



VALSE-XT: Eine integrierte Lösung für die SoC-Verifikation

www.edacentrum.de/projekte/

Zusammensetzung
des Projektkonsortiums

Partner:

Concept Engineering GmbH <<
Infineon Technologies AG <<
Lucent Technologies
Network Systems GmbH <<
Melexis GmbH <<
Robert Bosch GmbH <<

Unterauftragnehmer:

Universität Bremen <<
Universität Darmstadt <<
Universität Freiburg <<
Universität Hannover <<
Universität Kaiserslautern <<
Universität Tübingen <<
Fraunhoferinstitut für
Integrierte Schaltungen Dresden <<
Institut für mikroelektronische-
und mikromechanische-
Systeme GmbH <<
Konrad-Zuse-Zentrum Berlin <<

Förderkennzeichen:

01 M 3069 A

Laufzeit des Vorhabens:

01.08.2003 – 31.07.2005

Projektziele

SoCs ermöglichen fast unbegrenzte Produktinnovationen. Aber beim Entwurf solcher Chips wird die Verifikation zum begrenzenden Faktor. 60-80% der Entwurfsaufwände entfallen auf die Verifikation, 1-2 Redesigns pro Projekt könnten durch eine verbesserte Verifikation vermieden werden und oft ist ein teurer, verspäteter Markteintritt die Folge unterschätzter Verifikationsaufwände.

Die Projektpartner von Valse-XT gehen davon aus, dass die Unvollständigkeit der Simulation maßgeblich für das Verifikationsproblem verantwortlich ist, dass die Simulation für wichtige Verifikationsaufgaben durch weit leistungsfähigere, spezialisierte Verfahren ersetzt werden kann und dass dieser Schritt massive Produktivitäts- und Qualitätsgewinne mit sich bringt.

Aus dieser Arbeitshypothese wurden das Valse-Programm und insbesondere das Arbeitsprogramm für Valse-XT abgeleitet. Es sieht vor

- » die Technik der formalen Eigenschaftsprüfung zu einer erschöpfenden, hochautomatisierten Verifikation auszubauen, die digitale Komponenten, diskretisierte Mixed-Signal-Schnittstellen, kleine eingebettete HW/SW-Systeme sowie asynchrone Systemaspekte überprüfen kann,
- » die Korrektheit automatischer und händischer Entwurfsverfeinerungen für digitale Schaltungen und Analogzellen durch mathematische Äquivalenzvergleiche zu garantieren und
- » durch eine vollständige Betriebsfehleranalyse kostengünstig die Robustheit sicherheitskritischer Systeme gegen Betriebsfehler sicherzustellen.

Einleitung

Mit dem Valse-Programm wollen die Projektpartner für große Verifikationsaufgaben überlegene Alternativen zur Simulation bereitstellen. Auf Basis grundlegender Arbeiten aus dem Valse-Projekt verfolgt Valse-XT (die 2. Phase dieses Programms) dieses Ziel (s. Abbildung 1.2) mit folgendem technischen Programm:

- » Eigenschaftsprüfung:
Mit Weiterentwicklungen der formalen Modulverifikation aus Valse (Arbeitspaket V-XT-1/2) und Anpassungen der Technik an die Besonderheiten von Mixed-Signal-Schaltungen (Arbeitspaket V-XT-3) sollen für das Gros aller Schaltungsklassen lokale Fehler

- diese machen oft mehr als 50 % des gesamten Fehleraufkommens aus - frühzeitig und vollständig entfernt werden. Der Anwendernutzen (Qualität, Produktivität) im Vergleich zu den Substitutionskosten (Ausbildung, Flow-Anpassungen, Werkzeuginvestitionen etc.) wird als sehr hoch bewertet. Dieser Nutzen wird weiter vergrößert, indem die Modulverifikation in die bestehende Verifikationslandschaft und in den Trend der transaktionsbasierten Verifikationsplattformen (Arbeitspaket V-XT-4) integriert wird. Die Basistechnik der formalen Modulverifikation soll darüber hinaus erprobt werden, um kleine, eingebettete HW/SW-Systeme sowie asynchrone Systemaspekte zu verifizieren (Arbeitspaket V-XT-5).

