[Mibench] http://www.eecs.umich.edu/mibench/

[Nicolaidis] Nicolaidis, „A Time Redundancy Based Soft-Error Tolerance to Rescue Nanometer Technologies", in 17th IEEE VLSI Test Symposium, 1999.

[San09] B. Sander, J. Schnerr, O. Bringmann: „ESL Power Analysis of Embedded Processors for Temperature and Reliability Estimations", International Conference on Hardware/Software Codesign and System Synthesis, Grenoble, France, 2009.

[Seb08] M. Sebastian, R. Ernst. „Modelling and Designing Reliable On-Chip Communication Devices in MPSoCs with Real-Time Requirements". In 13th IEEE International Conference on Emerging Technologies and Factory Automation. Hamburg, 2008.

[Seb09] M. Sebastian, R. Ernst. „Reliability and Safety Guarantees in Modern MPSoCs with Real-Time Requirements". edaWorkshop 2009. Dresden, 2009.

[SebE09] M. Sebastian, R. Ernst. „Reliability Analysis of Single Bus Communication with Real-Time Requirements". In 15th Pacific Rim International Symposium on Dependable Computing, 2009.

[Stechele07] W. Stechele, O. Bringmann, R. Ernst, A. Herkersdorf, K. Hojenski, P. Janacik, F. Rammig, J. Teich, N. Wehn, J. Zeppenfeld, D. Ziener, „Concepts for Autonomic Integrated Systems", eda-Workshop, Hannover, June 19-20, 2007

[Tamir90] Y. Tamir, Marc Tremblay: „High-Performance Fault-Tolerant VLSI Systems Using Micro Rollback". IEEE Trans. Computers 39(4): 548-554 (1990)

[WOR04] F. Worm, P. Ienne, P. Thiran, and G. De Micheli, „On-Chip Self-Calibrating Communication Techniques Robust to Electrical Parameter Variations," IEEE Design & Test of Computers, vol. 21, no. 6, pp. 524–535, Nov. 2004.

[XIL] Xilinx, http://www.xilinx.com/.

[ZT08] D. Ziener and J. Teich, „Concepts for Autonomous Control Flow Checking for Embedded CPUs", In Proceedings of the 5th International Conference on Autonomic and Trusted Computing (ATC-08), pp. 234-248, Oslo, Norway, June 23-25, 2008.

[ZT09] D. Ziener and J. Teich. „Concepts for run-time and error-resilient control flow checking of embedded RISC CPUs". Int. Journal of Autonomous and Adaptive Communications Systems, Vol. 2, No. 3, pages 256-275, 2009, Inderscience Enterprises Ltd.

SANITAS – Sichere Systeme auf Basis einer durchgängigen Verifikation entlang der gesamten Wertschöpfungskette

BMBF-Projekt zur Verbesserung der Verifikation entlang der Wertschöpfungskette für die exemplarische Anwendung an der Industrieautomatisierung gestartet.

Gefördert durch das Bundesministerium für Bildung und Forschung

Die Beherrschung hochautomatisierter Fertigung von äußerst komplexen Produkten, die oft höchste Anforderungen an die Betriebssicherheit erfüllen müssen, macht den Standort Deutschland heute einmalig und auch im Vergleich zu Niedriglohnländern als Entwicklungs- und Produktionsstandort wettbewerbsfähig. Der Erfolg hängt dabei wesentlich davon ab, dass die Sicherheitseigenschaften der Produkte, Systeme und der Fertigungsanlagen, auf denen sie hergestellt werden, durch eine lückenlose Verifikation garantiert werden können. Das vom BMBF seit dem 1.10.2009 unter dem Förderkennzeichen 01 M 3088 geförderte Forschungsvorhaben SANITAS erforscht und entwickelt eine ebenenübergreifende Systemverifikationsmethodik auf Basis virtueller Modelle. SANITAS bezieht dabei alle Ebenen der Produktentwicklungskette vom mikro-/nanoelektronischen Teilsystem bis zum Endprodukt in die Verifikation mit ein. So wird erstmalig eine durchgängige Verifikation entlang der gesamten Entwicklungskette bis hin zur Fertigung zur Verfügung gestellt.

Man stelle sich ein in naher Zukunft durchaus realistisches Szenario vor, in welchem ein mobiler Serviceroboter als elektronischer Assistent für alltägliche Handgriffe im Haushalt zur Verfügung steht. Anstatt jedoch zuverlässig einen frisch gebrühten Kaffee zu servieren, kollidiert der Helfer auf seinem Weg aus der Küche mehrfach und verschüttet so die Hälfte des Getränks. Die andere Hälfte geht verloren, als die Tasse knapp neben der Tischplatte abgestellt wird.

