzelne Testlauf das System jeweils nur unter einer vorgegebenen Abfolge von Eingaben prüft. Beim Modelchecking werden dagegen in einem Verifikationslauf sämtliche Abläufe des Systems unter sämtlichen möglichen Eingaben analysiert. Wird eine Spezifikation nicht erfüllt, gibt der Modelchecker neben dieser Tatsache auch einen dazugehörigen Fehlerpfad aus, welcher das System in ein die geforderte Eigenschaft verletzenden Systemzustand versetzt. Der Fehlerpfad zeigt eine Folge von Eingaben und Zuständen des Systems und wird in einem Waveform-Viewer visuell dargestellt. Der Fehlerpfad kann ebenso zum Treiben der Simulation verwendet werden. Dieses Feedback stellt für den Entwickler die wirkliche Leistungsstärke dar, da genaue Fehlerdiagnose-Informationen gerade in der Systemkonzeptionsphase von entscheidender Bedeutung sind und somit das Verifikationswerkzeug zu einer Reduktion der Entwicklungszeit beiträgt.

Eine Besonderheit der Verifikation von ASCET-SD Modellen ist die Verwendung des von ASCET-SD erzeugten C-Codes, wodurch neben der Erkennung von Modellfehlern zusätzlich auch das Auffinden von durch eine fehlerhafte Code-Generierung bedingten Fehlern ermöglicht wird. Der erzeugte C-Code wird zur Verifikation von einem Compiler übersetzt und an den Modelchecker übergeben, welcher den Code anschließend gegen eine Modellanforderung verifiziert.

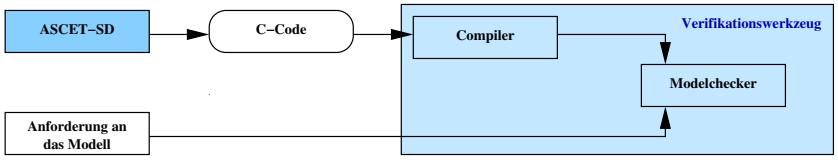

Abbildung 1: Architektur der Verifikation von ASCET-SD Modellen via generiertem C-Code.

3 Fallstudie: Aktivlenkung

Bei der Aktivlenkung handelt es sich um ein aktuelles industriell entwickeltes Modell. Um ein unkontrolliertes Eingreifen des Aktivlenkungsstellers oder eine zur Fahrsituation unpassende Veränderung der Momentenunterstützung (Servotronic / ECO), verursacht durch Fehler der Sensorik, der Aktuatorik oder des Steuergerätes, zu unterbinden, muss in einer dedizierten Weise auf diagnostizierte Fehler reagiert werden, so daß der Fahrer stets in der Lage ist, das Fahrzeug sicher zu beherrschen. Gleichzeitig muß eine hohe Verfügbarkeit der Aktivlenkungssystemfunktionalitäten sichergestellt werden als Basis für ein wachsendes Vertrauen bzw. Zufriedenheit des Fahrers in dieses System.

Grundlage für eine geeignete Systemreaktion im Fehlerfall ist eine schnelle Fehlererkennung bzw. -diagnose des Systems sowie eine situativ geeignete Fehlerbehandlung, zu der das System dann noch in der Lage ist. In einer Vielzahl von Fehlerfällen, die im wesentlichen die Aktivlenkungskomponenten zur Ausführung eines Stellkommandos betreffen, kann dabei nur mehr durch den unmittelbaren Übergang in den systembedingten mechanischen bzw. hydraulischen FailSafe-Zustand reagiert werden. Demgegenüber können wiederum auf eine Vielzahl von Fehlern, vor allem in der Aktivlenkung-Sensorik, Maßnahmen zur Behandlung des Aktivlenkung-Stellkommandos greifen, die eine nur geringe Funktionseinschränkung bewirken.

Neben der eigentlichen regelungstechnischen Kernfunktionalität, beinhaltet die Aktivlenkung eine diskrete Sicherheitskomponente (Abschaltlogik). Die Abschaltlogik nimmt je nach Bewertung der Sensorwerte eine etwaige (kontrollierte) Abschaltung des Systems vor und eignet sich aufgrund ihres großen logischen Anteils hervorragend für die formale Verifikation.

