Schlussbericht zum Förderprojekt „Funktionale Verifikation von Systemen“

Zuwendungsempfänger	Albert Ludwigsuniversität Freiburg im Breisgau, Johann Wolfgang Goethe Universität Frankfurt am Main, Technische Universität Darmstadt, Technische Universität Ilmenau, Technische Universität Kaiserslautern, Universität Tübingen
Koordination	edacentrum
Förderkennzeichen	01M3072
Vorhabenbezeichnung	FEST: Funktionale Verifikation von Systemen
Laufzeit des Vorhabens	01.07.2004 – 30.06.2007

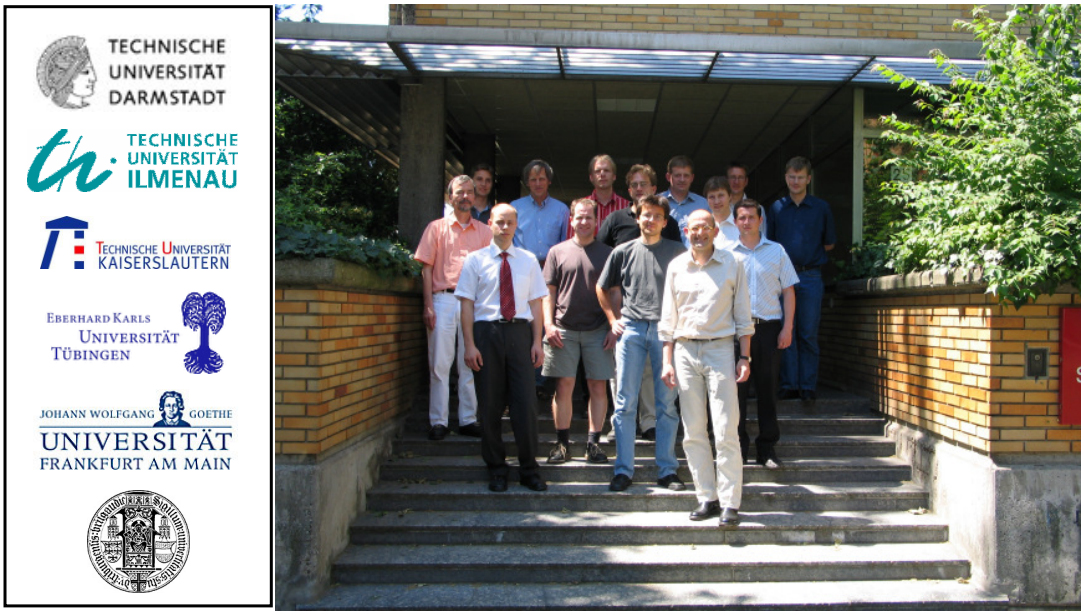

Abbildung 1: Forschungspartner im Projekt

Abbildung 2: BMBF und Industriepartner fördern das Projekt

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 01M3072 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegen bei den Autoren.

1 Ziele und Aufgaben

Das Projekt FEST hat sich zum Ziel gesetzt Lösungen zu erforschen, die eine einheitliche Verifikation von SoCs ermöglichen. Hierzu werden – ausgehend von einer Systembeschreibung – bis hinunter zur elektrischen Ebene Methoden und Verfahren erforscht, die vorhandene Verifikationslücken schließen und dadurch ein hohes Verbesserungspotenzial ermöglichen. Die Projektpartner unterstützen mit dem gewonnenen Forschungs-Know-how die Halbleiter-Industrie in Deutschland mit dem Ziel, die deutsche Kompetenz auf diesem Gebiet auch in Zukunft auf höchstem Niveau zu halten. Eine noch weiter gesteigerte Qualität in der Verifikationsmethodik ermöglicht es der deutschen Industrie Risiken von Entwurfsfehlern zu verringern und den dazu nötigen Aufwand zu minimieren. Die Verifikation – eine Schlüsselkomponente des SoC-Entwurfs – wird mit diesem Forschungsvorhaben nachhaltig gestärkt und verhilft der Industrie zu einer nachhaltigen Stärkung der Wettbewerbssituation. Mit dem Projekt werden Verifikationslücken geschlossen, um somit dem langfristigen Ziel eines geschlossenen Verifikationsflows von der Systemebene bis zur Transistorebene näher zu kommen. Die neu erforschten Modellierungsverfahren und Methoden ergänzen und verbessern bestehende Verfahren, so dass problematische Verifikationslücken geschlossen werden.

Dieser Bericht fasst die Arbeiten des Projekts zusammen. Einzelergebnisse und Details können aus den Berichten und Publikationen der Projektpartner entnommen werden. Die folgende Abbildung stellt die Themenschwerpunke des Projekts dar, die in zwei Arbeitspaketen bearbeitet werden. Die umfangreiche Literatur, die während der Projektlaufzeit veröffentlicht wurde, gibt einen detaillierten Einblick in die Forschungsergebnisse. Nutzen Sie hier die angegebenen Kontaktadressen.

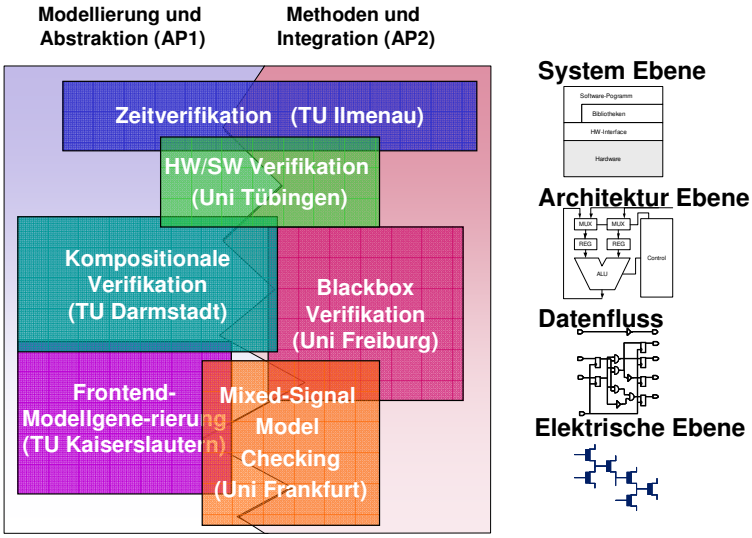

Abbildung 3: Themenschwerpunkte und Arbeitspakete im FEST-Projekt

2 Randbedingungen des Vorhabens

2.1 Motivation zu diesem Projekt

Durch eine permanente Reduzierung des Stromverbrauchs sowie durch neue technologische Integrationstechniken erleben wir stetig neue Anwendungsmöglichkeiten und eine beispiellose Miniaturisierung von elektronischen Produkten: Bis heute wird von Mikroelektronik und deren mikroelektronischen Systemen gesprochen, obwohl es sich längst um Nanoelektronik und nanoelektronische Systeme handelt. Mit ihren analogen Ein- und Ausgängen ermöglichen sie die Kommunikation mit dem Men-

schen, die Verbindung zu nicht-elektrischen Signalen sowie die effiziente Übertragung durch Funk. Durch ihre digitalen Prozessoren und Datenspeicher verwirklichen sie eine unvorstellbar leistungsfähige Datenverarbeitung, z.B. sind neueste Mobilfunkgeräte in der Lage Videos abzuspielen. Allein die Nanoelektronik bietet das Potenzial, um weiterhin den Leistungshunger bei Multimedia- und Spiel-Applikationen zu befriedigen. Diese nanoelektronischen Systeme sind hochintegrierte Bausteine und werden auch als „Systeme auf einem Chip“ (System on a Chip, SoC) bezeichnet. Die Miniaturisierung dieser SoCs bringt zwar viele Vorteile mit sich, aber auch große Herausforderungen:

- Hat man noch die Fähigkeiten Produkte in neuen Technologien fehlerfrei zu entwerfen?
- Ist die Größe der Entwurfteams für SoC-Entwürfe noch ausreichend?
- Wie lange dauert es ein System bis zur Marktreife ohne Fehler zu entwerfen?
- Kann die nationale Industrie noch die Produkte entwerfen, die zur Absicherung wichtiger deutscher Märkte notwendig sind?

Der Benutzer erwartet von diesen Produkten, dass alle Funktionen zuverlässig ausgeführt werden. Diese Anforderungen nach Zuverlässigkeit und Sicherheit stehen der wachsenden Komplexität nanoelektronischer Systeme gegenüber. Die Halbleiter-Industrie bewegt sich damit in einem Bereich, der sich durch höchste Anforderungen, Komplexität, Kurzlebigkeit der Produkte und extremen Kostendruck auszeichnet. Um sich hier zu behaupten, ist ein zuverlässiger Entwurfsprozess eine entscheidende Voraussetzung. Dieser zuverlässige Entwurfsprozess kann aber nur zur Verfügung stehen, wenn die Anstrengungen, die zur Qualitätssicherung unternommen werden müssen, in Zukunft noch weiter gesteigert werden.

2.2 Viele lukrative Märkte haben sehr hohe Anforderungen an die Zuverlässigkeit

Die deutsche Industrie hat sich in Märkten etabliert, die sehr hohe Anforderungen an die Zuverlässigkeit stellen. Exemplarisch sind hier zwei Märkte beschrieben. In der Automobiltechnik erfolgen die meisten Innovationen schon jetzt nur in Verbindung mit der Nanoelektronik. Hier sind die Bereiche Infotainment, fahrerunterstützende Systeme, Zuverlässigkeit und Sicherheit hervorzuheben. Der Industrie ermöglichen diese Innovationen sich insbesondere im Premiumsegment von anderen Wettbewerbern zu differenzieren. Die Selbstverpflichtung der europäischen Mitgliedsstaaten zur Halbierung der Anzahl der Unfalltoten wird die Anwendungen von SoC-Produkten beschleunigen, um der Anforderung nach mehr Sicherheit im und am Auto nachkommen zu können. So hat laut Statistischen Bundesamt ein falscher Reifendruck im Jahre 2002 rund 25 Prozent der Verkehrsunfälle verursacht. Elektronische Reifendruck-Sensoren können hier zusätzlich Sicherheit schaffen. Ein von einer deutschen Firma beherrschter Markt sind Sicherheits- und Smartcards-ICs. Hier dominiert Infineon den weltweiten Markt, gefolgt von Philips und STM. Das Marktvolumen ist zwar nicht groß, ist aber in vielen Massenprodukten zu finden. Beispiele sind intelligente Kreditkarten, Mobilfunktelefon und elektronische Schlüsselsysteme. Durch den Zuwachs an mobilen Anwendungen und der schnellen und sicheren Authentifizierung wird die Bedeutung von Sicherheit-ICs in Zukunft stark wachsen und eine Schlüsselstellung beim Entwurf von komplexen Sicherheitsanwendungen werden.

2.3 Zuverlässigkeit ist eine Tugend zukünftiger SoCs

Die Anforderungen an Sicherheit und Zuverlässigkeit steigen, wenn nanoelektronische Produkte für immer neue Anwendungen im Auto eingesetzt werden. In diesem Zusammenhang ist eine der großen Schwachstellen beim Schaltungsentwurf die Überprüfung der implementierten Funktionalität der komplexen Systeme. Als prominentes Beispiel einer Verifikationslücke beim Chip-Entwurf kann der als Pentium-Bug bezeichnete Fehler der Firma Intel genannt werden. Die Firma hatte einen massiven Gewinneinbruch in dem Jahr, in dem ein eklatanter Fehler in bereits ausgelieferten Pentium-

Prozessoren festgestellt wurde, der auf eine Verifikationslücke zurückzuführen war. Dieses steht aber nur als Synonym für eine in der Technik bekannte Problematik von unzulänglich implementierten oder unzureichenden Spezifikationen. Sie werden über Errata-Listen den Kunden mitgeteilt werden, die die Auswirkungen der Fehler umgehen müssen.

2.4 Neue Anforderungen werden an den Entwurfsprozess gestellt

Simulationstechniken reichen schon lange nicht mehr aus, um Entwurfsfehler wie den Pentium-Bug aufzudecken. Eine Simulation prüft exemplarisch mit ausgewählten Daten, ob beispielsweise eine arithmetische Operation ausgeführt werden kann. Alle möglichen arithmetischen Operationen in modernen Schaltungen auszuführen hieße, dass die Simulationen Monate oder gar Jahre benötigen, was inakzeptabel ist. Eine Verifikation hingegen kann prüfen, ob in allen möglichen Fällen die arithmetische Operation richtige Ergebnisse liefert. Sie kann darüber hinaus Gegenbeispiele liefern, an welcher Stelle der Schaltungsentwurf versagt. Solche Berechnungen können schon nach wenigen Minuten oder Stunden abgeschlossen sein. Dies verdeutlicht, dass die Verifikation eine entscheidende Komponente beim Schaltungsentwurf ist, deren Auswirkungen über Verlust oder Gewinn einer Firma entscheiden. Im Projekt VALSE-XT zeigte ein Vergleich mit einem simulationsbasierten Ansatz die Überlegenheit der formalen Methodik, da die Steigerung der Entwurfsqualität mit einem geringeren und besser vorhersagbaren Verifikationsaufwand einhergeht.