Was im skizzierten Zukunftsszenario für den privaten Endanwender einfach nur ärgerlich ist und ihn eventuell davon abhalten wird, weitere Roboter zu erwerben, besitzt im Kontext der industriellen Fertigung bereits heute eine deutlich dramatischere Dimension: In heutigen automatisierten Fertigungsanlagen ist ein Betrieb von Industrierobotern nur in Sicherheitskäfigen oder abgeschirmten Räumen möglich, um so eine Gefährdung der beteiligten Bedienkräfte aus-

Zusammensetzung des Projektkonsortium

Projektpartner
Fraunhofer-Gesellschaft, IIS
Forschungszentrum Informatik
Infineon Technologies AG
Micronas AG
Robert Bosch GmbH
Siemens AG
Tieto Deutschland GmbH
Universität Bremen
Universität Paderborn

Unterauftragnehmer
Universität Tübingen
OFFIS e.V. – Institut für Informatik
TU München

Förderkennzeichen des Vorhabens
01M3088

Laufzeit
01.10.2009 – 30.09.2012

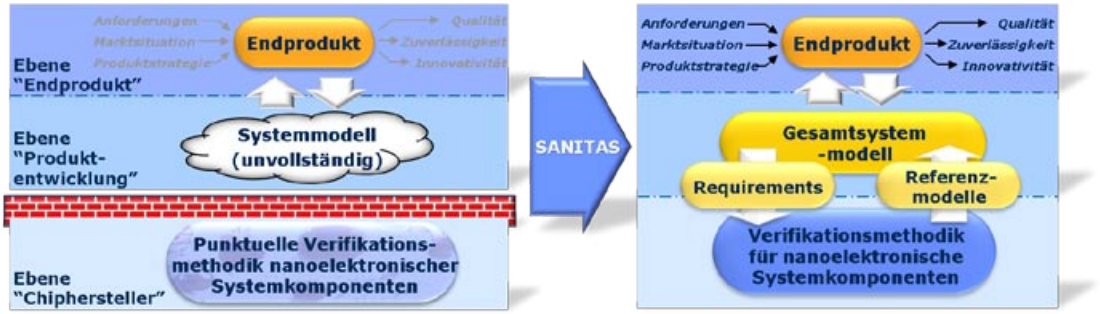

Abbildung 1.11: Verbesserung der Produktentwicklungskette

zuschließen. Ebenso ist ein Zugriff auf den Roboter nur bei abgeschalteter Anlage gefahrlos möglich. Dies schränkt die Zusammenarbeit von Mensch und Maschine wesentlich ein. Dabei kommt gerade dem engen Ineinandergreifen von menschlichen und automatisierten Arbeitsschritten eine Schlüsselrolle in zukünftigen Produktionsprozessen zu: So stoßen etwa konventionelle Industrieroboter an ihre Grenzen, wenn die Aufgabenausführung ein besonders hohes Maß an Wahrnehmung, Geschicklichkeit, Flexibilität oder Entscheidungsfähigkeit erfordert. Dies kann heute nicht vollautomatisiert unter der Gewährleistung von Arbeitssicherheit und Kosteneffizienz verwirklicht werden. Dabei leisten Industrieroboter wertvolle Unterstützung, wenn hohe Kraft, Ausdauer, Schnelligkeit und Präzision erforderlich sind oder die Umgebungsbedingungen – etwa hohe Temperaturen oder chemische Belastungen – ein Arbeiten des Menschen schwierig oder unmöglich machen. Damit stellt das enge und wirkungsvolle Ineinandergreifen von Mensch und Maschine die Grundvoraussetzung für eine effiziente und flexible Produktion zukünftiger hochinnovativer Güter dar.

Die Forschungs- und Entwicklungsaktivitäten im Rahmen des SANITAS-Projektes schaffen die Grundlage dafür, die Flexibilität und den sicheren Betrieb komplexer mikroelektronikgestützter Systeme, z. B. in der Fertigungsautomatisierung oder Automobilelektronik, zu steigern. Hierfür will SANITAS eine für die gesamte Wertschöpfungskette – also vom Halbleiterunternehmen bis zum Hersteller des Endprodukts, in dem die neu entwickelten Chips eingesetzt werden – eine durchgängige Verifikationsmethodik schaffen, die bereits in der Entwicklungsphase der Systemkomponenten eingesetzt wird. Mit der Verifikationsmethodik lassen sich Fehler noch vor der eigentlichen Produktion der Systemkomponenten aufdecken.