4 Verifikation ausgewählter Eigenschaften der Failsafe Komponente

Die Failsafe Komponente beinhaltet neben der diskreten Logik ebenfalls Berechnungen auf kontinuierlichen Werten zur kontrollierten Abschaltung der berechneten Stellwerte durch Einsatz von entsprechenden Rampenfunktionen. Da kontinuierliche Größen nach derzeitigem Entwicklungsstand nicht direkt vom Verifikationswerkzeug berücksichtigt werden können, sind diese Anteile durch eine automatische Abstraktion vollständig entfernt worden. Dadurch war es möglich, das sich in der Entwicklung befindliche Modell ohne eine über die Änderung einiger Wertebereiche hinausgehende Anpassung zu übernehmen. Eigenschaften der Kontrolle in einem Steuergerät hängen meist nur mittelbar von kontinuierlichen Datenwerten ab. Daher kann von der konkreten Berechnung auf kontinuierlichen Daten abstrahiert werden ohne Kontrolleigenschaften zu beeinflussen. Viele sicherheitsrelevante Anforderungen lassen sich mit dem abstrahierten Modell nach diesem automatisierten Schritt weiterhin verifizieren.

Bei fehlerhaftem Eingangssignal der Aktivlenkungsstabilisierungsfunktion ist ein Stelleingriff bedingt zu unterbinden, bzw. in konkreterer Form: Bei instabiler Fahrt (`LwWC_YRC>0`) muß die Gierratenregelung durch eine Rampenfunktion abgeschaltet werden, sobald in der

Eingangsvariable `I_RR_qual` das erste Bit gesetzt ist, wodurch ein fehlerhaftes Signal angezeigt wird. Die Formalisierung dieser Eigenschaft wird unter Zuhilfenahme eines vordefinierten Spezifikationsmusters umgesetzt, wodurch der zeitliche Umstand ausgedrückt werden kann, daß die Reaktion des Systems erst nach einer gewissen Anzahl von Berechnungsschritten erfolgen muß. Das Modell erfüllte diese Eigenschaft nicht!

Das Ergebnis der Berechnung dieser Verifikationsaufgabe ist in Abbildung 2 dargestellt und zeigt eine Situation, in der die Eigenschaft keine Gültigkeit hat. Anhand der Variable `Shutdown_act` ist die Fehlersituation zu erkennen, da trotz entsprechendem Sensorausfall (Bit 1 in `I_RR_qual` ist gesetzt) die Rampenfunktion zur Abschaltung nicht aktiviert wird (`Shutdown_act` bleibt 0).

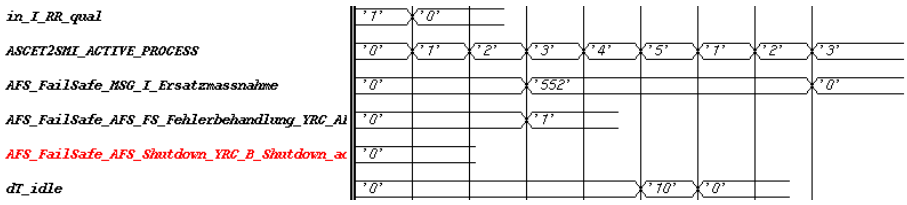

Abbildung 2: Diagnose-Fehlerpfad des Modelcheckers. Trotz `I_RR_qual==1` erfolgt keine Reaktion in `Shutdown_act` innerhalb der vorgegebenen Zeitspanne.

Nach erfolgter Korrektur des Modells wird nach erneutem Modelchecker-Verifikationslauf das Ergebnis `TRUE` ausgegeben, gleichbedeutend mit der Aussage, daß das System nun unter allen möglichen Umgebungsverhalten die Anforderung einhält. Nach ähnlichem Schema sind eine Reihe weiterer Beweisaufgaben bzgl. der FailSafe-Komponente durchgeführt worden, welche die Korrektheit bzgl. dieser Anforderungen bestätigt haben[2]. Die benötigte Rechenzeit zur Durchführung dieser Beweisaufgaben beträgt wenige Minuten.