Die Komplexität des Entwurfsprozesses – bedingt durch die Miniaturisierung der nanoelektronischen Strukturen – wächst stark an. Neben der oft fehlenden Kompetenz, komplexe Systeme überhaupt entwerfen zu können, werden die ausufernden Kosten für den SoC-Entwurf zu einem weiteren großen Problem. Hinzu kommt, dass die Einmal-Kosten zur Produktionsvorbereitung bei neuen Technologien einen großen Kostenanteil bei der Produktentwicklung ausmachen. Sie wachsen mit dem Einsatz neuester Lithographieverfahren so stark an, dass ein Re-Design des Produkts zusammen mit der zusätzlichen Lieferverzögerung ein großes finanzielles Risiko bedeutet. Es ist daher bereits beim ersten Entwurf von entscheidender Bedeutung, jeden Fehler zu vermeiden, der ein Re-Design erfordern würde (First-Time-Right). Notwendig dazu sind neue und umfassendere Lösungen in allen Bereichen der Verifikation. Diese Problematik wird noch dadurch verschärft, dass in den oben beschriebenen Märkten höchste Anforderungen an die Entwurfsqualität der Nanoelektronik gestellt werden: Die Verifikation entwickelt sich zur Achillesverse des SoC-Entwurfs. Gesteigert wird dieses Problem dadurch, dass die Software zu einem unzuverlässigen Verhalten bei Funktionen beiträgt. Die Erforschung einer gemeinsamen Verifikationsmethodik für Hardware und Software stellt die größte Herausforderung in der Verifikation in den nächsten Jahren dar.

Eine geschlossene Lösung zur Verifikation komplexer SoCs ist auf dem EDA-Markt nicht verfügbar. Es gibt nur punktuelle Lösungen, die einen reduzierten Bereich eines SoC-Entwurfs verifizieren. Um für die oben beschriebenen Probleme Lösungen anbieten zu können, müssen auf allen Ebenen des Schaltungsentwurfs innovative und umfassende Verifikationsmethoden erforscht werden. Zur Erhöhung der Sicherheit und Zuverlässigkeit der Nanoelektronik ist dabei der Einsatz der richtigen Verifikationsverfahren beim SoC-Entwurf der Schlüssel zum Erfolg. Dabei sollen durch die Erhöhung der Produktivität die Entwurfskosten und -zeit der SoCs reduziert werden.

3 Zur innovativen Clusterforschung

Die Clusterforschung sind spezielle Projekte, die durch das edacentrum initiiert werden. Sie unterstützen Universitäten und Forschungseinrichtungen in der Methodenforschung für den industriellen Einsatz. Dabei sollen Machbarkeitsstudien erstellt werden, die das Ziel haben, dass ein Industrieller Einsatz in 5-10 Jahren möglich ist. Sie bereiten dabei mit ihrer Methodikforschung klassisches F&E Projekte vor. Clusterforschungsprojekte haben eine typische Größe von 5-6 Personen, die in 3 Jahren an

einem von der Industrie gestellten Thema arbeiten. Die Koordination der Projekte erfolgt durch das edacentrum. Eine praxisnahe Betreuung, wie die Bereitstellung von Demonstratoren, erfolgt durch die Industriepartner. Ca. alle 1,5 Jahre startet ein neues Clusterforschungsprojekt.

Die Industriepartner wählen das Forschungsthema für die Clusterforschungsprojekte aus. Hierzu werden Themenvorschläge durch das RSS Leitungsgremium vorgeschlagen. Ein Industriegutachtergremium wählt das Konsortium unter den eingereichten Themenvorschlägen der Forschungseinrichtungen aus. Die Industriepartner übernehmen die Finanzierung des Industrieanteils, die sich aus den Industriepartnern der aktuellen Ekompass-Projekte ergibt. Sie sind weiterhin Ratgeber für industrielle Anforderungen und stellen industrielle Demonstratoren zur Verfügung. Die Industriepartner verwerten und nutzen die neue Entwurfsmethoden zur Verbesserung ihrer Entwurfsmethodik. Dabei erfolgen die Anpassungen an industrielle Anforderungen in der Regel über neue F&E Projekte.

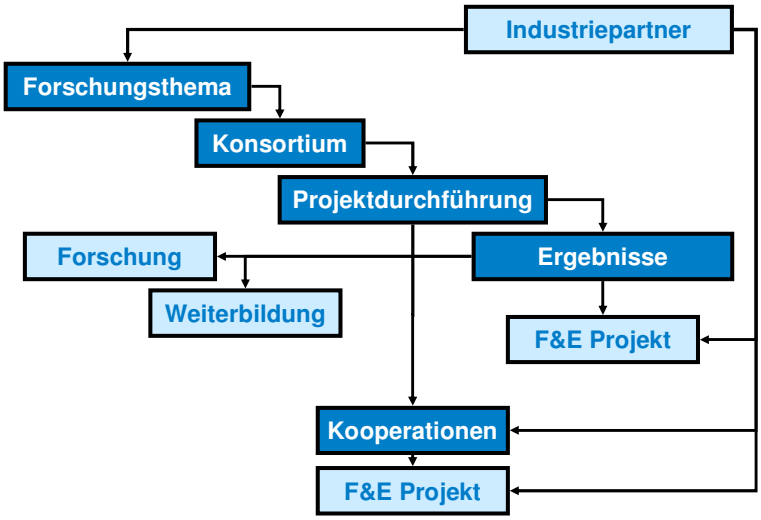

Abbildung 4: Nutzung und Verwertung von Clusterforschungsergebnissen für die Industrie

4 Planung und Ablauf des Vorhabens

Das Projekt teilt sich zwei Arbeitspakete auf, die sich in Aufgaben gliedern. Die Aufgaben werden von den einzelnen Partnern in ihrem partnerspezifischen Bericht individuell beschrieben.

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
Phase	Arbeitsinhalte	2004-09	2004-12	2005-03	2005-06	2005-09	2005-12	2006-03	2006-06	2006-09	2006-12	2007-03	2007-06
P1	Erforschen und Evaluieren von neuen Methoden	P1: Erforschen und Evaluieren von neuen Methoden											
P2	Implementieren von Verfahren		P2: Implementieren von Verfahren										
P3	Validieren der Verfahren							P3: Validieren der Verfahren					

Abbildung 5: Das Projekt lief in drei sich überlappenden Phasen ab

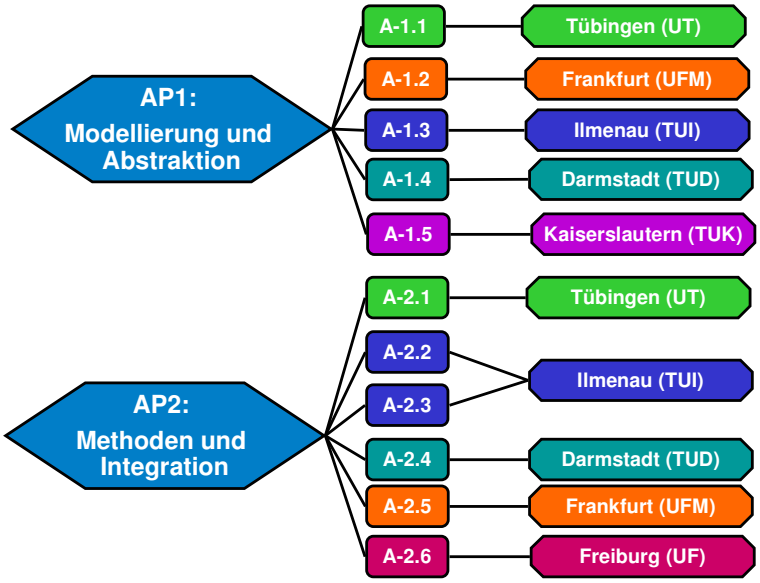

Abbildung 6: Das Projekt teilte sich in 2 Arbeitspakete auf

Meilenstein	Partner	Abgabe	Beschreibung
M1-A1.2-1	UFM	31.12.2004	Konzept zur Modellierung von Mixed-Signal-Modellen
M1-A1.3-1	TUI	31.12.2004	Konzeption der Constraint Language
M1-A1.5-1	TUK	31.12.2004	Konzeption einer Bitebenen-Normalform für die Behandlung von Arithmetik
M1-A1.5-2	TUK	31.12.2004	Konzeption der Frontend-Maßnahmen zur Behandlung von sequenziellem Verhalten
M1-A1	AP1	30.06.2005	Spezifikation einer Modellierungsumgebung
M1-A1.1-1	UT	31.12.2005	Definition eines einheitlichen HW/SW Modell zur Verifikation
M1-A1.1-2	UT	31.12.2005	Entwicklung einer Methode zur Extraktion von Verifikationseigenschaften
M1-A1.4-1	TUD	30.06.2005	Konzeption eines Modellgenerators und Bewertung von Implementierungsalternativen
M2-A1.5-1	TUK	31.12.2005	Implementierung der Invariantengenerierung zur Behandlung sequenzieller Systeme
M2-A1.5-2	TUK	31.12.2005	Analyse des Konvergenzverhaltens der Automatentraversierung
M2-A1	AP1	30.06.2006	Methodik zur Modellierung und Abstraktion
M2-A1.1-1	UT	30.09.2006	Integration der Methode zur Extraktion von Eigenschaften mit existierenden Verifikationstools/Techniken
M2-A1.2-1	UFM	30.06.2006	Verfahren zur automatischen Modellierung von Mixed-Signal-Modellen
M2-A1.4-1	TUD	31.12.2006	Implementierung des Modellgenerators
M2-A1.5-3	TUK	31.12.2006	Integration der Modellierungskonzepte für Arithmetik in einen SAT-Solver
M3-A1	AP1	30.06.2007	Ergebnisse der Validierung der Modellierungs- und Abstraktionstechniken
M3-A1.1-1	UT	30.06.2007	Validierung des entwickelten Extraktionsverfahrens an einem realen Beispiel
M3-A1.3-1	TUI	30.06.2007	Validierung des implementierten Konzepts zur Behandlung von Zeiteigenschaften und deren Restriktionen
M3-A1.4-1	TUD	30.06.2007	Validierung des Modellgenerators an einem industriellen Beispiel
M3-A1.5-1	TUK	30.06.2007	Validierung der entwickelten Techniken an Beispielen komplexer Arithmetik

Abbildung 7: Meilensteine in AP1

Meilenstein	Partner	Abgabe	Beschreibung
M1-A2.6-1	UF	31.12.2004	Spezifikation von Methoden für die approximative Eigenschaftsprüfung für Systeme mit Black-Boxes
M1-A2	AP2	30.06.2005	Spezifikation der Algorithmen und Verfahren
M1-A2.1-1	UT	30.06.2005	Erforschung von semi-formalen Verifikationstechniken
M1-A2.4-1	TUD	30.06.2005	Erforschung von Techniken zur verifikationsgerechten Spezifikation von Blockinteroperabilität
M1-A2.5-1	UFM	30.06.2005	Konzept zur Verifikation von Mixed-Signal-Modulen
M2-A2.6-1	UF	30.06.2005	Integration der Konzepte Black-Box-Eigenschaftsprüfung und Evaluierung anhand „kleiner“ Beispiele
M1-A2.2-1	TUI	31.12.2005	Spezifikation des Dekompositionsverfahrens unter Verwendung der Constraint Language für die Zeitverifikation
M1-A2.3-1	TUI	31.12.2005	Spezifikation der Algorithmen und Verfahren mit Hilfe der Modellierungen aus AP1 und Untersuchung der Transformationenverfahren an Beispielmodellen
M2-A2.6-2	UF	31.12.2005	Anwendung der Konzepte und Anpassung auf Generierung von Gegenbeispielen
M2-A2	AP2	30.06.2006	Integration der Verfahren
M2-A2.1-1	UT	30.06.2006	Integration eines semi-formalen Analyseverfahrens in ein Werkzeug
M2-A2.4-1	TUD	30.06.2006	Methodik für die kompositionale Verifikation von Systemeigenschaften
M2-A2.5-1	UFM	30.06.2006	Methoden zur Verifikation von Mixed-Signal-Modulen
M2-A2.6-3	UF	30.07.2006	Anwendung der Konzepte und Anpassung auf Fehlerlokalisierung
M2-A2.3-1	TUI	31.12.2006	Implementierung der Transformationsverfahren
M2-A2.6-4	UF	31.12.2006	Weiterentwicklung der Verfahren und prototypische Implementierung
M3-A2	AP2	30.06.2007	Ergebnisse der validierten Verfahren und Algorithmen
M3-A2.1-1	UT	30.06.2007	Validierung des entwickelten semi-formalen Analyseverfahrens an einem realen Beispiel
M3-A2.2-1	TUI	30.06.2007	Implementierung und Validierung des Dekompositionsverfahrens für die Zeitverifikation
M3-A2.3-1	TUI	30.06.2007	Validierung der implementierten Verfahren und Algorithmen
M3-A2.4-1	TUD	30.06.2007	Validierung der Methodik am Beispiel des ARM AHB Protokolls
M3-A2.5-1	UFM	30.06.2007	Validierung des Verfahrens zur Verifikation von Mixed-Signal-Modulen
M3-A2.6-1	UF	30.06.2007	Demonstration und Validierung der Verfahren in einer Verifikationsumgebung durch industrierelevante Beispiele

Abbildung 8: Meilensteine in AP2

5 Stand der Wissenschaft und Technik zu Beginn des Vorhabens

Das Projekt teilt sich in 6 Domänen der Forschung zur Verbesserung der Verifikationsmethodik auf. Diese sind im Überblick dargestellt.

5.1 Zeitverifikation auf Systemebene

Für die Zeitverifikation im hierarchischen Mehrebenenentwurf existieren derzeit Verfahren zur bevorzugten Anwendung in den unteren Abstraktionsebenen. Diese eignen sich nicht für den Einsatz auf Systemebene und ermöglichen dort nur eine stark reduzierte Verifikation. Wichtige Vorläuferarbeiten sind RAVEN [Ruf99], welches die Zeitverifikation mit Clocked-Computation-Tree-Logic und diskreten Zustandsautomaten bearbeitet. UPPAAL [Upp] ist ein Werkzeug zur Zeitverifikation, das mit Hierarchical-Timed-Automata und diskreten Intervallen arbeitet. Weitere Forschungsergebnisse sind in den Prototypen T-MSC eingeflossen [FeKDHS01], [FeHFS02], das die Zeitverifikation mit so genanten Message-Sequence-Charts und die Überführung in Zeitintervall-Petrinetze ermöglicht.