» Äquivalenzvergleich:

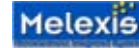
Es sollen problemspezifische Lösungen für den sequenziellen Äquivalenzvergleich entwickelt werden, um die nach obigem Vorgehen für die Designphasen erzielbare hohe Qualität in nachfolgenden Entwurfschritten nicht zu gefährden. Diese Verfahren sollen im Digitalentwurf sicherstellen, dass technischer Fortschritt bei der Synthese und neue Optimierungsmöglichkeiten ohne Kompromisse bei der Verifikation voll ausgenutzt werden können (Arbeitspaket V-XT-6). Mit ganz andersartigen mathematischen Verfahren soll für Analogzellen die Übereinstimmung ihrer SPICE- und VHDL-Views garantiert werden (Arbeitspaket V-XT-3).

» Betriebsfehleremulation:

Unter den nichtfunktionalen Anforderungen spielt die Robustheit des Systemverhaltens bezüglich der Betriebsfehler eine zentrale Rolle - gerade für die sicherheitskritischen Systeme der Kfz-Elektronik. Durch Vervollständigung der Verfahrenskette von der Fehlerklassifikation über die Fehlereinspielung in einen Low-Cost-Emulator, die Bestimmung der Auswirkungen eines Fehlers auf den Fahrbetrieb bis hin zur Optimierung der Testprogramme soll in Valse-XT eine bisher einzigartige Zertifizierungstechnik für sicherheitskritische Systeme entstehen.

Arbeitspaket V-XT-1: „Formale Modulverifikation“

Kritisch für die Realisierung kompletter Systeme auf einem Chip ist die Verfügbarkeit qualitativ hochwertiger Module, aus denen das Chipdesign idealerweise „zusammengesteckt“ wird. Denn die Wahrscheinlichkeit für korrektes Verhalten des Systems ist höchstens das Produkt der Wahrscheinlichkeiten für korrektes Verhalten der Module. Für einen Entwurf mit 100 Modulen, die jeweils eine Wahrscheinlichkeit von 99,9 % für korrektes Verhalten aufweisen, beträgt



Valse-XT Hochautomatisierte, zertifizierende und skalierende VALidierung von „System-on-Chip“-Entwürfen – 2. Phase

Thematische Ausrichtung

Das Verifikationsproblem

- 60 – 80 % der Entwurfskosten entfallen auf die Verifikation!
- 1-2 Redesigns pro Projekt werden von funktionalen Fehlern verursacht!
- Teurer, verspäteter Markteintritt ist oft die Folge unterschätzter Verifikationsaufwände!

Arbeitshypothese

- Unvollständigkeit der Simulation ist maßgeblich für das Verifikationsproblem verantwortlich.
- Simulation kann für wichtige Verifikationsaufgaben durch weit leistungsfähigere Verfahren ersetzt werden.
- Zu erwarten sind massive Produktivitäts-/Qualitätsgewinne.

Valse-XT-Arbeitsprogramm

Erschöpfende, hochautomatisierte Verifikation

- digitaler Komponenten (Interrupt Controller, Arbitr, ..., Prozessoren)
- diskretisierter Mixed-Signal-Schnittstellen
- kleiner, eingebetteter HW/SW-Systeme
- asynchroner Systemaspekte

Garantierte Übereinstimmung von

- SPICE- und VHDL-Views für Analogzellen mit einigen Hundert Transistoren
- Darstellungen digitaler Schaltungen mit unterschiedlichen Zustandskodierungen (Retiming, ..., FPGA-Synthese)

Vollständige Betriebsfehleranalyse zur

- kostengünstigen Sicherung der Robustheit sicherheitskritischer Systeme gegen Betriebsfehler

Formaldaten

Laufzeit: 8/2003-7/2005
 Personaleinsatz: ca. 63 PJ
 davon 23,5 PJ an Hochschulen/Instituten
 Projektkoordination:
 Prof. Dr. W. Büttner, Infineon Technologies AG
 Wissenschaftlicher Direktor:
 Prof. Dr. W. Kunz, Universität Kaiserslautern

Umsetzung des Valse-XT-Programms

Highlights

Eigenschaftsprüfung digitaler Komponenten

- neuer Arithmetikkalkül erlaubt die Eigenschaftsprüfung komplexer, arithmetischer Blöcke mit Wortbreiten von 32 und mehr Bits (Infineon)
- Eigenschaftsprüfung aus Valse-XT ermöglicht es 90% der Beweisarbeit bei der Prozessorverifikation automatisch durchzuführen (Infineon, Verisort-Partner)

