



## HERKULES: Hardwareentwurfstechnik für Null-Fehler-Designs

**Ziel von HERKULES ist es, einen Großteil der bei der Verifikation der Kommunikationsstruktur anfallenden Aufgaben formal durchzuführen, höchste Qualität mit überlegener Produktivität zu koppeln und diese Qualität zu einem Produktvorteil zu machen. Für die Verifikation des Gesamtsystemkonzepts wird die simulationsbasierte Verifikation weiterhin benötigt werden. Sie wird aber durch HERKULES-Techniken von einer Fülle von Aufgaben der Codeverifikation entlastet, die so weit besser bewältigt werden können.**

### Ein verdecktes Problem – Folgekosten von Hardwarefehlern

Die Gesellschaft hat sich daran gewöhnt: Hardware- und Softwaresysteme sind so komplex geworden, dass Fehlfunktionen unvermeidlich sind. Immer wieder wird diese Zwangsläufigkeit anhand schwerer Unfälle oder wirtschaftlicher Schäden in großer Höhe medienwirksam in Szene gesetzt. So schwerwiegend solche Fehlfunktionen sind, und so wichtig es ist, die Fehlerfolgen zu diskutieren, geht es im industriellen Alltag vielmehr um die Auswirkungen von Fehlern im Allgemeinen.

Je nach Branche muss die Industrie extrem viel Zeit und Geld investieren, um das Restfehlerrisiko zu minimieren. Dennoch, Fehler werden gemacht, und daher sind die Entwicklungsprozesse für IT-Produkte so angelegt, dass Fehler auch dann noch durch „Patches“ (Nachbessern) behoben werden können, wenn sie – oft lange nach ihrer Entstehung – gefunden werden. Ganze Abteilungen und Firmen leben von solchen „Patches“, die allerdings über die Zeit ein ursprünglich wohlstrukturiertes System in ein nicht mehr beherrschbares „digitales Monster“ verwandeln können. Man verwaltet Fehler eher, als diese gleich nach ihrer Entstehung zu eliminieren – da korrekter Code nach dem Stand der Kunst nicht möglich ist. Diese eingefahrene Praxis hat ihren Preis. Die „Veredelungskette“ einer Hardwaresteuerung, eines sogenannten Mikrocontrollers, soll dies verdeutlichen:

Jeder Hersteller eines solchen Chips liefert mit diesem ein Dokument (Errataliste) aus, das bislang bekanntes Fehlverhalten des Controllers beschreibt und, wo möglich, angibt, wie dieses Fehlverhalten bei der Programmierung des Controllers umgangen werden kann. Je länger ein Controller vertrieben wird, desto mehr Fehler werden von der wachsenden Anzahl seiner Nutzer gemeldet. Zwar werden in jeder neuen Version Fehler eliminiert, doch die Fehlerbehebung ist auch Quelle neuer Fehler. Bereits für die mittlere Leistungsklasse von Mikrocontrollern sind mehr als 30 derart dokumentierte Fehlfunktionen nicht ungewöhnlich. Die Dunkelziffer für – noch – nicht entdeckte Fehler im ersten Drittel der Lebenszeit eines Mikrocontrollers schätzen Fachleute auf mindestens 5 Fehler pro 10 000

Zeilen Code des zugehörigen Designs. Diese Fehler – dokumentierte wie undokumentierte – verursachen zusätzlichen Aufwand und Risiken in den nachfolgenden Wertschöpfungsstufen, denn der Programmierer des Controllers muss neben dem normalen auch noch das „außerplanmäßige“ Verhalten der Hardware verstehen und bei der Programmierung berücksichtigen. Der Maschinenbauer, der danach diese Steuerung in seine Maschine einbaut, stößt bei der Integration auf unerwartetes – manchmal unerwünschtes – Verhalten, das nachzubessern ist. Schlimmstenfalls wird ein Anlagenbauer, in dessen Anlage diese Maschine arbeitet, mit teuren Produktionsausfällen beim Einsatz seiner Anlage konfrontiert.

Der Preis eines Standard-Mikrocontrollers rangiert zwischen Cents und wenigen Euro. Die oben ange-deuteten Folgekosten von Fehlern dieser Controller liegen dagegen um viele Größenordnungen über diesem Preis. Aufgrund der millionenfachen Verbreitung solcher Hardwarebausteine liegt daher in der Verfügbarkeit korrekter Controller (s. u.) ein enormes volkswirtschaftliches Einsparpotential. Im Übrigen deuten erste Umfragen bei Nutzern solcher Bausteine darauf hin, dass der Markt die Hersteller korrekter Mikrocontroller mit verstärkter Nachfrage und höheren Preisen „belohnen“ würde, wenn es sie denn gäbe. Diese Hersteller würden sogar in doppelter Weise profitieren, denn mittlerweile müssen sie einen wachsenden „software content“ mit ihren Hardwareprodukten liefern und wären daher selbst Nutznießer des o. g. Einsparpotenzials an Fehlerfolgekosten.