Der Entwurf auf Systemebene erfolgt domänenübergreifend. Für die Zeitverifikation auf Systemebene wird deshalb die Integration unterschiedlicher Modellierungsdomänen benötigt. Diese Eigenschaft

fehlt allen beschriebenen Prototypen. Auch existiert keine ausreichende Unterstützung in einem EDA-Tool. Die im hierarchischen Mehrebenenentwurf bestehende Notwendigkeit zur Unterstützung mehrerer Abstraktionsebenen im Verifikationsprozess ist ebenfalls im heutigen Stand der Technik nicht ausreichend vorhanden.

Am Institut für Theoretische und Technische Informatik werden Grundlagen für Entwurfssysteme für komplexe eingebettete Systeme (z.B. autonome mobile Systeme [Ze03], Nanopräzisionsmaschinen [FeDDL03] und SoC) auf Missions- und Systemlevel für verschiedene Entwurfsdomänen erforscht. Gegenstand sind beispielsweise Multi-Level- und Multi-Resolution-Technologien für die Modellierung sowie effiziente Simulationsalgorithmen für Multi-Domain-Umgebungen. Diese waren und sind Basis des Design-Tools ML-Designer der MLDesign GmbH Ilmenau. Weiterhin existieren Forschungsergebnisse auf dem Gebiet der Modellierung, Verifikation und Modelltransformation von kontinuierlich-diskreten Systemen [FrZ03] unter Berücksichtigung der Modellvielfalt und ihrer zeitlichen Eigenschaften, die im Wesentlichen im DFG-Schwerpunkt 1040 [FeKDHS01] und im Graduiertenkolleg GRK 164/1-96 entstanden. Beispielsweise wurden umfangreiche Untersuchungen zur Verifikation technischer Systeme mit Hilfe zeitintervallbewerteter Petrinetze durchgeführt. Zusammenfassend resultieren umfangreiche Erfahrungen sowohl im Bereich der Erstellung und Verifikation von Modellen als auch bezüglich Modellierungswerkzeugen und Modellierungstechnologien.

5.2 HW-/SW-Verifikation

Die meisten Ansätze im Bereich der HW-/SW-Verifikation basieren auf der separaten Verifikation des Software- und des Hardwareanteils. Für beide Teilsysteme kommen traditionelle Ansätze der symbolischen Modellprüfung oder Äquivalenzprüfung zum Einsatz. Ansätze, die das HW-/SW-System als Ganzes betrachten, sind unter der Bezeichnung der Co-Verifikation bekannt geworden. Die bekanntesten Co-Verifikationsverfahren sind eng mit der Co-Simulation von Systemen verbunden, wobei Hardware- und Softwarekomponenten (SW-Komponenten) gemeinsam mit ihrer Schnittstelle simuliert werden. So werden beispielsweise im Ansatz von Lavagno [LaSe97] beide Komponenten auf spezielle endliche Automaten reduziert und dann mit Verfahren der Modellprüfung verifiziert. In [KuLMPY02] wird die symbolische Modellprüfung mit partiellen Reduktionstechniken kombiniert um HW-/SW-Systeme zu verifizieren. Die bisherigen Ansätze gehen meist entweder von partitionierten Systemen aus oder bieten keine Lösung für die Verifikation von gemischten HW-/SW-Systemen.

Der Antragsteller ist seit vielen Jahren auf dem Gebiet der formalen Verifikation aktiv [KuSK93]. Die Forschungsarbeiten haben zu zahlreichen internationalen Veröffentlichungen sowie zu einem Standardlehrbuch über dieses Gebiet geführt [Kr99]. Aktuelle Arbeiten umfassen Forschungsaktivitäten im Bereich der formalen Verifikation von Systemen, insbesondere in den Bereichen Systembeschreibungssprachen, symbolische Modellprüfung, Verifikation und Extraktion von Zeiteigenschaften, kombinatorische Äquivalenzprüfung, Fehleranalyse und semi-formale Verifikationstechniken [RuK98], [RuK00], [RuHKR01]. Des Weiteren verfügt das Institut über Expertise im Bereich der Modellierung von HW-/SW-Systemen. So umfassen frühere Arbeiten beispielsweise die Definition einer Verifikationssemantik für die Hardwarebeschreibungssprachen Verilog und VHDL sowie der Systembeschreibungssprache SystemC [MuRHGR01]. Aus den bisherigen Arbeiten sind u.a. das Werkzeug RAVEN im Bereich Zeitverifikation sowie das Werkzeug AC3 im Bereich Fehlerdiagnose entstanden.

5.3 Verifikation auf Architekturebene

Die auf dem sog. Bounded-Model-Checking basierenden industriellen Verifikationswerkzeuge zur Eigenschaftsprüfung erlauben derzeit nur die Behandlung einzelner RT-Blöcke bis zu ca. 50.000 Gatter, aber nicht von kompletten Systemen [BiCC99]. Die Überprüfung von Architektureigenschaften geschieht deshalb meist mit schwächeren Techniken wie z.B. durch Simulation. Durch eine Leistungssteigerung der Basisverifikationswerkzeuge alleine wird sich an dieser Situation aufgrund des gleich-

zeitigen Anwachsens der Systemgröße nichts ändern. Ein alternativer Ansatz, die Komplexität der handhabbaren Blöcke zu steigern, liegt in der Verwendung von Black-Box-Techniken, die in diesem Projekt erforscht werden sollen. Ein Hauptaugenmerk liegt dabei auf der Eigenschaftsprüfung: Zum Model-Checking von Eigenschaften vollständig spezifizierter Schaltungen existieren zwar ausgereifte Werkzeuge wie z.B. SMV [BUCMDH92], VIS [VIS96]. Allerdings wählen diese Werkzeuge zur Modellierung von Implementierungen mit unvollständiger Information eine Ersetzung der Black-Box-Ausgänge durch so genannte Pseudo-Inputs. Diese Vorgehensweise ist unzureichend und kann zudem zu fehlerhaften Ergebnissen führen.

Das Fachgebiet Rechnersysteme der Technischen Universität Darmstadt betreibt seit über 10 Jahren intensive Forschung auf dem Gebiet der formalen Verifikation [Ev00]. In der Vergangenheit entstanden Arbeiten insbesondere auf den Gebieten: Verifikation von Entwürfen auf RT-Ebene, Entwicklung und Anwendung von Multi-Domain Entscheidungsdiagrammen, Verifikationsmethodik. In letzter Zeit hat sich der Forschungsschwerpunkt zunehmend auf Verifikationsverfahren für höhere Entwurfsebenen verlagert unter Benutzung von Techniken der symbolischen Simulation [Ri00], die Unterstützung von Esterel [BlELR01] und anderer synchroner Programmiersprachen, und schließlich Techniken des eigenschaftsbasierten Entwurfs. Der Modellierungsgesichtspunkt wurde mit der Erarbeitung einer XML-basierten Repräsentation von Modellen behandelt [LeKEB02].

Das Institut für Informatik bildet zusammen mit dem Institut für Mikrosystemtechnik die Fakultät für Angewandte Wissenschaften der Universität Freiburg. Einer der Forschungsschwerpunkte dieser Fakultät liegt im Entwurf, in der Analyse und in der Verifikation von eingebetteten Systemen. Ein wesentliches Schwerpunktthema insbesondere am Institut für Informatik ist die Entwicklung und Anwendung Formaler Verifikationsmethoden. Die Antragsteller selbst arbeiten seit über 10 Jahren auf dem Gebiet des computerunterstützten Schaltkreis- und Systementwurfs, hier insbesondere in den Bereichen Verifikation, Test und Synthese. Auf allen Gebieten konnten international anerkannte Ergebnisse erzielt werden, die Eingang in die industrielle Anwendung gefunden haben. Für den Bereich Verifikation sei hier insbesondere auf die Arbeiten zur symbolischen Zustands-Traversierung [HeSB00], [GUHeB01], [HeB01] und zur kombinatorischen Äquivalenzprüfung bei unvoll-ständiger Information [ScB01b], [ScB02a], [ScB02b] verwiesen. Sie stellen wichtige Vorarbeiten für die hier geplanten Vorhaben dar. So sind Algorithmen zur Zustands-Traversierung eine wesentliche Komponente bei der Eigenschaftsprüfung. Die Arbeiten zur Modellierung unvollständiger Information bei der kombinatorischen Äquivalenzprüfung sind notwendige Voraussetzung für die geplante Entwicklung von Black-Box-Techniken bei der Eigenschaftsprüfung.

5.4 Verifikation auf RT-Ebene

Für die Verifikation auf RT-Ebene steht zwar seit geraumer Zeit eine Palette von Verfahren für die Eigenschaftsprüfung zur Verfügung, allerdings konnte sich erst kürzlich eine spezielle Ausprägung der Eigenschaftsprüfung auf Basis von Satisfiability-Solving (SAT-Solving) im größeren Stil industriell durchsetzen. Dieses so genante Bounded-Model-Checking [BiCC99] erlaubt es, Blöcke von bis zu 50k Gatter robust zu bearbeiten. Allerdings stößt diese Technik bei der Verifikation komplexen sequentiellen Verhaltens sowie bei Arithmetik schnell an ihre Grenzen. Bei der Verifikation sequentiellen Verhaltens können sehr lange Untersuchungsfenster entstehen, die bei der Abbildung auf ein SAT-Problem zu extrem großen kombinatorischen Blöcken führen. Arithmetik liefert besonders schwierige Problemstellungen für die Beweiser, da die arithmetische Natur des Problems von den rein auf Aussagenlogik beruhenden Beweisern nicht ausreichend berücksichtigt wird. Die aktuelle Forschung konzentriert sich vor allem auf die Effizienzsteigerung der zugrunde liegenden Beweiser. Es existieren auch einzelne Arbeiten zur Vorverarbeitung auf der RT-Ebene. Spezielle Modellierungstechniken zur Abbildung der RT-Beschreibung auf die Booleschen Beweiser, wie sie in diesem Projekt untersucht werden sollen, sind dagegen bis auf einige stark eingeschränkte Arbeiten unerforscht.

Die Arbeitsgruppe hat langjährige Erfahrung in den Bereichen Testen, Synthese mikro-elektronischer Systeme und formale Hardwareverifikation. Prof. Kunz gehört zu den Begründern der heute weit verbreiteten Methodik des strukturellen Äquivalenzvergleichs, die als Wegbereiter der formalen Verifikation in industriellen Anwendungen diente und unverzichtbar geworden ist. Aktuelle Arbeiten zeigen viel versprechende Fortschritte im Bereich des sequenziellen Äquivalenzvergleichs [StK97] sowie des Äquivalenzvergleichs für Arithmetik [StK01]. Ergebnisse der Arbeitsgruppe sind weltweit in Industriewerkzeuge eingeflossen. Die Erfahrungen auf dem Gebiet des Äquivalenzvergleichs stellen eine gute Grundlage für die hier geplanten Untersuchungen zur Eigenschaftsprüfung dar.

5.5 Verifikation auf elektrischer Ebene

Für rein analoge, stark nichtlineare, dynamische Schaltungen sind erst wenige Ansätze zum Equivalence-Checking und Model-Checking bekannt [HeH01], [HaHB02]. Auch für Mixed-Signal-Systeme gibt es nur wenige Ansätze, die aus dem Umfeld der formalen Verifikation für digitale Systeme stammen. Sie sind häufig auf die analoge Schaltungsklasse linearer Systeme eingeschränkt oder behandeln Sonderklassen, wie z.B. Timed-Automata [HeHW97]. Tragfähige Ansätze für Systeme mit Digitalteil und stark nichtlinearem, dynamischem Analogteil sind nicht bekannt. Da jedoch in zunehmendem Masse in SoCs Mixed-Signal-Module enthalten sein werden, wird eine neue Verifikationsmethodik und -modellierung, die möglichst viele Schaltungsklassen und verschiedene Abstraktionsebenen umfasst, dringend benötigt.

Das Institut für Informatik arbeitet mit den Arbeitsgruppen aus der Technischen Informatik schon seit langer Zeit auf dem Gebiet der Entwurfsautomatisierung mikroelektronischer Schaltungen. Der Antragsteller ehemals aus dem Fachgebiet Entwurfsautomatisierung des Institut für Mikroelektronische Systeme an der Universität Hannover bearbeitet seit langem als Forschungsschwerpunkte Methoden zum Entwurf analoger Schaltungen. Diese gliedern sich in die Themen symbolische Analyse, Verhaltensmodellgenerierung, Synthese und formale Verifikation auf [HeB95], [HeH01], [HaHB02]. Eine damit einhergehende Untersuchung der erfolgreichsten Verfahren zur formalen Verifikation hybrider und digitaler Systeme stellt eine fundierte Kenntnis der notwendigen Grundlagen für die Entwicklung von formalen Methoden für Mixed-Signal-Systeme sicher. Auch auf dem Gebiet der toleranzbehafteten Schaltungen sind Untersuchungen gemacht worden [HeB98]. Die Ergebnisse auf dem Gebiet des Equivalence-Checkings analoger Schaltungen finden in Zusammenarbeit mit einem Industriepartner/Infineon gerade Eingang in dessen Validierungsumgebung.