Eigenschaftsprüfung von Mixed-Signal-Blöcken

- vollständige Verifikation eines SAR-ADC mit hochauflösender ADC-Diskretisierung (Infineon)

Eigenschaftsprüfung von kleinen, eingebetteten HW/SW-Systemen

- Verifikation einer Echtzeitanforderung an 16-Bit Mikrocontroller (Melexis)

Eigenschaftsprüfung auf Spezifikationsebene

- Abstraktion eines Sonet/SDH-Protokolls über Tausende von Takten verifiziert (Lucent)

Äquivalenzvergleich von Analogzellen

- schrittweitengesteuerter Vergleich beschleunigt Rechenzeiten um Faktor 10 (Infineon)

Sequentieller, digitaler Äquivalenzvergleich

- Syntheschritt für Block mit 200k Gattern und mehreren sequentiell optimierten Teilblöcken verifiziert (Infineon)

Vollständige Betriebsfehleranalyse

- prototypische Implementierung einer homogenen Fehleremulationsumgebung (Bosch)

- Verfügbarkeit von kommerziell nicht erhältlichen Lösungen und Beratungskompetenz für schwierige Verifikationsprobleme
- Impulsgeber für große deutsche „formal methods community“
- Ergebnistransfer in weitere Branchen
- technologischer Vorteil beim weltweiten Wettbewerb um Designprojekte

Standortvorteile durch Valse-XT



Abbildung 1.2:

Darstellung der thematischen Ausrichtung und der Highlights von VALSE-XT

die Wahrscheinlichkeit für korrektes Verhalten des Gesamtsystems höchstens 90%. Liegt also die Fehlerwahrscheinlichkeit der Module nicht unterhalb des Promillebereichs - und dies ist nur mit formalen Methoden zu erreichen -, dann bleibt die Systemsimulation weiterhin hoffnungslos überfrachtet mit dem Aufdecken lokaler Probleme anstelle einer Konzentration auf Systemaspekte.

Der Preis, den das angestrebte extreme Qualitätsniveau fordert, ist ein „White-Box“-Vorgehen: Aus Spezifikation und Code des Moduls wird für Teile der Funktionalität eine Hypothese in Form einer so genannten Eigenschaft gebildet. Eine Eigenschaft beschreibt den erwarteten Verlauf wichtiger Signale über ein Taktfenster. Kann per Eigenschaftsprüfung die Gültigkeit dieses Signalverlaufs nachgewiesen werden, dann ist ein Stück Verhalten des Moduls identifiziert und bewiesen worden. Andernfalls muss nachgebessert werden bzw. liefert die Überprüfung einen Trace (ein so genanntes Gegenbeispiel), der das fehlerhafte Verhalten des Moduls erklärt. Auf diese Weise entsteht eine formale Spezifikation des Moduls inklusive Korrektheitsnachweis.

Abbildung 1.3:

Qualitative Gegenüberstellung
Simulation vs.
Formale Modulverifikation

Im Arbeitspaket V-XT-1 geht es vor allem darum, die Eigenschaftsprüfung auf den Datenpfad und auf Schaltungen von großer sequentieller Tiefe performant auszuweiten. Zu diesem Zweck wurde ein Reduktionsverfahren entwickelt, das eine gegebene Eigenschaftsprüfung automatisch auf spezielle Eigenschaftsprüfungen auf Bitebene reduziert. Bei den besonders schwierigen Reduktionen für Arithmetik wurde ein Durchbruch erzielt. Bisher kann schwierige Arithmetik allenfalls durch „Bit-Slicing“ verifiziert werden, d.h. die Verifikation wird nur für wenige ausgewählte Bits durchgeführt, während die übrigen Bits konstant gehalten werden. Auf Basis einer Normalisierungstechnik, die auf elementaren arithmetischen 1-Bit-Operationen beruht, können nun komplexe arithmetische Operationen vollautomatisch auf voller Bitbreite verifiziert werden. Die Praxistauglichkeit der Verfahren wurde anhand der formalen Verifikation handoptimierter Arithmetikbefehle des TriCore2-Prozessors von Infineon nachgewiesen.

Erwähnenswert ist auch der Fortschritt bei der Erweiterung der Eigenschaftsprüfung auf lange Taktfolgen. Anhand der Überprüfung der maximalen Dauer der Abarbeitung von Requests einer industriellen Schedulingseinheit (ca. 600 Takte) wurde gezeigt, welche Komplexitäten der derzeitige Leistungsstand bewältigen kann.