Die durchgängige Verifikationsmethodik erlaubt z. B. die automatische Überprüfung, ob technische Vorgaben umsetzbar sind. Außerdem arbeiten die Projektpartner an neuen Modellierungsverfahren, die es Zulieferern erlauben sollen, virtuelle Referenzmodelle ihrer Komponenten zu entwickeln. Mit diesen Modellen können Systemhersteller ihre Produkte am Computer entwerfen und sie noch vor der tatsächlichen Herstellung testen, korrigieren und verifizieren. Die neuen Methoden sollen exemplarisch an Systemen der Industrieautomatisierung erarbeitet werden. Sie werden aber gleichermaßen in anderen Domänen z. B. in der Kommunikations- und Automobilindustrie einsetzbar sein.

Das im vom BMBF geförderten Projekt SANITAS angestrebte Ziel einer Methodik für eine durchgängige Verifikation entlang der gesamten Wertschöpfungskette von der Mikroelektronik bis hin zum Endprodukt hebt die zum heutigen Zeitpunkt bestehende Barriere zwischen Systemintegratoren (Ebene „Produktentwicklung“ in Abbildung 1.11) und Teilsystemzulieferern (Ebene „Chiphersteller“ in Abbildung 1.11) auf. Dadurch wird erstmalig ein geschlossener Entwurf von komplexen und hochinnovativen Komponenten und Systemen ermöglicht, die bereits bei der ersten Inbetriebnahme sicher funktionieren. Die dadurch erzielbare Verkürzung der Entwicklungszeiten für sicherheitskritische Komponenten und Systeme führt zusätzlich zu einer weiteren Verbesserung der Wettbewerbsfähigkeit deutscher Unternehmen.

Ziele

In SANITAS wird eine Absicherungsstrategie verfolgt, die gewährleistet, dass folgende Anforderungen berücksichtigt werden: effektives Ineinandergreifen der verschiedenen Ebenen der Produktentstehung, Gewährleistung der Kommunikation zwischen Systemintegrator und Teilsystemzulieferer selbst bei komplexen Produktanforderungen, Erzielung einer geringen Leistungsaufnahme, Lieferung höchster Qualität als Basis sicherer und zuverlässiger Produkte. Diese Absicherungsstrategie setzt sich zusammen aus der Anwendung von virtuellen System-Prototypen als Referenzmodelle und der automatischen Erstellung von Verifikationsumgebungen aus Requirements. Die Absicherungsstrategie wird in drei Phasen umgesetzt:

1. Phase: Systemdefinition (durch Systemintegratoren, Ebene Produktentwicklung)
   Die Produktanforderungen werden in formalen Modellen (Metamodelle) erfasst, aus denen in einem automatisierten Prozess schnelle Simulationsmodelle und Verifikationsszenarien erzeugt werden. Die Metamodelle der Produktanforderungen (Requirements) des Gesamtsystems werden weiter in Metamodelle der Teilsysteme aufgeteilt. Metamodelle können also auch hierarchisch aufgebaut sein.

2. Phase: Verifikation Teilsystem/SOC (durch Teilsystemzulieferer, Ebene Chiphersteller)
   Virtuelle Prototypen für die Teilsysteme werden teil-automatisch aus den Metamodellen der Teilsysteme von Phase 1 generiert. Für die Verifikation werden weiter abstrahierte Referenzmodelle sowie Verifikationsszenarien erstellt. Verifikationsszenarien für die Teilsysteme werden automatisch aus den Metamodellen erzeugt und damit die virtuellen Prototypen der Teilsysteme verifiziert und optimiert. Diese werden später zur Absicherung des weiteren Implementierungsprozesses eingesetzt. Die Referenzmodelle der Teilsysteme werden an den Produkthersteller geliefert.
3. Phase: Systemverifikation (durch Systemintegratoren, Ebene Produktentwicklung)
   Mit den in Phase 1 generierten Verifikationsszenarien und den Referenzmodellen der Teilsysteme aus Phase 2 wird eine Systemsimulation durchgeführt. Dabei wird die Systemarchitektur analysiert. Bei zu hoher Leistungsaufnahme werden die Schritte 1-3 mit einer weiter optimierten Architektur wiederholt.