6 Zusammenarbeit mit anderen Stellen

Das Projekt hat auf vielfältige Weise kooperiert. Hier stand im Vordergrund, dass die Industriepartner des Projekts durch gemeinsame Diskussionen, Präsentationen und Workshops neue Aspekte der Verifikation erfahren. Als herausragendes Beispiel ist hier der Kooperations-Workshop Verifikation am 16.10.2007 in Hannover genannt. Verschiedene Beiträge von Ekompass-Projekten (FEST, HERKULES, URANOS, VeronA und VISION) wurden präsentiert. Das Ziel des Workshops war der Austausch von Gedanken, Sichtweisen, Lösungsansätzen, Erfahrungen zum Thema Verifikation. Der Workshop erfolgte in Kombination mit Arbeitsgruppen und Vorträgen. Das FEST-Projekt war mit einer Reihe vorn Präsentationen vertreten:

- Hans Eveking: Assertions und Eigenschaften auf Systemebene
- Stefan Lämmermann: Assertion basierte Verifikation auf verschiedenen Abstraktionsebenen
- Wolfgang Kunz: Formale Verifikation software-implementierter Protokolle
- Sebastian Steinhorst (VERONA/FEST): Formale Methoden zur Verifikation analoger Schaltungen

Die Projektpartner sind am Ende der Projektlaufzeit eng in den Ekompassverbund eingebunden. Weitere Beschreibungen von Kooperationen und Technologietransfer in die Industrie befindet sich in den Berichten der Partner.

7 Verwendung der Zuwendung und des erzielten Ergebnisses mit Gegenüberstellung der vorgegebenen Ziele

Es ergibt sich ein hervorragendes Verhältnis zwischen dem Einsatz der Zuwendung und den Ergebnis des Projekts. Es wurden eine Fülle von Publikationen, Demonstratoren und Berichten mit einem sehr geringen Budget fertig gestellt. Den hohen Einsatz der konnte man beispielsweise daran erkennen, dass zu Projekttreffen pro Forschungspartner 2-4 Personen angereist sind, obwohl nur eine Person gefördert wurde. Darüber hinaus sind die Aktivitäten der Industriepartner im Projekt zu erwähnen. Obwohl ihre Leistungen nicht gefördert wurden, standen sie mit Rat und Tat bei der Ausrichtung des Projekts den Forschungspartnern zur Seite und zu den Erfolgen bei. Weitere Darstellungen befinden sich in den Berichten der Partner.

8 Wichtige Positionen des zahlenmäßigen Nachweises

Das Projekt wurde mit 537.305 € jeweils von dem BMBF und eine m Industriekonsortium gefördert. Das Industriekonsortium plant die Nutzung und Verwertung der Ergebnisse, um ihre industrielle Verifikationsmethodik in 5-10 Jahren zu verbessern.

9 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die hervorragenden wissenschaftlichen Ergebnisse konnte nur durch die Einbindung von Kompetenzzentren aus der Forschung erreicht werden, die hochwertige Ergebnisse schon nach kurzer Zeit erreichen konnten. Darüber hinaus wurden zusätzliche Ressourcen aus den Forschungseinrichtungen genutzt, um neue Aspekte, Technologietransfer und Schnittstellen zu ermöglichen.

10 Nutzen und Verwertbarkeit der Ergebnisse

Die Forschungspartner im Projekt haben im Projekt neue Verifikationsmethoden erforscht, Prototypen implementiert und diese an industrienahen Beispielen evaluiert. Durch den engen Verbund konnte vielfältige Schnittstellen erforscht und erstmalig implementiert werden. Ein Überblick über die herausragenden Ergebnisse und Kooperationen stellen die folgenden Bilder dar.

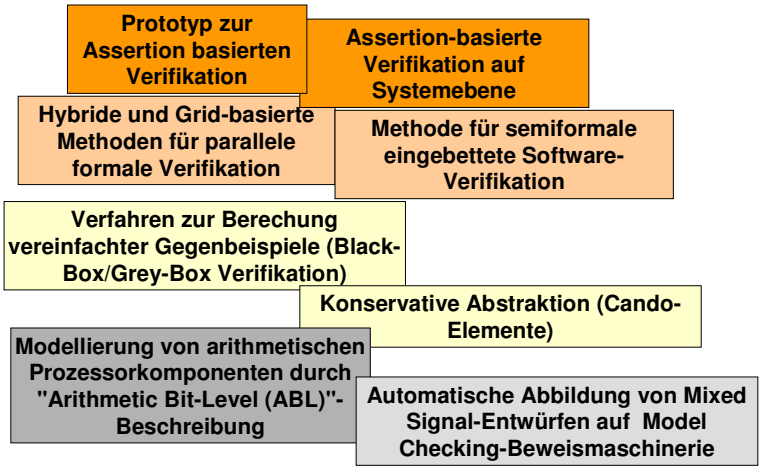

Abbildung 9: Wissenschaftliche Highlights des Projekts

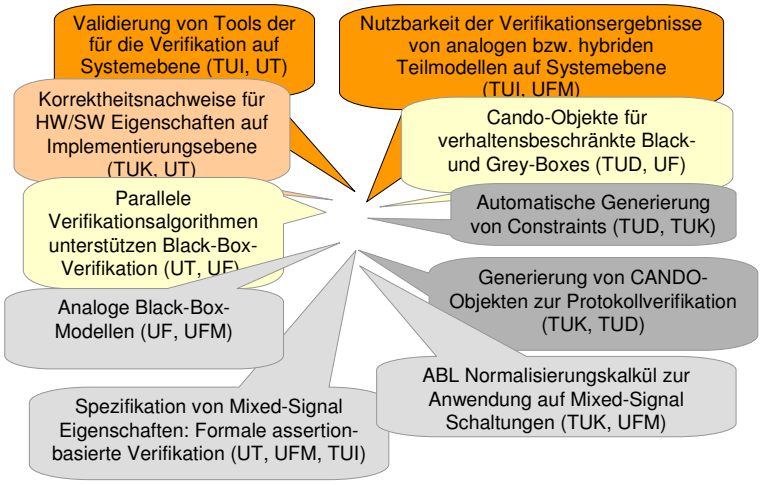

Abbildung 10: Highlights der internen Kooperationen zwischen den Forschungspartnern

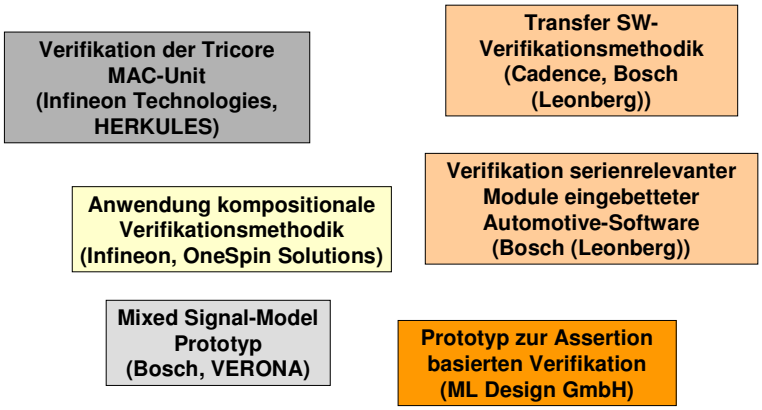

Abbildung 11: Highlights der Industriekooperationen

Erste Methoden von FEST werden schon in F&E Projekten (VERONA, HERKULES) evaluiert oder verfeinert. Darüber hinaus erhält die Lehre und Forschung viele neue Anregungen. Erste Ergebnisse sind hier schon sichtbar, um die Nachhaltigkeit in der Forschung durch Dissertationen und Lehre zu verbessern. Somit verbessern sich Lehrveranstalten an den Hochschulen und erfolgt eine Weiterführung der Ergebnisse in der Forschung. Darüber hinaus wurden Tutorials auf renommierten Konferenzen gehalten. Direkt im Projektzusammenhang und im Rahmen institutsinterner Kooperation wurde eine Reihe von Dissertationen beeinflusst, die mit Namen gelistet sind.

- A. Pacholik, F. Pigorsch, P. Nalla, A. Jesser, M. Schickel, M. Wedler, J. Klöckner, S. Köhler, P. Peranandam, M. Nguyen, S. Steinhorst

Weitere laufende, durch FEST beeinflusste Doktoranden sind erfolgt.

- J. Behrend, S. Disch, M. Herbstritt, S. Lämmermann, D. Lettnin, T. Nopper, M. Oberkönig

Weitere Verwertungsschritte werden in 2008 diskutiert. Detaillierte Darstellungen befinden sich in den Berichten der jeweiligen Forschungspartner.

11 Fortschritt der Wissenschaft und Technik während der Laufzeit des Vorhabens

Eine systematische und methodische Vorgehensweise zur Verifikation von der System-Ebene bis zur elektrischen Ebene fehlt bis heute. Das Projekt FEST will die Lücke schließen und neue Ansätze zur Verifikation von Systemen erforschen und die Integration in einem Gesamtsystem erproben. Es arbeiten dabei 6 Universitäten im Projekt zusammen, um über die eigenen Verifikationskompetenzen hinaus eine Vernetzung der unterschiedlichen Forschungsergebnisse zu erreichen. Hierzu werden neue Verifikationsansätze auf ihre Wirksamkeit erforscht: ausgehend von Beschreibungen der Systemebene über Modelle der Architektur- und Register-Transfer-Ebene bis hin zur elektrischen Schaltungsebene, wobei Komplexitätsgrenzen realer Schaltungsgrößen berücksichtigt werden. Die folgende Abbildung zeigt schematisch auf welche Abstraktionsebenen sich die oben beschriebenen Untersuchungen konzentrieren. Hier wird deutlich, dass auf allen Ebenen eine Modellierung notwendig ist, um Algorithmen und Verfahren zur Verifikation anzuwenden. Diese beiden Schwerpunkte werden in diesem Projekt eine herausragende Rolle spielen, um existierende Ansätze zu vernetzen.

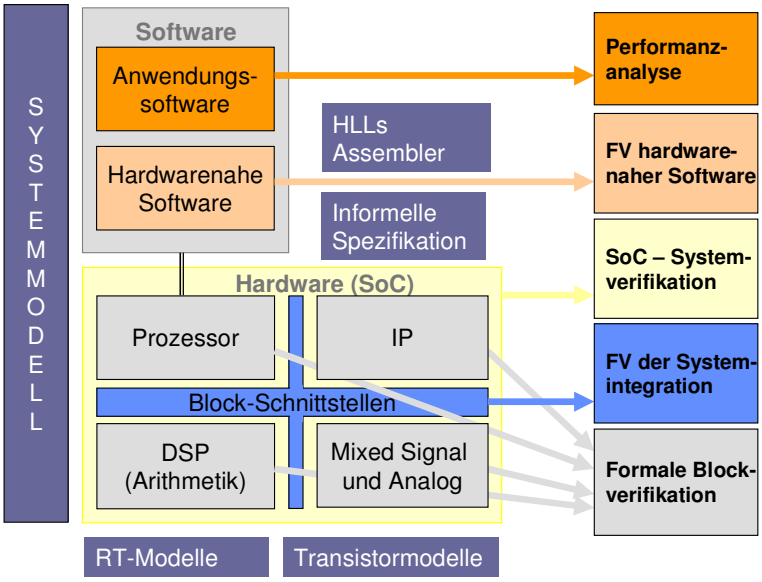

Abbildung 12: Einordnung der Verifikationsschritte und Verifikationsmodelle in die Abstraktionsebenen

Auf Systemebene werden von der TU Ilmenau Methoden zur Modellierung von Zeiteigenschaften – auch Zeitverifikation genannt – erforscht, die das Verhalten des gesamten Systems überprüfen können, bevor eine Implementierung erfolgt. Ein Ziel dieses Ansatzes ist, die Anzahl der Backtracks im Entwurfsprozess in der Implementierung der Halbleiterbausteine zu halbieren. Ein weiteres Ziel sowohl auf Systemebene als auch auf Architekturebene wird von der Uni Tübingen erforscht. Hier wird ein einheitlicher Ansatz für HW-SW-Verifikation von Systemen zu erforscht, der die gemeinsame Behandlung von Soft- und Hardwarekomponenten erlaubt und die bis heute dominierende getrennte Behandlung ablösen wird. Die TU Darmstadt erforscht die Verifikation auf Architekturebene mit einem Verfahren, welches die Systemeigenschaften in einem kompositionalen Verifikationsprozess mit Hilfe individueller Blockeigenschaften prüft. Die Uni Freiburg erforscht Eigenschaftsprüfungen zur Erweiterung der Blockverifikation, so dass eine Technik noch in Szenarien anwendbar ist, wo die einfache Blockspezifikation noch unvollständig ist (Black- und Grey-Boxes). Die gewonnenen Techniken werden genutzt, um Gegenbeispiele zu generieren und Fehler bei der Eigenschaftsprüfung zu lokalisieren. Zur Verbesserung erforscht die Uni Kaiserslautern die Modellgenerierung im so genannten Front-End, um dadurch die Leistungsfähigkeit der Verifikationsmethodik für digitale Blöcke deutlich zu steigern. Bei der Lösung von pathologischen Fällen der Verifikation sequentieller Schaltungen und bei Arithmetikblöcken, wird eine Effizienzsteigerung um eine Größenordnung angestrebt. Auch werden Verifikationen erstmals möglich, bei denen heutige EDA-Werkzeuge und -Methoden noch scheitern. Für gemischt analog-digitale Schaltungen erforscht die Uni Frankfurt eine Methodik zum Mixed-Signal

Model-Checking. Diese wird in der Lage sein, Toleranzen der Parameter des Analogteils der Schaltung zu berücksichtigen und in einer digitalen Verifikationsumgebung einzusetzen, damit SoCs mit digitalen und analogen Blöcken verifizierbar sind.

Im Folgenden werden die Ergebnisse der Forschungspartner und deren Einbindung ins Gesamtprojekt dargestellt.