Die in V-XT-1 entwickelten Verfahren sind in ihrer Algorithmik schwierig, in ihrem Effekt aber sehr gut darstellbar: Im Rahmen des BMBF-Projektes Verisoft läuft zur Zeit die weltweit vermutlich größte und anspruchsvollste formale Verifikation einer Industrieschaltung mit dem Ziel, den TriCore2-Prozessor von Infineon vollstän-

dig zu verifizieren. In diesem Projekt wurden bisher ca. 1400 Eigenschaften erstellt und verifiziert. Diese Eigenschaften beschreiben etwa 70% der Funktionalität des Prozessors.

Mit Hilfe der Performanzsteigerungen aus V-XT-1 konnten 99,9 % dieser Eigenschaften in weniger als zwei Minuten bewiesen werden; es blieben sechs „Langläufer“, die mit einer Gesamtlaufzeit von 12 Stunden verifiziert wurden. Manche dieser Eigenschaften werden gegen mehr als 200 k Gatter verifiziert.

Im Vorgriff auf V-XT-2 und V-XT-4 sei hier schon auf den zu erwartenden Nutzen der formalen Modulverifikation hingewiesen: Das Verfahren liefert eine Qualität, die der einer erschöpfenden Simulation entspricht. Lokale, d.h. in Modulen angesiedelte Fehler werden vollständig eliminiert. Bezogen auf die erreichte Qualität ist die Produktivität pro Personenmonat mit 3-6 k Zeilen vollständig verifizierten Codes sehr hoch (s. Abbildung 1.3).

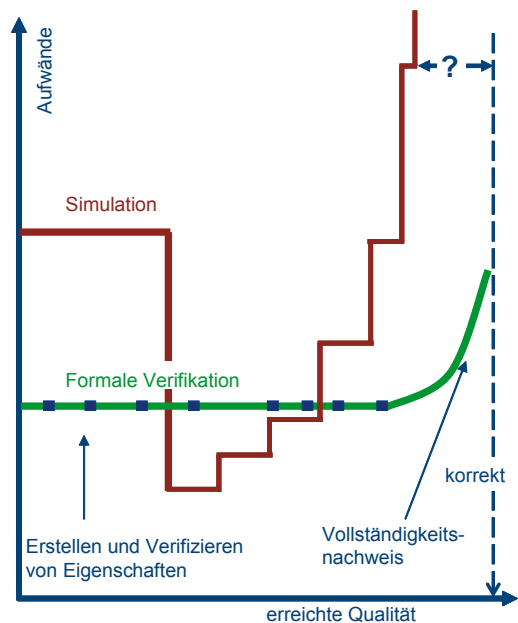


Abbildung 1.3

Die Verteilung von Fehlern lässt erwarten, dass von angenommenen drei Redesigns eines Projektes durch konsequenten Einsatz des Verfahrens ein Redesign eingespart werden kann. Weitere Einsparpotentiale, die das beschleunigte Hochfahren der Chip-/ Systemsimulation sowie HW/Simulatorkosten betreffen, sind allerdings noch nicht quantifiziert worden.

Arbeitspaket V-XT-2:

„Debugging für die formale Modulverifikation“

Die formale Modulverifikation erkennt das Vorhandensein bzw. - das ist das wichtigste Unterscheidungsmerkmal gegenüber der Simulation - garantiert die Abwesenheit von logischen Fehlern. Die im Fehlerfall sich anschließende Aufgabe des Debugging beansprucht heute einen Großteil der manuellen Aufwände und erfordert Einsicht in die Arbeitsweise der entsprechenden Werkzeuge. Durch Automatisierung des

kompletten Debugging-Zyklus soll diese Hürde für den Breitereinsatz deutlich abgesenkt werden. Dieser Zyklus umfasst das automatische Erkennen von Lücken oder Widersprüchen in der vom Verifikationsingenieur erstellten Eigenschaftsbeschreibung eines Moduls (Vollständigkeits-tests), die Erkennung „vermeintlicher“ Fehler, z. B. aufgrund ungenügender Berücksichtigung von Umgebungsinformation (Erreichbarkeitsanalyse) und schließlich das „eigentliche“ Debugging, d.h. das Finden von Designfehlern.