Struktur

Zum Erreichen dieses dreiphasigen Prozesses ist das Projekt SANITAS in vier thematisch stark ineinandergreifende Arbeitspakete gegliedert:

AP 1: TLM-Verifikationsmethodik
AP 2: Generierung der TLM-Verifikationsumgebung
AP 3: Abstrakte Analysemodelle
AP 4: Durchführung der Verifikation

Im Arbeitspaket 1 „TLM-Verifikationsmethodik“ werden neue Verifikationstechniken entwickelt und als grundlegende Technik den weiteren Arbeitspaketen zur Verfügung gestellt, welche die Besonderheiten der TLM-Modellierung ausgleichen und auf existierende Techniken zurück führen. Insbesondere soll die Abfolge von Ereignissen in den TLM-Modellen in ein geordnetes Raster überführt werden, um eine deterministische Ordnung und zeitliche Anordnung zu erhalten. Als zweiten Schritt soll eine Verfeinerungsstrategie und Verfeinerungsnotation für Metamodelle von Produkten – zum Beispiel der digitalen Fabrik – entwickelt werden, um damit Verifikationsszenarien automatisch aus den Metamodellen herleiten zu können. Die Generierung der Verifikationsszenarien und auch der Verifikationsumgebung soll modellorientiert im Arbeitspaket 2 „Generierung der Verifikationsumgebung“ erforscht werden. Dabei liegt der Schwerpunkt der Arbeiten darin, die allgemeine Methode an die Anforderungen der Verifikation von komplexen Produkten in den Domänen sicherer Kommunikationstechnik, hochqualitativer Bild- und Signalverarbeitung sowie intelligenter Automobilelektronik und flexibler Industrieautomatisierung anzupassen und dafür sogenannte Spezifikationen für Metamodelle und Code-Generatoren zu erstellen. Um den so – hoch effizient – generierten Verifikationsszenarien Erwartungswerte an die Hand geben zu können, werden im Arbeitspaket 3 „Abstrakte Analysemodelle“ noch abstraktere Modellierungsmethoden als die der TLM-Modellierung erforscht. Ansatzpunkte sind hier die Einbeziehung von Firmware in die Funktionalität der Modelle, die Akkumulierung des Leistungsverbrauchs ähnlich der Akkumulierung von Zeiten bei der TLM-Modellierung, und die Optimierung von Zeit- und Leistungsparametern in Modellen, um die Genauigkeit von Simulationen auf niedrigeren Abstraktionsebenen zu erreichen. Eine 50x schnellere Simulationszeit bei 10 % Abweichung der nichtfunktionalen Werte von der TLM-Simulation wird hier angestrebt. Um TLM-Modelle, Verifikationsumgebung, Verifikationsszenarien und Referenzmodell gemeinsam simulieren zu können, werden im Arbeitspaket 4 „Durchführung der Verifikationsumgebung“ Verfahren zum Zugriff der Verifikationsmodelle auf Designmodelle erarbeitet. Darüber hinaus werden in diesem Arbeitspaket spezielle Debugging-Techniken für die Komplettsimulation untersucht und der beste Ansatz weiter ausgearbeitet.

Projektstatus

Das SANITAS-Projekt wurde zum 01.10.2009 mit einer Laufzeit von drei Jahren vom Bundesministerium für Bildung und Forschung bewilligt (Förderkennzeichen 01M3088). Die Partner haben ein Kickoff-Treffen bei dem Projektpartner Infineon Technologies AG in Neubiberg abgehalten (s. Abbildung 1.12). Erste Ergebnisse werden im 1. Quartal des kommenden Kalenderjahres erwartet und auf dem edaWorkshop10 vorgestellt.

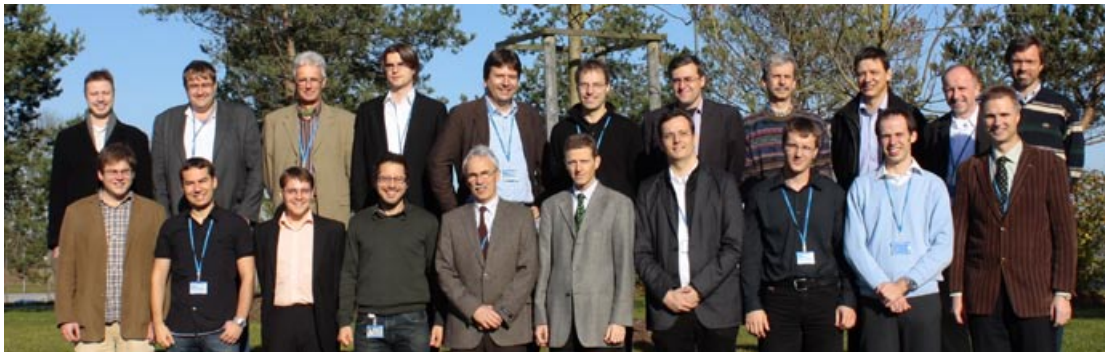

Abbildung 1.12: Das Projektkonsortium beim Kickoff-Treffen

Kont@kt & Autor
Dr. Volkan Esen
Projektkoordination und -management
Infineon Technologies AG
fon: (0 89) 2 34 – 2 78 14,
Volkan.Esen@infineon.com