5 Rolle des formalen Modells innerhalb des Entwurfsprozesses bei BMW

Die Funktionsentwicklung zur Aktivlenkung startet mit der Spezifikationsphase. In dieser Phase wird versucht, zum einen die Erreichung des Gesamtziels bestmöglich sicherzustellen und zum anderen, die Entwicklung speziell der Funktionsalgorithmen für die fahrdynamische Regelung der Aktivlenkung transparent zu halten und auf ein möglichst solides regelungstechnisches Fundament zu stellen. Anhand einer Closed-Loop Simulation mit detaillierten Fahrzeug-Modellen wird der Funktionsentwurf bezüglich der definierten Ziele validiert, sowie eine geeignete Grundapplikation der Reglerfunktionen erstellt. Der Nachweis der Stabilität eines Reglers ist dabei eine notwendige Voraussetzung für einen realen Fahrzeug-Funktionstest im fahrdynamischen Grenzbereich. Im nächsten Schritt wird

[2]Leider ist das prototypische Verifikationswerkzeug erst kurz vor der Serienreife der Aktivlenkung zum Einsatz gekommen, weswegen etwaige Fehler nur auf älteren Versionen nachgewiesen werden konnten. Die neueren Versionen waren bzgl . der untersuchten Eigenschaften bereits fehlerfrei.

das Funktionsmodell diskretisiert und in echtzeitfähigen Code umgesetzt. Ohne den Ballast der ”Serienfähigkeit” einer Steuergeräte-Hardware wird für den ersten Funktionstest im Fahrzeug eine Art ”Online”-Simulation auf einem modularen Experiment-Steuergerät ausgeführt, so dass die Entwicklungszeit in dieser Phase enorm verkürzt wird. Im Fahrversuch bestätigte Funktionen werden schließlich mittels einer automatisierten Target-Code-Generierung in die serientaugliche Software integriert, feinappliziert und nach weiteren systematischen Tests im Fahrzeug sowie an verschiedenen Prüfständen freigegeben. Die Funktionstests werden schließlich noch ergänzt mit dem für sicherheitsrelevante Software-Anwendungen obligatorischen Nachweis über die Korrektheit der Software, wie z.B. SW-Modul-Test, Äquivalenz-Klassen-Test, Integrationstest und formale Verifikation. Entscheidend für die Aussagekraft sämtlicher Sicherungsmaßnahmen in einer Systementwicklung ist schließlich ein konsequentes und striktes Änderungsmanagement, das die Freigabe nur vollständig getesteter Funktionen garantiert.

Die formale Verifikation wurde prototypisch in der Entwicklung der Abschaltlogik der Aktivlenkung eingesetzt. Dabei wurden zwei Anwendungsszenarien identifiziert:

1. Konzeptabsicherung durch formale Verifikation der Anforderungen an die entsprechende ASCET-SD Komponente
2. Regressive Absicherung der während der Entwicklung geänderten Komponenten.

6 Zusammenfassung

Mit diesem Beitrag wurde Einblick gegeben in die Verwendung formaler Verifikation zur Überprüfung von Sicherheitsseigenschaften mit diskret reaktivem Teilverhalten einer hybriden Komponente, wie sie typischerweise in eingebetteten Systemen wie z.B. Steuerungssystemen im Automobil Einsatz findet. Anhand der Fallstudie Aktivlenkung wurde beispielhaft der Nachweis einer Eigenschaft an einem industriell eingesetzten Beispiel gezeigt. Durch die Einordnung des Modelcheckings speziell im BMW-Entwurfsprozeß konnte der Nutzen dessen Einsatzes sowie die damit verbundenen Vorteile für die Produktentwicklung identifiziert werden.

Literatur

[BDKW01] T. Bienmüller, W. Damm, J. Klose, and H. Wittke. Formale Analyse und Verifkation von Statemate-Entwürfen. *it+ti, Informationstechnik und Technische Informatik*, 43/1(1):29–34, Februar 2001.

[EPK+02] M. Eckrich, M. Pischinger, M. Krenn, R. Bartz, and P. Munnix. Die Aktivlenkung - Anforderungen an Sicherheitstechnik und Entwicklungsproze. In *11. Aachener Kolloqium Fahrzeug- und Motorentechnik 2002, 8. - 9.10, Aachen*, 2002.

[Gro96] The VIS Group. VIS : A System for Verification and Synthesis. In *8th international Conference on Computer Aided Verification*, number 1102 in LNCS, 1996.