11.1 Zeitverifikation auf Systemebene

Partner im Projekt: Technische Universität Ilmenau, Fachgebiet Rechnerarchitektur

Um die gesteigerte Komplexität elektronischer Systeme bewältigen zu können und Redesign Zyklen zu minimieren, werden Verfahren zur Evaluierung auf Systemebene erforscht. Diese Verfahren beinhalten die effektive funktionale Simulation auf abstraktem Niveau sowie die Modellierung und Simulation von Performance und Zuverlässigkeit. Beim funktionalen Entwurf (Functional Level) existieren verschiedene Modellierungsdomänen, genannt seien hier Discrete Event, Finite State Machine und Synchronous Dataflow, die innerhalb eines Systemmodells vorkommen und verschiedene Systemaspekte adressieren. Im Bereich der Validierung auf Missionsebene und Electronic System Level (ESL) durch Simulation existieren zahlreiche Forschungen seitens der TU Ilmenau. Zu erwähnen sei hierbei vor allem das Werkzeug MLDesigner. Als weiteres Forschungsfeld ist die Petri-Netz-basierte Modellierungsanalyse von eingebetteten Systemen zu erwähnen, die eine Prüfung von Zeiteigenschaften erlaubt.

Bei abstrakten funktionalen Multidomänenmodellen besteht die Problematik der Integration von Zeiteigenschaften, da einige Domänen nicht zeitbehaftet sind oder spezielle Konstrukte zu deren Integration benutzt werden. Im Projekt FEST werden die einheitliche Notation von Zeiteigenschaften in Multidomänenmodellen sowie Methoden der Extraktion und Prüfung des Zeiteigenschaftsmodells untersucht. Zusätzlich werden Aspekte der Dekomposition von Modell und Zeiteigenschaften betrachtet. Für die verschiedenen Modellierungsdomänen wurden Anforderungen an die Constraint-Beschreibung definiert und in Prototypen umgesetzt. Die Forschung ist hier allerdings noch nicht abgeschlossen. Zur einheitlichen Beschreibung wurden Transformationsmöglichkeiten untersucht und für eine softwaretechnische Umsetzung aufbereitet. Zur Verfeinerungen von Constraints wurden Regeln definiert und Prüfmöglichkeiten betrachtet.

Kooperation bestehen im Projekt mit der Uni Tübingen, deren Forschungsschwerpunkt in der Erforschung von Verfahren und Tools zum Model Checking besteht. Ziel der Kooperation ist der Austausch von Modellen und Methoden (Tools). Eine weitere Kooperation zum Austausch von Modellen insbesondere unter Aspekten der Zeitbeschreibung und -verifikation besteht mit der Uni Frankfurt.

Nach Abschluss des Projekts wird die entwickelte Methodik geeignet sein, ein formales Zeitmodell aus einem Constraint annotierten funktionalen Multidomänenmodell zu extrahieren, wobei für das funktionale Modell bestimmte Beschränkungen in Bezug auf Domänen und Elementen einzuhalten sind. In dem formalen Modell sind vorgegebene Zeitbeschränkungen auf Systemebene prüfbar. Weiterhin wird eine Konsistenzprüfung der Constraints zwischen bestimmten Hierarchieebenen ermöglicht.

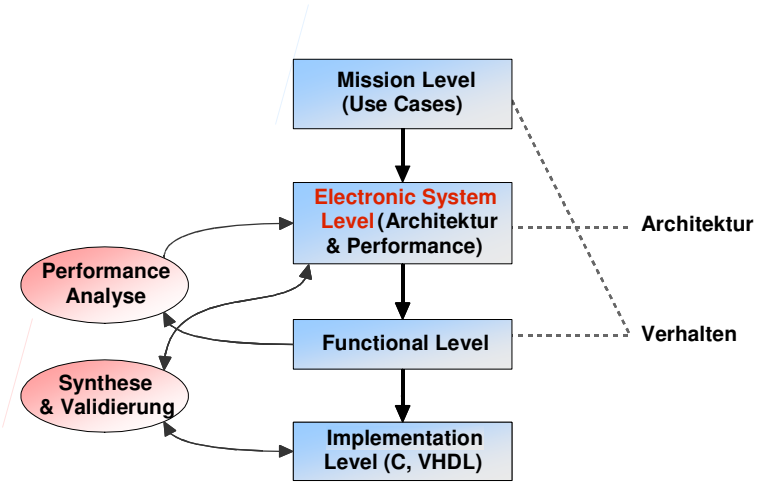

Abbildung 13: Mission Level Designmethodik

11.2 Methoden und Tools zur Hardware/Software Co-Verifikation

Partner im Projekt: Universität Tübingen, Wilhelm-Schickard-Institut für Informatik, Lehrstuhl Technische Informatik

Die Verifikation hardwarenaher eingebetteter Softwarekomponenten soll durch Anpassung und Weiterentwicklung existierender Verifikationstechniken aus dem Bereich der Hardwareverifikation ermöglicht werden. Zudem werden verschiedene formale und semiformale Techniken kombiniert und Teile der Algorithmen parallelisiert, um Systeme mit größeren Zustandsräumen analysieren zu können. Ein weiterer Schwerpunkt liegt auf der automatischen Extraktion von Verifikationseigenschaften aus Modellen auf hohen Abstraktionsebenen. Diese aus UML/SysML gewonnenen Systemeigenschaften werden dann in der HW-SW-Verifikation auf niedrigeren Abstraktionsniveaus wieder verwendet. Außerdem finden sie ihre Anwendung bei der Bestimmung von Überdeckungsmaßen bei semiformalen Techniken.

Die zentrale Idee bei der Parallelisierung der Zustandsraum-Traversierung besteht in der Verteilung der Berechnung von Folgezuständen (Image Computation) auf mehrere Knoten eines Clusterrechners. Ein Einsatz in Grid-Umgebungen soll mit der Firma Bosch evaluiert werden. Die Knoten kommunizieren untereinander mittels des Message Passing Interface (MPI). Die Überlappungen der verteilten Zustandsmengen müssen minimiert werden, um die Verfahren effizient einsetzen zu können. Folgearbeiten konzentrierten sich auf diesen Punkt, um diese Überlappung statisch und dynamisch zu reduzieren. Eine neue Guiding Technik wurde implementiert, welche automatisch die Menge der „interessanten“ Variablen im Design mit Hilfe der spezifizierten Eigenschaften findet. Diese Variablen dienen zur Steuerung der Zustandsraumexplosion. Das Verfahren beschleunigt den gesamten Verifikationsprozess.

Als Basistechnologie für die Extraktion von Eigenschaften wird der von der Uni Tübingen entwickelte SystemC Checker überarbeitet, der es erlaubt, temporallogische Formeln in PSL (Property Specification Language) gegen simulierte SystemC-Modelle zu prüfen. Für die Eigenschaftsextraktion wurde der mögliche Einsatz des FZI SystemC-Parser untersucht, welcher ein SystemC-Modell in eine XML-Repräsentation umwandelt. Diese Darstellung wurde für eine Analyse des Systems verwendet, um Eigenschaften zu generieren.

Die Methode der Eigenschaftsextraktion wurde dahin gehend überarbeitet, dass nicht mehr ein SystemC-Modell als Grundlage verwendet wird, sondern Modelle der Unified Modeling Language

(UML) bzw. Systems Modeling Language (SysML). Durch den Einsatz dieser Modelle werden die Eigenschaften aus einer hohen Abstraktionsebene extrahiert, die sich sehr nah an der Spezifikation befindet. Im Rahmen dieser Arbeiten fand eine Kooperation mit der technischen Universität Ilmenau statt. Es besteht die Möglichkeit, die Eigenschaftsextraktion und die Methoden der Zeitverifikation in einem gemeinsamen Verifikationsframework zu verbinden. Diese Methode wird zurzeit an den beiden Universitäten untersucht. Es wurden weiterhin C-Software-Verifikationswerkzeuge untersucht, um einen Überblick über den Stand der Technik zu erstellen, aktuelle Werkzeuge zu vergleichen und die Grenzen der aktuellen Ansätze herauszuarbeiten. Die Arbeit wurde im Rahmen einer laufenden Kooperation mit der Firma Bosch durchgeführt. Die Ergebnisse dieser Aktivität werden in die Entwicklung unserer eigenen Verifikationswerkzeuge zur hardwarenahen Softwareverifikation fließen.

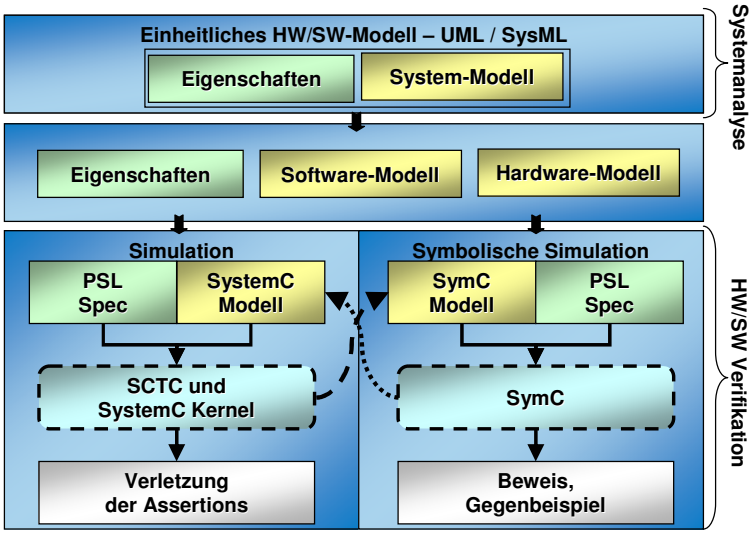

Abbildung 14: Verifikationsablauf und Werkzeuge für die Hardware/Software Co-Verifikation

11.3 Kompositionale Verifikation auf Systemebene

Partner im Projekt: Fachgebiet Rechnersysteme, Technische Universität Darmstadt

Der gegenwärtige Stand der Technik erlaubt die formale Verifikation von Blöcken, aber nicht von kompletten Systemen. Sind die Blöcke aber formal verifiziert, dann sind die zur Verifikation benutzten Eigenschaften auch eine abstrakte Repräsentation der Funktionalität der Blöcke. Beispielsweise kann in Eigenschaften auf Signalwerte zu mehreren Zeitpunkten referenziert werden und nicht nur, wie z.B. bei Zustandsdiagrammen, zum gegenwärtigen und nächsten Zeitpunkt. Die Abstraktheit der Blockeigenschaften kann daher ausgenutzt werden, um Blöcke durch abstrakte Modelle zu ersetzen, die aus den Blockeigenschaften generiert werden. Die aus den Eigenschaften erzeugten abstrakten Modelle werden „Cando-Objekte“ genannt, weil sie jedes bis auf das durch die Eigenschaften explizit verbotene Verhalten nachbilden. Für Cando-Objekte gelten eine Reihe von Kompositionalitäts-Eigenschaften. Systemeigenschaften können daher nicht mehr nur auf dem ursprünglichen Modell, sondern auch auf einem Modell verifiziert werden, bei dem die Blöcke durch die Cando-Objekte ersetzt sind.

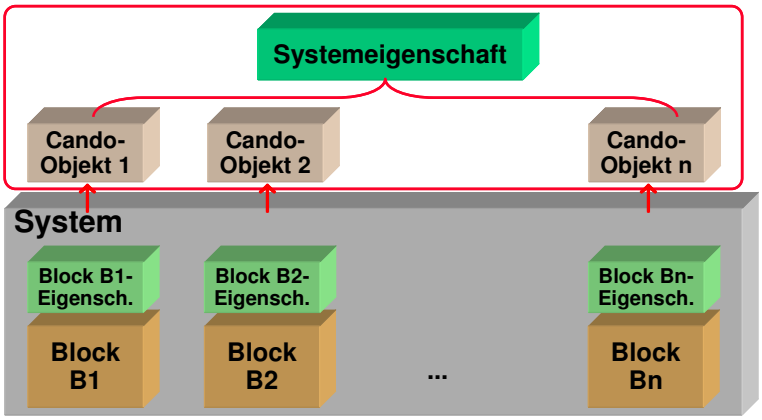

Abbildung 15: Kompositionale Verifikation mit Cando-Objekten

An der TU Darmstadt werden Verfahren zur effizienten Generierung von Cando-Objekten aus Blockeigenschaften entwickelt. Die Eigenschaften können z.B. in PSL spezifiziert werden. Cando-Objekte werden als VHDL-Beschreibungen erzeugt und können für die formale Verifikation, aber auch für die Simulation weiterbenutzt werden. Mit diesen Verfahren ist es an der TU Darmstadt zum ersten Mal gelungen, aus Eigenschaftssätzen signifikanter Komplexität (Bus-Protokolle wie z.B. AMBA-AHB oder PCI) ausführbare abstrakte Modelle zu generieren. Darüber hinaus können die Verfahren zur Lösung einer Reihe weiterer Probleme wie z.B. Konsistenz und Vollständigkeit von Eigenschaftssätzen benutzt werden.

11.4 Black-Box-Techniken bei der Eigenschaftsprüfung

Partner im Projekt: Universität Freiburg, Institut für Informatik

Black-Box-Techniken werden eingesetzt, um Fehlererkennung und -lokalisierung schon in einem frühen Stadium des Entwurfs zu ermöglichen. Die Anwendung automatisierter, formaler Verifikationsmethoden auf SoC-Entwürfe und ihre Integration mit Black-Box-Techniken zieht eine wesentlich exaktere Fehlererkennung und Fehlerlokalisierung nach sich, als dies bei simulationsbasierten Ansätzen der Fall wäre. In unserem Ansatz gehen wir von einer Spezifikation durch eine Menge temporaler Eigenschaften aus, die durch eine gegebene sequentielle Implementierung erfüllt werden sollen. Erfüllt die Implementierung die spezifizierten Eigenschaften nicht, dann soll der Fehler dem Designer durch die Berechnung „guter Gegenbeispiele“ erklärt werden. Diese Gegenbeispiele stellen Abläufe des Systems dar, die zum einen den Fehlereffekt sichtbar machen, zum anderen für die praktische Anwendung so kurz wie möglich sein sollten und so wenige Systemkomponenten wie möglich benutzen sollten. Neben der optimierten Berechnung von Gegenbeispielen stellen wir Methoden zur automatischen Lokalisierung von Designfehlern zur Verfügung. Beide Ziele werden unter Anwendung so genannter Black-Box-Techniken erreicht.