Für die lückenlose Erfassung der Funktionalität eines Moduls durch eine Eigenschaftsspezifikation wurde ein effizient verifizierbares Kriterium aufgestellt. Dieses Kriterium beschreibt etwa Anforderungen an die Vollständigkeit der Spezifikation einer Schaltungsoperation durch Eigenschaften. Es wurde ein Test entwickelt der die Eigenschaftsbeschreibung eines Moduls auf Erfüllung dieses Kriteriums überprüft. Der Test funktioniert mittlerweile für kleine bis mittelgroße Module. Verbesserungspotentiale sind identifiziert.

Weiterhin wurde eine Prozedur entwickelt, um Zusammenhänge (Erreichbarkeitsinformation) in einer Schaltungsbeschreibung zu finden, die einen (vermeintlich) fehlerhaften Ablauf im Design unmöglich machen. Die grundlegende Idee des Ansatzes ist es, das Design in kleine Teile zu zerlegen und o.g. Zusammenhänge für diese Teile zu berechnen. Durch sukzessive Kombination solcher Teile können prinzipiell komplexe Zusammenhänge erkannt werden, solange die entsprechenden lokalen Erreichbarkeitsanalysen noch durchführbar sind.

Basierend auf diversen Vorarbeiten wurde schließlich ein experimentelles RTL-Debugging-Werkzeug erstellt, das Fehlerlokalisierung und -beseitigung vereinfacht. Der aktuelle Prototyp erlaubt z.B. die grafische Darstellung und interaktive Navigation innerhalb fehlerrelevanter Designabschnitte („cone of influence“). Durch die verschiedenen Darstellungsformen der RTL-Fragmente und durch den Bezug zum RTL-Sourcecode ist eine vereinfachte Fehlersuche auf verkleinertem Suchraum gegeben.

Arbeitspaket V-XT-3:

„Semiformale Modulverifikation“

In diesem Arbeitspaket wird eine formale Verfahrenskette entwickelt, um zunächst mit einer Variante der formalen Modulverifikation eine geeignete Diskretisierung eines Mixed-Signal-Blocks zu verifizieren und dann durch einen mathematischen Vergleich von VHDL- und SPICE-Views der beteiligten Analogzellen Korrektheit der Netzliste zu garantieren.

Diese Analogzellenqualifikation erfordert eine anspruchsvolle Mathematik: Zunächst werden der VHDL- bzw. der SPICE-View einer Zelle durch zwei Differentialgleichungssysteme D1, D2 repräsentiert. Diese sind äquivalent, falls es gelingt, ihre Lösungs-

gebilde für alle Eingänge „hinreichend gut“ ineinander zu transformieren. Durch lokale Linearisierung der Lösungsgebilde entsteht ein Gleichungssystem, aus dem ein Stück der gesuchten Transformation berechnet wird. Nach diesem Prinzip wird die Transformation stückweise aufgebaut. Die Komplexität dieser Berechnungen ist der begrenzende Faktor beim analogen Äquivalenzvergleich. Durch schrittweitengesteuerte Berechnung der lokalen Lösungsgebilde ist es zurzeit möglich für Zellen mit bis zu ca. 40 Transistoren die Korrektheit der Verfeinerung nachzuweisen.

Der zweite Schwerpunkt von V-XT-3 betrifft die Verifikation von Mixed-Signal-Blöcken per Eigenschaftsprüfung unter der Annahme korrekt arbeitender Analoganteile.

Diese Verifikation von Mixed-Signal-Blöcken geht von einer hierarchischen VHDL-Beschreibung aus. Die Analogteile eines solchen Blocks sind durch VHDL-Modelle beschrieben, mit denen Verstärker, Spannungsteiler, Analogmultiplexer, Spannungsvergleicher u. a. in ihrem quasi-statischen Verhalten, d. h. ohne Berücksichtigung von Einschwingvorgängen oder Frequenzabhängigkeiten, dargestellt werden können. Elektrische Größen wie Spannung und Widerstand werden in diesen Modellen durch reelle Zahlen beschrieben. So konnte etwa das Verhalten einer Switch-Matrix, die im Wesentlichen aus Verstärkern, Analogschaltern und einer digitalen Ansteuerung bestand, dargestellt werden. Es ist aber auch möglich, Schaltungen mit Rückwirkungen zwischen analogen und digitalen Teilen zu beschreiben, wie dies z. B. bei verschiedenen ADC-Implementierungen der Fall ist.

