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

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.

Ziel von VALSE-XT ist es, 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. Weiterhin 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.

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 mit folgendem technischen Programm:

» Eigenschaftsprüfung:
Mit Weiterentwicklungen der formalen Modulverifikation aus Valse und Anpassungen der Technik an die Besonderheiten von Mixed-Signal-Schaltungen 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 integriert wird. Die Basistechnik der formalen Modulverifikation soll darüber hinaus erprobt werden, um kleine, eingebettete HW/SW-Systeme sowie asynchrone Systemaspekte zu verifizieren.

» Äquivalenzvergleich
Es sollen problemspezifische Lösungen für den sequenziellen Äquivalenzvergleich entwickelt werden, um die nach obigem Vorgehen für die Designphasen erzielbare hohe Qualität in nachfolgenden Entwurfsschritten 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. Mit ganz andersartigen mathematischen Verfahren soll für Analogzellen die Übereinstimmung ihrer SPICE- und VHDL-Views garantiert werden.

» 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.

„Formale Modulverifikation“ (AP1)
In diesem Arbeitspaket 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. Auf Basis einer Normalisierungstechnik, die auf elementaren arithmetischen 1-Bit-Operationen beruht, können 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.

Die in AP1 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 vollständig zu verifizieren. In diesem Projekt wurden bisher ca. 1400 Eigenschaften erstellt und verifiziert. Diese Eigenschaften beschreiben etwa 70% der Funktionalität des Prozessors.

„Debugging für die formale Modulverifikation“ (AP2)
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.

Weiterhin wurde eine Prozedur entwickelt, um Zusammenhänge (Erreichbarkeitsinfor-

Projektinformation

Stand: Q1/2005

Förderkennzeichen
01 M 3069 A

Förderzeitraum
01.08.2003 bis 31.07.2005

Schlüsselworte:
Erschöpfende Modulverifikation, formale Verifikation, Äquivalenzvergleich, Betriebsfehleremulation

Kontakt:
Prof. Dr. Wolfram Büttner
Infineon Technologies AG
Otto-Hahn-Ring 6
81739 München
wolfram.buettner@infineon.com

Zusammensetzung des Prokjektkonsortiums:

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 fürIntegrierte Schaltungen Dresden
- Institut für mikroelektronische-und mikromechanische-Systeme GmbH
- Konrad-Zuse-Zentrum Berlin

mation) 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.

„Semiformale Modulverifikation“ (AP3)
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 die Korrektheit der Netzliste durch einen mathematischen Vergleich von VHDL- und SPICE-Views der beteiligten Analogzellen zu garantieren.

Der zweite Schwerpunkt von AP3 betrifft die Verifikation von Mixed-Signal-Blöcken per Eigenschaftsprüfung unter der Annahme korrekt arbeitender Analoganteile. Mit der digitalen Eigenschaftsprüfung konnte das Verhalten für alle 263 = 1019 Modi der Switch-Matrix verifiziert werden, was per Simulation nicht möglich wäre. Für komplexere Schaltungen kann die Technik auch hierarchisch angewendet werden.

„Kopplung formaler und simulativer Verfahren“ (AP4)
In diesem Arbeitspaket werden 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.

Weit übertroffen wurden die Erwartungen bzgl. einer effizienten Eigenschaftsprüfung von Simulationsläufen: Hier ist ein Werkzeugprototyp entwickelt worden, der Eigenschaften (s. AP1) in Monitore umwandelt, d.h. es entstand Software, die die Erfüllung von Voraussetzungen und das Fehlschlagen von Eigenschaften erkennt und meldet.

„Pfadfinderthemen der Systemverifikation“ (AP5)
In diesem Arbeitspaket 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 eines Typkonzeptes und benutzerdefinierbaren Prozeduren sowie eine ausführliche Dokumentation des Spezifikationsprototyps und der zugehörigen Methodik.

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.

„Sequenzieller Äquivalenzvergleich“ (AP6)
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.

„Betriebsfehleremulation“ (AP7)
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, Fehleraktiverung) unabhängig von der tatsächlich verwendeten Emulationsplattform entwickelt werden können.

Ausblick und Perspektiven
Der Erfolg der SoC-Perspektive hängt designseitig 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.