Sowohl bei der Berechnung guter Gegenbeispiele als auch bei der Fehlerlokalisierung sind folgende grundlegenden Fragestellungen von Interesse. Auf Basis einer unvollständigen Schaltung, d.h. einer Schaltung, die sogenannte Black-Boxes enthält, ist einerseits die Frage zu beantworten, ob es möglich ist, die Black Boxes durch Implementierungen zu ersetzen, so dass die spezifizierte Eigenschaft erfüllt ist („Realisierbarkeit“). Andererseits wird die Frage gestellt, ob die Eigenschaft für jede mögliche Ersetzung der Black-Box erfüllt ist („Validität“). Hierzu wurde an der Uni Freiburg ein Modellprüfer entwickelt, mit dem es unter Einsatz von AIGs (And-Inverter-Graphen) als Mittel zur Repräsentation großer Zustandsräume gelingt, die angesprochenen Aufgaben zu lösen.

Zur Berechnung minimaler Gegenbeispiele, die auf möglichst wenigen Komponenten basieren, werden möglichst große Teile des Designs ausgeblendet, aus denen „Black-Boxes“ gebildet werden.

Wenn die folgende Eigenschaftsüberprüfung für das „Black-Box-Design“ fehlschlägt, d.h. wenn wir für das Black-Box-Design die Nicht-Realisierbarkeit zeigen können, wird dieses reduzierte Design zur Berechnung eines kompakten Gegenbeispiels verwendet. Dieses Gegenbeispiel ist dann in der Lage, den Fehlereffekt unabhängig von den ausgeblendeten Teilen zu erklären. Im Gegensatz dazu wird für die Fehlerlokalisierung nach kleinen Teilbereichen des Designs gesucht, so dass bei Ausblenden dieser Teile die Realisierbarkeit der gewünschten Systemeigenschaft gezeigt werden kann. Dies bedeutet, dass der vorliegende Fehler durch Abändern der ausgeblendeten Teile des Systems korrigierbar ist, so dass der mögliche Fehlerort eingegrenzt werden kann.

In Zusammenarbeit mit der Uni Darmstadt werden Black-Box-Techniken zu Grey-Box-Verifikationsansätzen verallgemeinert. Dabei wird das Innenleben der „Grey-Boxes“ durch einige wenige kritische Eigenschaften beschrieben. Die Anwendbarkeit der Konzepte auf analoge und Mixed-Signal-Schaltungen wird zusammen mit der Universität Frankfurt untersucht.

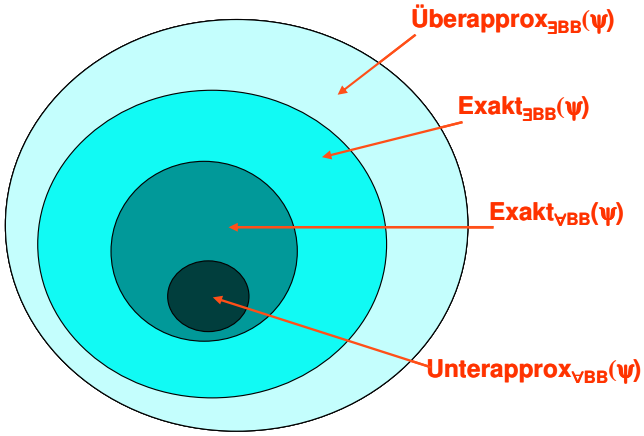

Abbildung 16: Darstellung von unter- und überapproximierten Zustandsmengen bei der Eigenschaftsüberprüfung für Black-Box-Designs

11.5 Frontend-Modellgenerierung

Partner im Projekt: TU Kaiserslautern, AG Entwurf Informationstechnischer Systeme

Durch gezielte Maßnahmen im Frontend eines Property Checkers kann die Performanz bei der Lösung komplexer Verifikationsaufgaben drastisch gesteigert werden. Dies wird anhand pathologischer Fälle der formalen Blockverifikation demonstriert. Ein besonders interessantes Anschauungsbeispiel ergab sich durch die Möglichkeit, in Kooperation mit der Firma OneSpin Solutions GmbH an der formalen Verifikation des bei Infineon in der Entwicklung befindlichen Tricore 2 Prozessors mitzuwirken. Die TU Kaiserslautern beschäftigte sich dabei mit der MAC Unit, die zahlreiche DSP-Instruktionen mit Multiply-Accumulate-Operationen implementiert. Der formale Nachweis der Korrektheit des arithmetischen Ergebnisses auf voller Bitbreite war mit herkömmlichen Techniken bis jetzt nicht möglich. Durch eine gezielte Modellierung der Prozessorarithmetik im Frontend des Property Checkers und eine entsprechende Anpassung des Flows konnten hier entscheidende Fortschritte erzielt werden. An der TU Kaiserslautern wurde das Modellierungskonzept des „arithmetic bit-level (ABL)“ und ein dazu passendes Normalisierungsverfahren erforscht [16]. Mit dessen Hilfe war es erstmals möglich die arithmetische Korrektheit aller MAC-Instruktionen des Tricore 2 auf voller Bitbreite nachzuweisen. Das internationale Interesse and dieser Lösung ist sehr groß, wie zahlreiche Anfragen und eine Vortragseinladung an der University of California at Berkeley belegen. Die Fortschritte bei der Arithmetikverifikation können auch in Hinblick auf die Eigenschaftsprüfung von Mixed-Signal-Schaltungen sehr nützlich sein. Dazu werden gerade in Kooperation mit der Uni Frankfurt Untersuchungen angestellt.

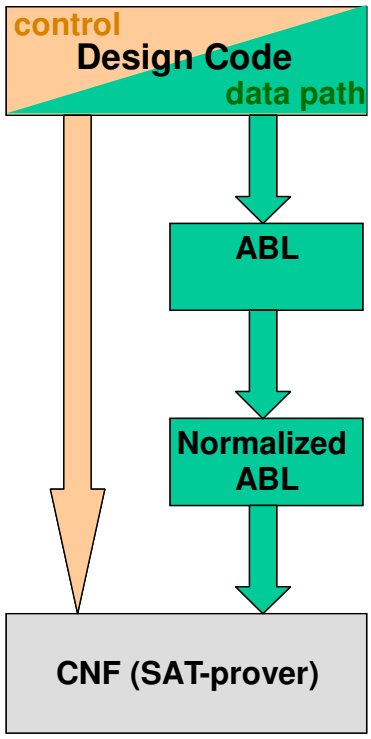

Abbildung 17: Verifikationsflow für Kontrolllogik und Arithmetik

Als zweites Thema werden Maßnahmen der Frontendmodellierung im Zusammenhang mit der Verifikation sequenzieller Systeme untersucht. Es konnte gezeigt werden, dass durch eine bestimmte Zustandskodierung die Generierung von Invarianten bei der temporalen Induktion effektiv unterstützt werden kann. Darüber hinaus wurde ein Verfahren zur Verifikation von Hardwareprotokollimplementierungen entwickelt, das auf einer geeigneten Dekomposition des Zustandsraumes beruht. Erste Untersuchungen an industriellen Entwürfen (Infineon) belegen, dass damit der manuelle Verifikationsaufwand drastisch reduziert werden kann. Auch die Frontend-Maßnahmen zur Verifikation sequenzieller Systeme sind in Fachkreisen auf großes Interesse gestoßen, wie ein eingeladener Vortrag zu diesem Thema auf der ASICON-05 belegt. Die an der TU Kaiserslautern entwickelten Methoden werden z.Zt. mit dem an der TU Darmstadt entwickelten Ansatz zur kompositionalen Verifikation kombiniert. Erste erfolg versprechende Ergebnisse liegen bereits vor. Ein besonderes Potential der erzielten Forschungsergebnisse in Hinblick auf zukünftige Arbeiten liegt insbesondere im Bereich der Verifikation hardwarenaher Software. Untersuchungen dazu werden bereits gemeinsam mit der Uni Tübingen durchgeführt.

11.6 Mixed-Signal Model-Checking

Partner im Projekt: Johann Wolfgang Goethe-Universität Frankfurt am Main, Institut für Informatik, Professur für Entwurfsmethodik

Ein weiteres Ziel des Projekts ist die in letzter Zeit an Bedeutung gewonnene Verifikation von gemischt analogen und digitalen Schaltungen. Eine Herausforderung besteht immer noch in der Modellierung von integrierten Schaltungsklassen, die einen unterschiedlichen Werte- und Zeitcharakter besitzen. Es existieren bereits Modellierungsmöglichkeiten (Timed Automata, Hybride Automaten etc.), die den kontinuierlichen Werte- und Zeitcharakter analoger Schaltungen wiedergeben können, jedoch bisher nicht in der Lage sind, vollständige Eigenschaftsprüfungen durchzuführen. Zudem unterliegen diese Modelle zumeist Restriktionen, welche die zu behandelnden Schaltungsklassen stark einschränken. Zwingend notwendig ist hier die Einführung von Zeitbedingungen, die die temporalen Abläufe der

Schaltungen wiedergeben und gleichzeitig die Signalabhängigkeiten innerhalb beider Schaltungsklassen berücksichtigt.

Ein neuer Ansatz besteht darin, das analoge Teilsystem in der Form zu diskretisieren, so dass eine Zusammenführung mit dem Modell des digitalen Teilsystems möglich ist. Ein besonderes Merkmal des Modells ist, dass die Zeit in beiden Teilsystemen unterschiedlich zu behandeln ist und modelliert werden muss. Ausgehend von einem Algebro-Differentialgleichungssystem wird der kontinuierlichen Zustandsraum der analogen Teilschaltung aufbaut und in geeigneter Weise diskretisiert. Hierdurch entsteht ein zeitbehaftetes Transitionssystem mit vielen unterschiedlichen diskreten Zeiten. Dieses wird zur symbolischen Weiterverarbeitung in ein Multi Terminal Binary Decision Diagram (MTBDD) überführt. Parallel werden MTBDDs erzeugt, welche die digitalen Schaltungszustände und deren Transitionen wiedergeben. Die so erzeugten MTBDDs werden anschließend gemeinsam mit einer zu verifizierenden Spezifikation einem Model-Checking Algorithmus zugeführt. Die verwendetet Spezifikationssprache ist CTL-AT, mit der es möglich ist neben dem Standard CTL-Sprachumfang Zeitintervalle und analoge Zustandsgebiete anzugeben.

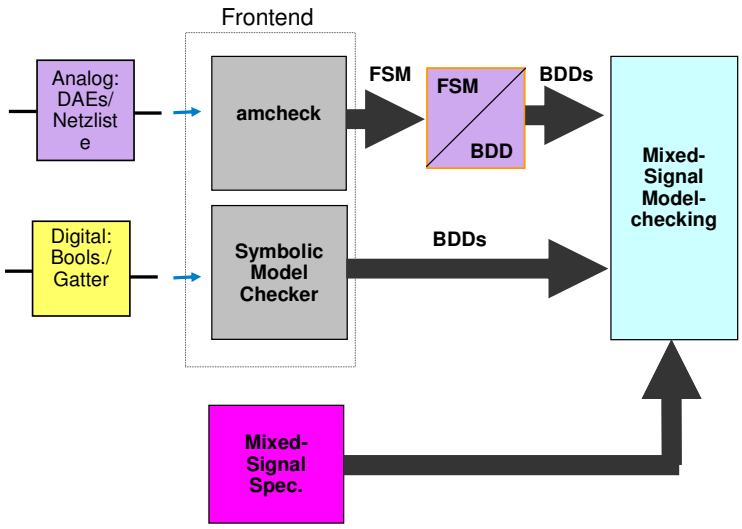

Abbildung 18: Mixed-Signal Model-Checking

11.7 Resümee

Nach drei Jahren Projektlaufzeit wurden wichtige Schritte zur Erprobung der neuen Verfahren erreicht. Die Kooperationen zwischen den Forschungspartnern werden in dem Projekt genutzt, um Methodiken und Modellierungsverfahren auszutauschen, um neue Verifikationsansätze vorzubereiten, die Gegenstand zukünftiger Forschung werden können. Eine Überführung der erforschten Methoden in die industrielle Praxis ist der nächste Schritt, um die Modelle und Methoden weiter für eine industrielle Anwendung zu verbessern. Erste Ansätze zum Einsatz im industriellen Umfeld sind erfolgt. Im letzten Jahr standen der intensive Austausch mit den Industriepartnern im Vordergrund der Projektarbeit, sowie die Verfeinerung der Demonstratoren, die im Rahmen der Forschungsaktivitäten erstellt wurden. Um die Ergebnisse für die Industrie in EDA-Werkzeugen und Flows nutzbar zu machen, sind weitere Forschungs- und Entwicklungsanstrengungen zusammen mit der Anwender- und EDA-Industrie notwendig.

12 Veröffentlichungen

Die Veröffentlichungen werden von den Projektpartnern individuell in ihren Berichten beschrieben. Hier folgt eine komplette Liste des Projekts.