Für die Verifikation per Eigenschaftsprüfung, werden die im VHDL-Modell der Schaltung vorkommenden reellen Zahlen quantisiert und es entsteht eine digitale Verifikationssaufgabe.

Die spezifizierten Eigenschaften der Mixed-Signal-Schaltung können dadurch in der auch für die digitale Eigenschaftsprüfung verwendeten Eigenschaftsbeschreibungssprache ausgedrückt werden. Mit der digitalen Eigenschaftsprüfung konnte das Verhalten für alle $2^{63} = 10^{19}$ Modi der oben genannten Switch-Matrix verifiziert werden, was per Simulation nicht möglich wäre. Für komplexere Schaltungen kann die Technik auch hierarchisch angewendet werden. Dies war z. B. bei einer Messschnittstelle mit einem 12-bit-SAR-ADC nötig, dessen DAC aus 4 Spannungsteilern mit jeweils 586 Abgriffen besteht. Bei der hierarchischen Vorgehensweise wurde der DAC als Einzelschaltung verifiziert. In der Verifikation der Gesamtschaltung konnte dadurch ein abstrakteres DAC-Modell verwendet werden, dessen Verhalten - wie bewiesen wurde - mit dem Original-DAC übereinstimmt. Durch dieses Vorgehen konnte die Komplexität so weit verringert werden, dass die Verifikation ohne eine Zerlegung der Schaltung möglich wurde.

Arbeitspaket V-XT-4:**„Kopplung formaler und simulativer Verfahren“**

Der Fortschritt bei der Modulverifikation wird in seiner Wirkung potenziert durch Technik und Methodik für die Kopplung von formaler Modulverifikation mit simulationsbasierten Verfahren der RT-Verifikation. Konkret werden in diesem Arbeitspaket Coverage-Metriken für eine ganzheitliche Bewertung eines durch Simulation und Eigenschaftsprüfung erreichten Verifikationsstandes gesucht. Darüber hinaus wird ein Konzept der effizienten Eigenschaftsprüfung von Simulationsläufen entwickelt und erprobt. Schließlich sollen durch gezielte „Systemausdünnungen“ Systemmodelle entstehen, deren Komplexität von einem Eigenschaftsprüfer gehandhabt werden kann.

Bei der Suche nach Coverage-Metriken ist noch kein guter Kompromiss zwischen ausreichender Aussagekraft einer solchen Metrik und effizienter Überprüfbarkeit gefunden worden.

Weit übertroffen wurden dagegen die Erwartungen bzgl. einer effizienten Eigenschaftsprüfung von Simulationsläufen: Hier ist ein Werkzeugprototyp entwickelt worden, der Eigenschaften (s. V-XT-1) in Monitore umwandelt, d.h. Software, die die Erfüllung von Voraussetzungen und das Fehlschlagen von Eigenschaften erkennt und meldet. Dabei werden auch Daten und Timing extrahiert, etwa für Performancestatistiken. Im Zusammenhang mit vollständigen Eigenschaftssätzen (s. V-XT-2) werden so Umgebungsbedingungen gerechtfertigt und mühelos ein vollständiger, transaktionsorientierter Satz funktionaler Coveragepunkte zur Überwachung einer Random-Pattern-Simulation bestimmt.

Vielversprechend entwickelt sich auch die Erprobung eines neuen Konzepts zur automatischen Systemabstraktion. Es zeigt sich, dass mit deutlich reduziertem Speicherplatzbedarf in einer solchen Beschreibung schwerwiegende Systemfehler gefunden werden können.

Arbeitspaket V-XT-5:**„Pfadfinderthemen der Systemverifikation“**

Aufbauend auf den Techniken der formalen Modulverifikation soll die technische Basis für neue Anwendungen in der Systemverifikation erarbeitet werden:

» Das Beheben von Fehlern, lange nachdem sie entstanden sind, ist bekanntlich teuer. Daher soll die Eigenschaftsprüfung ertüchtigt werden, prinzipiell auch Systemaspekte für komplexe Datenübertragungsprotokolle wie etwa SONET/SDH frühzeitig und systematisch zu verifizieren.

» Hoher Simulationsaufwand ist erforderlich, um sicherzustellen, dass Versionen neuer Basissoftware korrekt die Funktionalität älterer Versionen beinhalten. Dieses - im Allgemeinen hoffnungslose - Problem soll

für den in der Kfz-Elektronik wichtigen Spezialfall von in ROM gehaltener Software für kleine, flexible Prozessoren mit formalen Methoden bearbeitet werden.

