



## VALSE - Hochautomatisierte, zertifizierende und skalierende Validierung von „System-on-Chip“-Entwürfen

Die Realisierung kompletter Systeme auf einem Chip ist die große Herausforderung für EDA und die Verifikation dieser SoCs ist hier der ‚dickste Brocken‘. Kritisch für die Bewältigung dieser Aufgabe sind die Beherrschung der Interaktion im System, die Verfügbarkeit qualitativ hochwertiger Systemkomponenten und die Fähigkeit, das bei Nanometerstrukturen wachsende Risiko von Betriebsfehlern zu meistern. Mit formalen Methoden, das sind ausgeklügelte hochautomatisierte Beweisverfahren, und mit verbesserten Techniken zur Sicherung der Robustheit von Schaltungen gegenüber Betriebsfehlern bearbeitete VALSE im Zeitraum 4.2001 – 3.2003 die beiden letztgenannten Aufgabenschwerpunkte. Im Nachfolgeprojekt Valse-XT kommt seit August 2003 neben der Fortführung dieser Themen noch ihre Integration in den Mainstream der transaktionsbasierten Verifikationsplattformen zur Beherrschung der Verifikation auf Systemebene dazu.

### Positionierung des Vorhabens

Auf das seit Jahren beklagte „produktivität gap“, das ja vor allem von einer Verifikationskrise herührt, hat die EDA-Industrie mit Ansätzen für transaktionsbasierte Verifikationsplattformen reagiert. Ausgehend von der Mikroarchitektur eines SoC-Entwurfs soll sich die Verifikation/ Analyse dieser Architektur sowie nachfolgender Entwurfsverfeinerungen in einem festen Rahmen abspielen. Top-Down soll aus verifizierten Modellen der Systemkomponenten und ihrer Kommunikation eine verifizierte Implementierung entstehen. Dieser Rahmen integriert Testautomatisierungsinfrastruktur, Simulation für vielfältige Abstraktionsniveaus und Sprachen, die Modellierungsfähigkeiten von SystemC und SystemVerilog, Codechecker und Monitore sowie HW-Beschleuniger und Emulation. In Summe wird so die Last der RT-Systemverifikation durch Verteilung der Systemüberprüfung über Entwurfsebenen, schnelle Simulation, und Wiederverwendung von Testautomatisierungscodes sowie Simulationsstimuli reduziert. Das Zusammenspiel von HW und SW kann so in einem Sprachrahmen untersucht werden.

Für die Verifikation von Systemkomponenten bzw. Komponentenmodellen, ihrer korrekten Verfeinerung und protokollkonformer Kommunikation wird weiterhin auf Simulation gesetzt. Es bleiben daher für diese Aufgaben unverändert das prinzipielle Problem der Unvollständigkeit der Simulation, der Schwierigkeit aus der Systemperspektive effizient Fehler in Komponenten zu finden und die Tatsache, dass extreme Qualität von SoC-Komponenten ein ‚Muss‘ ist, weil die Wahrscheinlichkeit für korrektes Systemverhalten bestenfalls das Produkt der Wahrscheinlichkeiten für korrektes Verhalten der Systemkomponenten ist.

VALSE komplementiert daher den o.g. EDA-Mainstream mit speziellen Verifikationstechniken zur Bereitstellung von Höchstqualitätskomponenten. Formale Vergleichsverfahren sichern die auf RT-Ebene gewonnene Qualität in den Arbeitsschritten unterhalb dieser Ebene. Komplementär zum Mainstream sind auch die Arbeiten zur Betriebsfehleremulation. Triebfedern sind hier die zunehmende Anzahl von  $\mu\text{C}$ , die sicherheitskritische Funktionen ausführen, und daher robust gegen Funktionsveränderungen, z.B. durch Alterserscheinungen, sein müssen, und das bei Nanometerstrukturen wachsende Risiko von temporären Funktionsveränderungen z.B. durch Strahlungseinflüsse.

### Ergebnisse von Valse

#### Vollständige Verifikation von Blöcken:

Parallel zur RT-Codierung wird das erwartete Verhalten eines Blockes durch einen Satz von Eigenschaften vollständig beschrieben. Formale Eigenschaftsprüfung entdeckt dann frühzeitig jede Abweichung vom erwarteten Verhalten. Solche lokalen Fehler machen mindestens 50% aller funktionalen Fehler aus. Der Technikstand ist mit hohem Produktivitäts- und Qualitätsgewinn auf das Gros kontrollorientierter, digitaler Blöcke anwendbar. Evaluierungen der von Infineon entwickelten und von allen Projektpartnern angewendeten Technik an einer repräsentativen Auswahl von ASIC-Projekten konkretisieren diesen Nutzen:

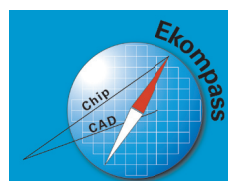
- garantierte Entdeckung aller lokalen Fehler; so Vermeidung umfänglicher Folgekosten (Redesigns, entgangene Gewinne durch verspäteten Markteintritt, Verzögerung anderer Projekte durch Reallokation von Ressourcen zur Fehlerbehebung, Imageschäden)

- 20–40% geringerer Aufwand verglichen mit der Fehlersuche durch Chip- bzw. Systemsimulation; für schwierige Blöcke Einsparungen bis über 90% (z.B. Blöcke mit vielen parallelen Operationen mit möglicherweise noch dynamisch wechselnden Konfigurationen);
- 30% Einsparungen bei Simulatorlizenzen/ Hardware (Messwert für vollständige Verifikation von 70k LoC (Lines of Code) VHDL in 80 Stunden deutet auf noch größeres Einsparpotenzial hin); schnellerer „ramp-up“ der Chip- bzw. Systemsimulation im Vergleich zur konventionellen Simulation;
- klares Kriterium, wann ‚genug verifiziert‘ wurde (Verifikation aller Eigenschaften); so gesteigerte Zuverlässigkeit der Projektplanung („time-to-market“);

Vor allem die Formale Verifikation aller Blöcke eines ASIC's mit über 10 Mio. Gattern (davon 2.2 Mio. neuentwickelte Logik) unter realen Randbedingungen ist als rekordverdächtiges Evaluierungsergebnis hervorzuheben. Der Technikbackground von Infineon wurde bereits in mehr als 30 ASIC-Entwicklungen eingesetzt. Ca. 150 Designer von Infineon und weitere 50 Designer aus Partnerfirmen wurden bis Ende 2002 ausgebildet.

#### Formale Analogzellenqualifikation:

Zwischen dem detaillierten SPICE-View einer Analogzelle und ihrem größeren VHDL-AMS-View wird für Zellen mit derzeit bis zu 100 Transistoren in einem mathematisch „harten“ Sinn vollautomatisch Äquivalenz nachgewiesen. In diese Kategorie fällt bereits ein relevanter Teil typischer Analogzellen. Bei zu erwartendem Technikfortschritt zeichnet sich folgender Nut-



### Projektinformation

#### Förderkennzeichen

01 M 3069

#### Förderzeitraum

01.03.2001 - 28.03.2003

#### Kontakt:

Prof. Dr. Wolfram Büttner  
wolfram.buettner@infineon.com

Infineon  
CL DAT DF LD V  
Otto-Hahn-Ring 6  
81730 München

## Zusammensetzung des Projektkonsortiums:

### Partner:

- » Infineon Technologies AG
- » Melexis GmbH
- » Robert Bosch GmbH

### Unterauftragnehmer:

- » Universität Frankfurt
- » Universität Hannover
- » Universität Tübingen
- » IMMS Erfurt
- » FHG, IIS/EAS, Dresden

zen einer solchen formalen Qualifizierung von Analogzellenbibliotheken ab:

- anstelle des aufwändigen Vergleichs per Simulation tritt eine ungleich sicherere Knopfdrucklösung
- ohne Qualitätsverlust kann bei der Verifikation eines Mixed-Signal-Blocks mit den VHDL-AMS-Views der Analogzellen des Blocks gearbeitet werden. Dadurch wird bei maximaler Sicherheit die Geschwindigkeit der Simulation um durchschnittlich eine Größenordnung gesteigert.
- in Kombination mit der Formalen Mixed-Signal-Blockverifikation (s.u.) entsteht eine geschlossene Verfahrenskette zur Verifikation von Mixed-Signal-Blöcken, die Qualität und Produktivität erheblich steigert.

### Hochautomatisierte Verifikation von Mixed-Signal-Blöcken:

Für Mixed-Signal-Blöcke mit ihrer im Vergleich zum Digitalentwurf noch schwierigeren Verifikationsproblematik wird in VALSE ein Durchbruch erzielt. Durch automatische Ersetzung des VHDL-AMS-Views der Analogzellen in einem Mixed-Signal-Block durch geeignete Diskretisierung oder durch manuelle Codierung entsteht eine digitale Verhaltensbeschreibung des Blocks, die mit der o.g. Formalen Blockverifikation hochproduktiv verifiziert werden kann. Bei massiver Steigerung von Qualität und Automatisierungsgrad erlaubt der entwickelte Ansatz anstelle einer aufwändigen Spezialentwicklung für Mixed-Signal ein sich abzeichnendes „Standardverfahren“ des Digitalentwurfs einzusetzen.