12.1 Veröffentlichungen des Projekts

1 M. Wedler, D. Stoffel, W. Kunz: Exploiting State Encoding for Invariant Generation in Induction-Based Property Checking; Proc. of the Asia and South Pacific Design Automation Conference, (ASPDAC), 2004

2 Jürgen Ruf, Roland J. Weiss, Thomas Kropf, Wolfgang Rosenstiel: Modeling and Formal Verification of Production Automation Systems; In "Integration of Software Specification Techniques for Applications in Engineering", Lecture Notes in Computer Science, Vol. 3147, Springer, 2004

3 T. Nopper and C. Scholl: Approximate symbolic model checking for incomplete designs; Formal Methods in Computer-Aided Design, pages 290-305, 2004

4 Prakash M. Peranandam, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Dynamic Guiding of Bounded Property Checking; IEEE International High Level Design Validation and Test Workshop (HLDVT 04), Sonoma Valley, California, USA, 2004

5 Pradeep K. Nalla, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Parallel Bounded Property Checking with SymC 8. GI/ITG/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen", München, Deutschland, April 2005

6 Pradeep K. Nalla, Prakash M. Peranandam, J. Ruf, R.J. Weiss, T. Kropf, W. Rosenstiel: Bounded Property Checking with SymC Design Automation and Test in Europe, University Booth (DATE 05), March 7-11, 2005

7 T. Nopper and C. Scholl: Flexible Modelling of Unknowns in Model Checking for Incomplete Designs; 8. GI/ITG/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen", München, Deutschland, April 2005

8 M. Wedler, D. Stoffel, W. Kunz: Normalization at the Arithmetic Bit-Level; Proc. IEEE/ACM Design Automation Conference (DAC), Anaheim CA, USA, 13-17. Juni 2005 2005-06

9 Pradeep K. Nalla, Roland J. Weiss, Prakash M. Peranandam, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Distributed Symbolic Bounded Property Checking; 4th International Workshop on Parallel and Distributed Methods in Verification (PDMC 2005), Lisabon, Portugal, 10. Juli 2005

10 Alexander Pacholik, Wolfgang Fengler, Horst Salzwedel, Oleg Vinogradov: Real Time Constraints in System Level Specifications Improving the Verification Flow of Complex Systems; Workshop on Object Oriented Software Design for Real Time and Embedded Computer Systems, Erfurt, Germany, Erfurt 19.-22.9.2005

11 Djones Lettnin, Roland J. Weiss, Axel Braun, Jürgen Ruf, Wolfgang Rosenstiel: Temporal Properties Verification of System Level Design; Workshop on Object Oriented Software Design for Real Time and Embedded Computer Systems, Erfurt, Germany, Erfurt, 19.-22.9.2005

12 Roland J. Weiss, Jürgen Ruf, Thomas Kropf, and Wolfgang Rosenstiel: Efficient and Customizable Integration of Temporal Properties into SystemC; Forum on specification and Design Languages (FDL'05), Lausanne, Switzerland, 27-30. September 2005 (best paper award)

13 M. Wedler, D. Stoffel, W. Kunz: Frontend model generation for SAT-based property checking; Proc. 6th Int. Conference on ASICs, Shanghai, China, 24-27. Oktober 2005

14 M. Nguyen, D. Stoffel, M. Wedler, W. Kunz: Transition-by-Transition FSM Traversal for Reachability Analysis in Bounded Model Checking; Proc. IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD), San Jose, California, USA, Nov. 2005

15 Prakash M. Peranandam, Pradeep K. Nalla, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Overlap Reduction in Symbolic System Traversal; IEEE International High Level Design Validation and Test Workshop (HLDVT 05), Napa Valley, California, USA, 30.11 - 2.12. 2005

16 A. Jesser, L. Hedrich, M. Wedler, W. Kunz: A case study on applying bounded model checking to analog circuit verification; 9. ITG/GI/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen" (MBMV 06), Dresden, Germany, 20 - 22.Februar 2006

17 F. Pigorsch, C. Scholl, and S. Disch: Advanced unbounded model checking by using AIGs, BDD sweeping and quantifier scheduling; 9. ITG/GI/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen" (MBMV 06), Dresden, Germany, 20 - 22. Februar 2006

18 Stefan Lämmermann, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Automatische Eigenschaftsextraktion auf Systemebene aus SystemC Modellen; 9. ITG/GI/GMM Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen" (MBMV 06), Dresden, Germany, 20 - 22.Februar 2006

19 O. Vinogradov, W. Fengler, A. Pacholik: Development of language of time-constraints for the design of reactive systems; Moskovskij Inženerno-Fizičeskij Institut: Intellektual, nye sis-temy i tech-nologii. - Moskva: MIFI, S. 90-91, 2006

20 Prakash M. Peranandam, Pradeep K. Nalla, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Fast Falsification Based on Symbolic Bounded Property Checking; 4th Design Automation Conference (DAC 2006), Moscone Center, California, USA, 24 - 28.Juli 2006

21 Stefan Lämmermann, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Automatic Generation of Verification Properties for SoC Design from SysML-Diagrams; 3rd International UML for SoC Design Workshop at DAC'06, San Francisco California, USA, 23. Juli 2006

22 H. Eveking, M.Schickel, M. Braun, V. Nimbler: On Consistency and Completeness of Property-Sets: Exploiting the Property-Based Design-Process; FDL, Darmstadt, 2006

23 V. Schöber, W. Fengler, H. Salzwedel, A. Pacholik, T. Kropf, J. Ruf, S. Lämmermann, M. Schickel, V. Nimbler, M. Braun, H. Eveking, B. Becker, C. Scholl, M. Nguyen, M. Wedler, D. Stoffel, W. Kunz, A. Jesser, L. Hedrich: FEST: Funktionale Verifikation von Systemen; Newsletter edacentrum 03, 2006

24 Pradeep K. Nalla, Prakash M. Peranandam, J. Ruf, S. Laemmermann, J. Behrend, R.J. Weiss, T. Kropf, W. Rosenstiel: Fast Distributed Property Checking; Design Automation and Test in Europe, University Booth (DATE 06), March 6-10, 2006

25 F. Pigorsch, C. Scholl, and S. Disch: Advanced Unbounded Model Checking Based on AIGs, BDD Sweeping, And Quantifier Scheduling; FMCAD'2006

26 T. Nopper, C. Scholl, B. Becker: Computation of Minimal Counterexamples by Using Black Box Techniques and Symbolic Methods; International Conference on Computer-Aided Design (ICCAD2007), San Jose, USA, 2007

27 M. Wedler, D. Stoffel, R. Brinkmann, W. Kunz: A Normalization Method for Arithmetic Data Path Verification; IEEE Transactions on Computer-Aided Design of Circuits and Systems, November 2007

28 M. Thalmaier, M. D. Nguyen, M. Wedler, D. Stoffel, W. Kunz: Formale Verifikation von SoC Protokollimplementierungen; 1.GMM/GI/ITG-Fachtagung Zuverlässigkeit und Entwurf, Munich, Germany, March 26-28 2007

29 Alexander Jesser, Stefan Lämmermann, Alexander Pacholik, Roland Weiss, Jürgen Ruf, Wolfgang Fengler, Lars Hedrich, Thomas Kropf, Wolfgang Rosenstiel: Analog Simulation Meets Digital Verification - A Formal Assertion Approach for Mixed-Signal Verification; 14th Workshop on Synthesis And System Integration of Mixed Information Technologies (SASIMI'07), Sapporo, Japan, pp. 507 - 514, Oktober 2007

30 Pradeep K. Nalla, Jörg Behrend, Prakash Peranandam, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Grid Based Fast Falsification for Bounded Property Checking; Forum on Specification and Design Languages (FDL 07), Barcelona, Spain, September 18-23, 2007

31 Djones Lettnin, Markus Winterholer, Axel Braun, Joachim Gerlach, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Coverage Driven Verification applied to Embedded Software; IEEE Computer Society Annual Symposium on VLSI (ISVLSI 07), Porto Alegre, Brazil, May 09-11, 2007

32 Stefan Lämmermann, Jörg Behrend, Roland J. Weiss, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: UML/SysML-Systemanalyse zur Generierung von formalen Verifikationseigenschaften für verschiedene Abstraktionsebenen; 10. GI/ITG/GMM Workshop, Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV 07), Erlangen, Germany, March 05-07, 2007

33 Djones Lettnin, Pradeep K. Nalla, Roland J. Weiss, Axel Braun, Jürgen Ruf, Thomas Kropf, Wolfgang Rosenstiel: Semiformal Verification of Temporal Properties in Embedded Software; 10. GI/ITG/GMM Workshop, Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV 07), Erlangen, Germany, March 05-07, 2007

34 J. Behrend, A. Braun, O. Bringmann, M. Krause, T. Kropf, S. Lämmermann, P. Nalla, W. Rosenstiel, J. Ruf, T. Schönwald, A. Viehl, J. Zimmermann: Entwurf und Verifikation von Hardware/Software - Systemen 5. Kooperationsmarkt des Ekompass-Workshops, Juni 19-20, 2007, Hannover, Germany.

35 M. Braun, M. D. Nguyen, H. Eveking, M. Schickel, W. Kunz: Methoden zur Verifikation von Kommunikationsstrukturen; 10. GI/ITG/GMM Workshop, Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV 07), Erlangen, Germany, March 05-07, 2007

36 M. Schickel, M. Overkönig, M. Schweikert, H.Eveking: A Case-Study in Property-Based Synthesis: Generating a Cache-Controller from a Property-Set; Forum on Specification and Design Languages (FDL 07), Barcelona, Spain, September 18-23, 2007

37 M. Oberkönig, M. Schickel, H. Eveking: A Quantitative Completeness Analysis for Property-Sets; FMCAD'07

38 H. Eveking, M. Schickel, M. Braun, M. Schweikert, V. Nimbler: Eigenschaftsbasierte Entwurfsmethodik für die Systemebene; edaForum07, München, 2007

39 H. Eveking, M. Braun, M. Schickel, M. Schweikert, V. Nimbler: Multi-Level Assertion-Based; Design Proc. of Formal Methods and Models for Codesign (MEMOCODE'2007), IEEE Computer Society, 2007

40 M. Schickel, V. Nimbler, M. Braun, Hans Eveking: CandoGen – A Property-Based Model Generator; University Booth at DATE 2007, Nice, France, 2007

41 H. Eveking, M. Braun, V. Nimbler, M. Schickel: Zuverlässigkeitserhöhung mit funktionalen Monitoren; 1. GMM/GI/ITG-Fachtagung "Zuverlässigkeit und Entwurf", 2007

42 M. Schickel, V. Nimbler, M. Braun, H. Eveking: An Efficient Synthesis Method for Property-Based Design in Formal Verification; In: Sorin Huss (Ed.): Advances in Design and Specification Languages for Embedded Systems, p. 163-182, Kluwer Acad. Publishers, Boston/Dordrecht/London, 2007

43 Marcus Müller, Alexander Pacholik, Wolfgang Fengler: Tool Support for Formal System Verification; In: Peter Scharff (Ed.): Computer science meets automation: 52. IWK, Internationales Wissenschaftliches Kolloquium; proceedings; 10 - 13 September 2007. ISBN 978-3-939473-17-6, Ilmenau: Univ.-Verl., Vol. II, pp. 137-142, 2007

44 T. Baumann, A. Pacholik, H. Salzwedel: Performance Exploration with MLDesigner unsing Standardized Communication Interfaces; University Booth at DATE '07, Acropolis, Nice, France, 16.-20. April 2007

45 Alexander Pacholik, Wolfgang Fengler: A System Model for Formal Verification of TLM based; Transaction Properties Communications and Networking Symposium, Spring Sim'07, Norfolk, 23.-27.03. 2007

46 Alexander Jesser, Lars Hedrich:A Symbolic Approach for Mixed-Signal Model Checking; 13th Asia and South Pacific Design Automation Conference (ASP-DAC'08), COEX, Seoul, Korea, pp. , January 2008

12.2 Publikationen zum Stand der Technik

[BiCC99] A. Biere, A. Cimatti, E. Clarke, Y. Zhu: Symbolic model checking without BDDs, TACAS 1999.

[BlELR01] C. Blank, H. Eveking, J. Levihn, G. Ritter: Symbolic Simulation Techniques - State-of-the-Art and Applications, IEEE Proc. HLDVT'01, Monterey 2001.

[BMBF02] BMBF: IT-Forschung 2006, Förderprogramm Informations- und Kommunikationstechnik, http://www.it2006.de/it-forschung_2006.pdf, 2002.

[Boer01] Boer, Gabrielli, Meo, Timed Concurrent Constraint Languages: A Comparison, http://www.cwi.nl/projects/alp/newsletter/nov01/nav/palamidessi/.

[BUCMDH92] J.R. Burch, E.M. Clarke, K.L. McMillan, D.L. Dill, L.J. Hwang: Symbolic model checking: 10^20 states and beyond, Information and Computation, 98(2):142-170, 1992.

[EU01] EU: „WEISSBUCH: Die europäische Verkehrspolitik bis 2010: Weichenstellungen für die Zukunft", http://europa.eu.int/comm/energy_transport/library/lb_texte_complet_de.pdf, 2001.

[Ev00] H. Eveking: Machine assisted verification, E. Börger (Hrsg.): Architecture design and validation methods, Springer, 2000.

[FeDDL03] Wolfgang Fengler, Bernd Däne, Vesselka Duridanova, Thomas Licht: Design Methodology for an Embedded System for High-Performance Computing. 27th IFAC/IFIP/IEEE Workshop on Real-Time Programming, ISBN 0-08-044203-X, pp. 99-104, Lagow, Po-land, May 14-17, 2003.

[FeHFS02] O. Fengler, T. Hummel, W. Fengler: Modellierung kooperierender Prozesse mit gefärb-ten Sequenzdiagrammen, in: J. Ruf (Hrsg.): 5. GI/ITG/GMM-Workshop: Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Syste-men. Shaker-Verlag Aachen (ISBN 3-8265-9859-8), S. 199-208, 2002.

[FeKDHS01] W. Fengler, E. Kallenbach, V. Duridanova, T. Hummel, E. Saffert: Zwischenbericht zum Forschungsvorhaben DFG: FE373/13-1: Entwurf eingebetteter paralleler Steuerungssysteme für integrierte multi-axiale Antriebssysteme, S. 1-20, TU Ilmenau, 2001.