Auf diesen Arbeitsfeldern wurde mehr erreicht als ursprünglich erwartet:

Es wurde gezeigt, dass es möglich ist, die formale Eigenschaftsprüfung auf Spezifikationsniveau zu heben. Hierfür werden aus einer formalen Beschreibung des Systems durch asynchron kooperierende Automaten quasi-synthetisierbare VHDL-Modelle generiert. Der Benutzer entwickelt in diesem Rahmen formale Anforderungen an das globale Systemverhalten, die durch Eigenschaftsprüfung auf dem VHDL-Modell auf Erfüllbarkeit geprüft werden.

Bisherige Projektergebnisse sind die Entwicklung eines Modellgenerators, basierend auf einem Python-Skript-Interpreter, wesentliche Erweiterungen der Systembeschreibungssemantik hinsichtlich Typkonzept und benutzerdefinierbaren Prozeduren und eine ausführliche Dokumentation des Spezifikationsprototyps und der zugehörigen Methodik.

Als größeres Anwendungsszenario werden aus der Systemspezifikation des Lucent Netzwerkelements Metropolis ADM (Universal) ca. 300 Requirements der dynamischen Bandbreitenverwaltung formal spezifiziert und eine Plausibilitätskontrolle mittels Eigenschaftsprüfung durchgeführt.

Für die Verifikation kleiner, eingebetteter HW/SW-Systeme wurden Werkzeuge erstellt, um ROM-Inhalte in ein verifizierbares Hardwaremodell zu überführen. Damit ist es möglich, in Verbindung mit einem HDL-Prozessormodell Software per Eigenschaftsprüfung zu verifizieren. Um die Einflüsse der Hardware auf die Software richtig abzubilden, ist es nötig, den kompletten Digitalteil einer Schaltung in den Beweis mit einzubeziehen. Als Demonstrator wurde eine Fensterhebersteuerung ausgewählt. Die Schaltung wurde entsprechend aufbereitet, mit Speichermodellen ergänzt und in ein zur Eigenschaftsprüfung konformes Abbild überführt. In ersten Versuchen konnten damit Befehlssequenzen bis zu einer Länge von 35 Instruktionen, die ca. 140 Takten entsprechen, verifiziert werden.

Im verbleibenden Projektverlauf wird für diesen Demonstrator ein Teil der Software verifiziert. So wird zum Beispiel das Verhalten der Schaltung nach einem Interrupt untersucht. Die daraus gewonnenen Ergebnisse werden mit denen der Simulation verglichen, um eine quantifizierte Aussage über den Nutzen der Verifikation gegenüber der Simulation zu erhalten.

Arbeitspaket V-XT-6:**„Sequenzieller Äquivalenzvergleich“**

Bereits heute werden Optionen der Synthese nicht genutzt, um die Durchführbarkeit des kombinatorischen

rischen Vergleichs nicht zu gefährden. Fortschritte bei dem schwierigen Problem des sequenziellen Vergleichs, einschließlich der Konzeption geeigneter Debuggingstrategien, sollen der Designpraxis dieses und zukünftiges Synthesepotenzial erschließen, ohne Kompromisse hinsichtlich der Qualität des Vergleichs hinnehmen zu müssen.

Das Vergleichsproblem soll durch Kombination zweier Ansätze gelöst werden. Ein globaler Ansatz sucht mit verschiedenen (lokalen) Vergleichstechniken für Teile einer Schaltung Äquivalenz nachzuweisen und mit Hilfe der so möglichen Ersetzungen die sequentiellen Unterschiede schrittweise zu reduzieren, bis man ein kombinatorisches Vergleichsproblem erhält, das sich mit bekannten Verfahren lösen lässt.

Der Verbund lokaler Vergleichstechniken reicht von erschöpfender Simulation bis hin zu Techniken der Eigenschaftsprüfung sowie Kombinationen dieser Verfahren, wie z.B. „Amplified Simulation“.

Gute Erfolge wurden mit dieser Vorgehensweise insbesondere bei der Verifikation von Retimingoptimierungen erzielt. Hier konnten Teilblöcke mit einer Größe von bis zu 6000 FlipFlops bzw. 200k Gatter als äquivalent verifiziert werden. Damit wird erstmals die Verifikation des Retimings von Blöcken in praxisrelevanter Größe ermöglicht.