Die prinzipielle Praxistauglichkeit des Verfahrens wurde von Infineon und Melexis unabhängig bestätigt. Insbesondere die hochautomatisierte, formale Verifizierbarkeit der notorisch fehleranfälligen A/D-Schnittstelle wird durch Verifikation diverser industrieller A/D-Wandler und digitaler Ansteuerungen von Analogverstärkern aus Mobilfunk- und Automobilelektronikprodukten belegt. Evaluierungen bei Infineon und Melexis konkretisieren den Nutzen des Verfahrens:

- für A/D-Schnittstellen, deren Analogzellen durch VHDL-AMS-Views beschrieben sind, kann mit geringen Einschränkungen Simulation durch weit überlegene erschöpfende Eigenschaftsprüfung ersetzt werden und so aufgrund der Überprüfung aller Betriebsmodi die Redesign-Wahrscheinlichkeit gesenkt werden.
- Durch Vermeidung von Redesigns bei 20 von 100 Entwürfen erwartet Melexis von der Technik Kosteneinsparungen von jährlich 300 bis 1000T€. Durch Vermeidung eines Projektverzugs von 4-6 Monaten beim Kunden sind in vielen Fällen noch beträchtlich größerer Einsparungen möglich.

### Erschöpfender Vergleich von Entwurfsverfeinerungen/-optimierungen:

Formaler Äquivalenzvergleich erhält die durch Techniken wie die Formale Blockverifikation erzielte hohe Qualität von RT-Designs in nachfolgenden Entwurfsschritten. Vor allem durch Durchbrüche bei der Behandlung von Arithmetik und von Spezialfällen des sequenziellen Vergleichs wurde hier der Technikstand vorangebracht. Hauptvorteile dieser Entwicklungen sind:

- Formale Bibliotheksqualifizierung eliminiert bibliotheksbezogene Fehlerquellen; Vergleichsgeschwindigkeit wird um Faktor drei beschleunigt;
- Uneingeschränkter flacher Vergleich von Schaltungen mit komplexer Arithmetik beseitigt fundamentale Schwäche des Vergleichs; beschleunigte Vergleichsgeschwindigkeit; gesteigerte Vergleichssicherheit;
- Besseres Timing ohne Qualitätseinbuße durch formale Überprüfung von Synthese mit Pipeline-Retiming;

### Zertifizierung der Robustheit sicherheitskritischer Systeme gegen Betriebsfehler:

Die Robustheit von Anwendungssystemen gegen Feldausfälle steuernder Mikrocontroller wird durch die Arbeiten von Bosch bereits im Entwurf präventiv gesichert durch vollständige Identifizierung möglicher Betriebsfehler und

effiziente Analyse ihrer Folgen per Betriebsfehleremulation. Neben der Möglichkeit Standardemulation um das Feature Fehleremulation zu erweitern, schafft eine FPGA-basierte Realisierung der Betriebsfehleremulation eine performante und auch für die mittelständischen Unternehmen akzeptable Alternative. Folgender Nutzen zeichnet sich ab:

- moderne HW-Emulationssysteme bieten keine direkte Unterstützung des Features „Fehleremulation“; durch die Erweiterung des Funktionsumfangs von Standardemulation wird diese Lücke geschlossen; durch Reduzierung der Emulationszeit Einsparung von ca. 50% pro Sicherheitsnachweis in typischem Fehleremulationsprojekt und Verbesserung des Faktors „time-to-market“;
- für o.g. FPGA-basierte Fehleremulationsplattform verkürzt sich die Emulationszeit applikationsabhängig sogar um Faktor 10-20; die HW-Investitionen reduzieren sich um ca. 85%;
- die entwickelten Techniken erlauben die umfassende Validierung von sicherheitskritischen Systemen weit höherer Komplexität als bisher; daher Einsatz der Zertifizierungstechnik auch im sicherheitskritischen High-End-Bereich praktikabel (z.B. x-by-wire-systems);

### Ausblick auf Valse-XT

Im Rahmen von Valse-XT sollen in VALSE identifizierte Lücken bei der formalen Verifikation von digitalen und Mixed-Signal-Blöcken geschlossen, dieser Fortschritt in seiner Wirkung durch Kopplung mit simulationsbasierter Chip-Level-Simulation potenziert, das so erreichte Qualitätsniveau durch maßgeschneiderte sequenzielle Vergleichstechniken sichergestellt und durch den Ausbau der Betriebsfehleremulation auch auf die Ebene der Betriebsfehler ausgedehnt werden.

Dem Projektkonsortium gehören führende System- und Halbleiterhäuser sowie Forschungsinstitute an.

Der Projektaufwand belief sich in der ersten Phase (1.3.2001 - 28.2.2003) auf 50 Personenjahre. Die zweite Phase ist für die Zeit vom 1.8.2003 - 31.7.2005 mit 76 Personenjahren geplant.