[Fi97] L. Fisher: Flaw reported in new Intel chip, New York Times, 5. Mai, 1997.

[FrZ03] A. Franck, V. Zerbe: A Combined Continuous-Time/Discrete-Event Computation Model for Heterogeneous Simulation Systems, APPT'03: International Workshop on Advanced Parallel Processing Technologies, Xiamen (China), 17.-19. 9. 2003.

[GUHeB01] W. Günther, A. Hett, B. Becker: Application of linearly transformed BDDs in sequential verification, SP Design Automation Conference, 91-96, 2001.

[Gr03] D. Grell: Rad am Draht, Innovationslawine in der Automobiltechnik, c't, 10.07.03.

[Gur00] Daniel Gurovic, Wolfgang Fengler, Jürgen Nützel: "Development of Real-Time System Specifications through the Refinement of Duration Interval Petri Nets", IEEE International Conference on Systems, Man & Cybernetics, Nashville, pp. 3098-3103, October 8-11, 2000.

[HaHB02] W. Hartong, L. Hedrich, E. Barke: On Discrete Modeling and Model Checking for Nonlinear Analog Systems, CAV '02: International Conference on Computer-Aided Verification, LNCS, Vol. 2404, pp. 401-413, 2002.

[HeB95] L. Hedrich, E. Barke: A Formal Approach to Nonlinear Analog Circuit Verification, ICCAD '95: International Conference on Computer Aided Design, pp. 123-127, 1995.

[HeB98] L. Hedrich, E. Barke: "A Formal Approach to Verification of Linear Analog Circuits with Parameter Tolerances", DATE '98: Design, Automation and Test in Europe, pp. 649-654, 1998.

[HeB01] A. Hett, B. Becker: Supervised dynamic reordering in model checking, ITG/GI/GMM-Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen", 21-30, 2001.

[HeH01] L. Hedrich, W. Hartong: "Approaches to Formal Verification of Analog Circuits", Low-Power Design Techniques and CAD Tools for Analog and RF Integrated Circuits, P. Wambacq, eds., Kluwer Academic Publishers, Boston '01, 2001.

[HeHW97] T. A. Henzinger, P.-H. Ho, H. Wong-Toi: "A Model Checker for Hybrid Systems", CAV '97: International Conference on Computer-Aided Verification, LNCS, pp. 460-463, 1997.

[HeSB00] A. Hett, C. Scholl, B. Becker: Distance driven finite state machine traversal, Design Automation Conference, 39-42, 2000.

[HUB] Homepage der Berliner Forschergruppe für zeitabhängige Systeme und Petrinetz-Analyse (HU Berlin), http://www.informatik.hu-berlin.de/lehrstuehle/automaten/research.html.

[ITRS02] The International Technology Roadmap for Semiconductors, http://public.itrs.net/, 2002.

[Kr99] T. Kropf: Introduction to Formal Hardware Verification. Springer Verlag, 1999

[Kr02] T. Kropf: Tool-Supported Validation of Embedded Systems in Automotive Applications, edaForum, Hannover, 2002.

[KuLMPY02] R. Kurshan, V. Levin, M. Minea, D. Peled, H. Yenigun: Combining Software and Hardware Verification Techniques, Formal Methods in System Design, 2002.

[KuSK93] R. Kumar, K. Schneider, and T. Kropf: Structuring and Automating Hardware Proofs in a Higher-Order Theorem-Proving Environment; International Journal of Formal System Design, pp. 165-230, 1993.

[LaSH97] L. Lavagno, A. Sangiovanni-Vincentelli, H. Hsieh: Embedded Systems Co-Design: Syn-thesis and Verification, Kluwer Academic Publishers, 1997.

[LeKEB02] J. Levihn, M. Krieger, H. Eveking, C. Blank: „MCML - a markup language for a model-of-computation centered design and verification environment", FDL'02, Marseille 2002.

[Medea02] Medea+ EDA-Roadmap, http://www.medeaplus.org/webpublic/publ_relation_eda.htm, 2002.

[MLD] Homepage von MLDesigner (MLDesign Technologies Inc.), http://www.mldesigner.com/mldesigner.html.

[Mo65] G. Moore:" Cramming more components onto integrated circuits", Electronics, Volume 38, Number 8, April 19, 1965, http://www.intel.com/research/silicon/mooreslaw.htm.

[MuRHGR01] W. Müller, J. Ruf, D. W. Hoffmann, J. Gerlach, T. Kropf, W. Rosenstiel: The simula-tion semantics of SystemC, Design Automation and Test Conference (DATE), pp. 64-70, IEEE Press, March 2001.

[Nü99] Jürgen Nützel: „Objektorientierter Entwurf verteilter eingebetteter Echtzeitsysteme auf Basis höherer Petri-Netze", Dissertation, Technische Universität Ilmenau, ISLE, ISBN 3-932633-35-0, 1999.

[Petri] Internationale Petrinetz-Homepage (Aarhus, Dänemark), http://www.daimi.au.dk/PetriNets/.

[Ri00] G. Ritter: „Sequential equivalence checking by symbolic simulation", Proc. FMCAD'00, Springer LNCS, 2000.

[RuHKR01] J. Ruf, D. Hoffmann, T. Kropf, W. Rosenstiel: Simulation guided property checking based on multi-valued AR automata, Design Automation and Test Conference (DATE), IEEE press, March 2001.

[RuK00] J. Ruf, T. Kropf: Analyzing Real-time Systems, Design Automation and Test Confer-ence (DATE), pp. 243-248, IEEE Press, March 2000.

[RuK98] J. Ruf, T. Kropf: Using MTBDDs for Composition and Model Checking of Real-time Systems, FMCAD 98, Springer Verlag, 1998.

[Ru99] J. Ruf: Techniken zur Modellierung und Verifikation von Echtzeitsystemen. Dissertation an der Universität Karlsruhe, 1999.

[ScB01] C. Scholl, B. Becker: Checking equivalence for partial implementations, Design Automa-tion Conference, pp. 238-243, 2001.

[ScB02a] C. Scholl, B. Becker: Equivalence checking in the presence of incompletely specified boxes: ITG/GI/GMM-Workshop "Methoden und Beschreibungssprachen zur Modellierung und Verifi-kation von Schaltungen und Systemen", 2002.

[ScB02b] C. Scholl, B. Becker: Checking equivalence for circuits containing incompletely speci-fied boxes, International Conference on Computer Design, 2002.

[Sc03] W. Schleuter: Innovation durch Mikroelektronik im Automobil, 2. Ekompass Workshop, Han-nover, 29. - 30. 4. 2003.

[Shim02] K. Shimizu: Writing, verifying, and exploiting formal specifications for hardware design, Dissertation, Stanford University, 2002.

[StK97] D. Stoffel, W. Kunz: Record & Play: A Structural Fixed Point Iteration for Sequential Circuit Verification, Proc. 1997 ACM / IEEE Intl. Conference on Computer-Aided Design (ICCAD), S. 394-399, Nov. 1997.

[StK01] D. Stoffel, W. Kunz: Verification of Integer Multipliers on the Arithmetic Bit Level, Proc. International Conference on Computer-Aided Design (ICCAD), November 2001

[TimAut] Übersichtsseite der MIT-Forschergruppe zu Timed Automata, http://theory.lcs.mit.edu/tds/timed-aut.html.

[TINA] Homepage zum Analysator für Zeit-Petrinetze TINA, http://www.laas.fr/tina/.

[UF] Literaturdatenbank der Universität Freiburg, http://ira.informatik.uni-freiburg.de/cgi-bin/search/search

[Upp] UPPAAL: A Tool Suite for Verification of Real-Time Systems, http://www.brics.dk/FormalMethods/UPPALL.html.

[VIS96] The VIS Group: VIS: A system for verification and synthesis, In Computer Aided Verification, volume 1102 of LNCS, pages 428-432, Springer Verlag, 1996.

[Ze03] V. Zerbe: Mission Level Design of Complex Autonomous Systems. Invited paper at XLVII ETRAN Conference Herceg Novi, Montenegro, June 8-13, 2003.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart Schlussbericht

3. Titel des Berichts
Schlussbericht zum Förderprojekt „Funktionale Verifikation von Systemen“

4. Autoren des Berichts (Name, Vorname(n))
Volker, Schöber, Hans Eveking, Martin Schickel, Thomas Kropf, Jürgen Ruf, Stefan Lämmermann, Lars Hedrich, Alexander Jesser, Bernd Becker, Christoph Scholl, Alexander Pacholik, Wolfgang Fengler, Wolfgang Kunz

5. Abschlussdatum des Vorhabens
30.06.2007

6. Veröffentlichungsdatum
31.12.2007

7. Form der Publikation
Bericht

8. Durchführende Institution(en) (Name, Adresse)
Albert Ludwigsuniversität Freiburg im Breisgau, Johann Wolfgang Goethe Universität Frankfurt am Main, Technische Universität Darmstadt, Technische Universität Ilmenau, Technische Universität Kaiserslautern, Universität Tübingen, edacentrum e.V.

9. Ber.Nr. Durchführende Institution

10. Förderkennzeichen *)
01M3072

11. Seitenzahl Bericht
30

12. Literaturangaben

13. Fördernde Institution (Name, Adresse)

Bundesministerium für
Bildung und Forschung (BMBF)

53170 Bonn

14. Tabellen

15. Abbildungen

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

Für Deutschland ist einer der wichtigsten Märkte der Automobilmarkt. Für die Halbleiter-Industrie ist dieser Markt besonders wichtig, da er kontinuierlich hohe Wachstumsraten aufweist und damit großen Umsatz- und Gewinnschwankungen anderer Märkte ausgleichen kann. Die Wertschöpfung von nanoelektronischen Systemen im Auto liegt dabei bis zu 40 % in der Oberklasse, wobei Prognosen bis 2010 dies als Durchschnitt in der Automobiltechnik für möglich halten. Die Hersteller der nanoelektronischen Systeme sind in der Halbleiter-Industrie zu finden. Nanoelektronische Systeme sind hochintegrierte Bausteine. Sie werden als „Systeme auf einem Chip“ (System on a Chip, SoC) bezeichnet und bilden die Basis für die Innovation in der Nanoelektronik. Diese Bausteine müssen im Entwurfsprozess verifiziert werden, ob die die Funktion im Sinne der Spezifikation erfüllen.
Das Projekt FEST hat sich zum Ziel gesetzt, Lösungen zu erforschen, die eine einheitliche Verifikation von SoCs ermöglichen. Hierzu werden von einer Systembeschreibung bis hinunter zur elektrischen Ebene Methoden und Verfahren erforscht, die existierende Verifikationslücken schließen. Dazu werden neue Verifikationsverfahren erforscht, die in der industriellen Praxis als große Hürde zu sehen sind. Die Vernetzung verschiedener neuartiger Ansätze wird dabei durch die Durchführung des Projekts als Verbundprojekt unterstützt. Die verschiedenen Verifikationsansätze werden auf einer gemeinsamen Plattform integriert, um eine einheitliche Verifikationsmethodik zu ermöglichen aber unabhängig von einzelnen Lösungswerkzeugen zu bleiben. Mit den neuen Verifikationsansätzen kann die deutsche SoC-Industrie eine Verbesserung ihrer Entwurfsmethodik in 3-10 Jahren erreichen.
In den Bericht zum Projekt befindet sich neben den Zielen und Ergebnissen des Projekts eine Liste der Publikationen, die während der Projektlaufzeit veröffentlicht wurden.

19. Schlagwörter
EDA, Entwurfsautomatisierung, Funktionale Verifikation, Analoge Verifikation, Blockverifikation, Zeitverifikation,

20. Verlag	21. Preis
-	-

*) Auf das Förderkennzeichen des BMBF soll auch in der Veröffentlichung hingewiesen werden.

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) Final Report

3. title
Schlussbericht zum Förderprojekt „Funktionale Verifikation von Systemen“

4. author(s) (family name, first name(s))	5.end of project
Volker, Schöber, Hans Eveking, Martin Schickel, Thomas Kropf, Jürgen Ruf, Stefan Lämmermann, Lars Hedrich, Alexander Jesser, Bernd Becker, Christoph Scholl, Alexander Pacholik, Wolfgang Fengler, Wolfgang Kunz	30.06.2007
	6. publication date 31.12.2007
	7. form of publication Report
8. performing organization(s) (name, address) Albert Ludwigsuniversität Freiburg im Breisgau, Johann Wolfgang Goethe Universität Frankfurt am Main, Technische Universität Darmstadt, Technische Universität Ilmenau, Technische Universität Kaiserslautern, Universität Tübingen, edacentrum e.V.	9. originator’s report no. 01M3072
	10. reference no. 30
	11. no. of pages
13. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. no. of references
	14. no. of tables
	15. no. of figures

16. supplementary notes

17. presented at (title, place, date)

18. abstract
The semiconductor and chip industry are forming a market where functional requirements, complexity, time to market, cost pressure and shorting-living products are increasing dramatically. To compete in this market, a qualified verification process with short turnaround times is a key figure especially in markets with strong requirements regarding security and reliability of SoCs. The miniaturization of SoCs comes along – beside several advantages – with new challenges and questions in the design process that lead to technical and economic risks.

The aim of the FEST project is to research solutions for the unification of the SoC verification process by closing verification gaps from system level down to electric level. In this project, promising solutions are clustered to vision a coherent verification process. By using these new verification methodologies in future, the risks of re-design can be reduced, the time to market can be shortened or even a protection of market share can be achieved. Additionally, SoCs with more complexity then can be verified by formal methods.

19. keywords
EDA, Electronic Design Automation, Functional Verification, Analog Verification, Block Verification, Time Verification

20. publisher	21. price