Arbeitspaket V-XT-7: „Betriebsfehleremulation“

Unter den nicht-funktionalen Anforderungen spielt die Robustheit des Systemverhaltens bezüglich der Betriebsfehler eine zentrale Rolle - gerade für die sicherheitskritischen Systeme der Kfz-Elektronik. Durch Vervollständigung der Verfahrenskette von der Fehlerklassifikation über die Fehlereinspielung in einen Low-Cost-Emulator, die Bestimmung der Auswirkungen eines Fehlers auf den Fahrbetrieb bis hin zur Optimierung der Testprogramme entsteht in Valse-XT eine bisher einzigartige Zertifizierungstechnik für sicherheitskritische Systeme.

Es wurde ein erster Prototyp der homogenen Betriebsfehleremulationsumgebung „PARSIFAL“ (Platform for Analysis and Reduction of Safety-critical Implementation's FAULTs) fertig gestellt, mit deren Hilfe Methoden zur Schaltungstransformation (z.B. automatische Konvertierung von Tristate-Bussen in Logik, Fehlerkompaktierung, Fehlerinjektion und Fehleraktiverung) unabhängig von der tatsächlich verwendeten Emulationsplattform entwickelt werden können (s. Abbildung 1.4). Ebenso können Verfahren zur Fehlerabdeckungsbestimmung plattformunabhängig implementiert werden. Der Prototyp unterstützt derzeit die Betriebsfehleremulation sowohl mit kommerziellen Logikemulationssystemen als auch mit FPGA-basierten (Field Programmable Gate Array) Rapid-Prototyping-Systemen unter Verwendung des Stuck-At-Fehlermodells. In der laufenden zweiten Projektphase erfolgt die

Konzeption weiterer Fehlermodelle wie z.B. Bit-Flip-, Verzögerungs- oder Brückenfehler sowie deren Integration in PARSIFAL.

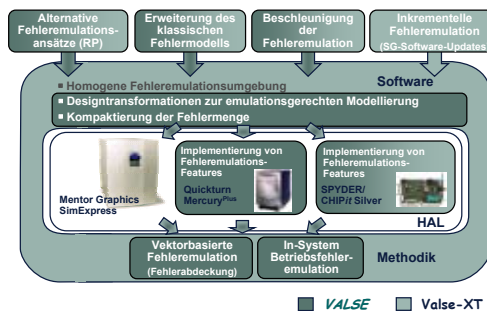


Abbildung 1.4

Ausblick und Perspektiven

Der Erfolg der SoC-Perspektive hängt designseitig kritisch von grundlegenden Verbesserungen bei der Komponenten-, Schnittstellen- und Architekturverifikation ab. Valse-XT schafft für die Komponentenverifikation solche Verbesserungen. Die Verifikation durch eine erschöpfende Eigenschaftsprüfung ermöglicht eine bisher kaum vorstellbare Qualität für digitale Module bis hin zu modernen Prozessoren z.B. der TriCore- oder ARM-Familien. Der Ansatz ist prinzipiell erweiterbar auf die Verifikation von Mixed-Signal-Schaltungen, von kleinen eingebetteten HW/SW-Systemen und von kontrollorientierten Systemaspekten. Die so erreichte Qualität kann durch Fortschritte beim digitalen bzw. analogen Äquivalenzvergleich auch bzgl. händischer oder automatischer Entwurfsverfeinerungen abgesichert werden. Zur Sicherstellung der Robustheit sicherheitskritischer Funktionen gegen Feldausfälle steuernder Mikrokontroller wird im Projekt eine weit reichende Zertifizierungstechnik aufgebaut.

Aufbauend auf diesen Erfolgen soll in einem zukünftigen Vorhaben (q.e.d.) auf Basis formaler und semiformaler Verifikationstechnik ein vergleichbarer Leistungssprung bei der Schnittstellen- und Architekturverifikation erfolgen.

Abbildung 1.4:

Betriebsfehler-Emulationsplattform PARSIFAL

Kont@kt:

Prof. Dr. Wolfram Büttner
Infineon Technologies AG
CL D DAT DF V
Otto-Hahn-Ring 6
81739 München
Fon: 089 234-46310
Fax: 089 636-42284

Weitere Informationen sind unter www.edacentrum.de/ekompass/projekte/valse.html zu finden.