### Durchbruch in der Entwurfstechnik

Im Rahmen des Projekts VALSE „Hochautomatisierte, zertifizierende und skalierende Validierung von System-on-Chip-Entwürfen“ wurde innerhalb von 4 Jahren eine Entwurfstechnik geschaffen (formale Modulverifikation), die das Gros der Fehler (sog. funktionale Fehler im Gegensatz etwa zu Produktionsfehlern) in Mikrocontrollern und vielen anderen Hardwarebausteinen zu eliminieren vermag. Während bei VALSE noch die Aufbereitung der formalen Basistechnik für die Anwendung auf industrielle Schaltungen im Vordergrund stand, verschob sich der Schwerpunkt der Arbeiten im

Zusammensetzung des  
Projektkonsortiums:

#### Partner:

Concept Engineering GmbH  
Infineon Technologies AG  
Alcatel-Lucent  
Melexis GmbH  
OneSpin Solutions GmbH  
Robert Bosch GmbH

#### Unterauftragnehmer:

IMMS Ilmenau  
Technische Universität Chemnitz  
Technische Universität Kaiserslautern  
Universität Bremen  
Universität Duisburg-Essen  
Universität Karlsruhe

Nachfolge-Projekt VALSE-XT auf die systematische Beschaffung und Analyse einer verlässlichen formalen Spezifikation, die dann als Eingabe für formale Prüfverfahren diente. Im BMBF-Projekt VERISOFT wird diese Technik – ergänzt um weitere Beweisverfahren – eingesetzt, um in einem weit vorgeschrittenen, weltweit einmaligen Großversuch nachzuweisen, dass die Entwicklung eines modernen eingebetteten 32-bit-Mikrocontrollers ohne funktionale Fehler technisch machbar und wirtschaftlich ist.

Die neuen Verfahren zur Entwicklung korrekter Hardwarebausteine ermöglichen aber nicht nur die oben diskutierten Produktvorteile. Messdaten aus den VALSE-Projekten und VERISOFT zeigen, dass sich darüber hinaus höchste Qualität mit hoher Produktivität der neuen Verifikationstechnik paart.

### **Umsetzung – technische und mentale Hürden**

Produktvorteile sowie massive Qualitäts- und Produktivitätsgewinne sind starke Argumente für eine neue Entwurfstechnik. Dennoch sind bei der Umstellung von der heutigen auf Simulation beruhenden Verifikationspraxis auf die neuen Verfahren erhebliche Hürden zu überwinden:

Ausbildung, Werkzeuge, Methodik und Designsysteme müssen aktualisiert werden. Hinter diesen Verfahren muss ein verlässliches kommerzielles Angebot mit ausreichenden Schulungskapazitäten stehen. Vor allem aber muss sich die Herangehensweise ändern. Diese ist in der Mikroelektronikindustrie auf die Funktion eines Chips, seine Herstellungskosten und das Zeitfenster mit den größten Marktchancen fixiert. Qualität wird nur vereinzelt als differenzierendes Produktmerkmal gesehen. Dass solche Einstellungen schnell ins Wanken kommen und dann hohe Kosten verursachen können, zeigt das Beispiel des Dieselfilters. Dieser hat nichts mit der hochoptimierten Funktion deutscher Diesellaggregate zu tun. Dennoch entsteht plötzlich durch mehr oder weniger berechtigte öffentliche Meinung und Gesetzesvorlagen massiver Druck auf die Automobilhersteller, ihre Emissionswerte für Dieselschadstoffe zu verbessern. Ansonsten drohen Marktpositionen und Image beeinträchtigt zu werden. Den Feinstaubpartikeln entsprechen bei den Hardwarebausteinen „schwer zu findende“ Fehler, die von den neuen Verfahren systematisch „herausgefiltert“ werden. Veränderungsdruck könnte hier von der Produkthaftung oder – besser – von Nachfrage und Marktchancen ausgehen.

### **Der nächste Durchbruch – von korrekten Hardwarebausteinen zu korrekten Hardwaresystemen**

Früher wurden Hardwaresysteme ausschließlich durch Verdrahtung von Chips auf einer Leiterplatte gebaut. Mit heutiger Fertigungstechnologie kann die Funktionalität kompletter Leiterplatten auf einem einzigen Chip, einem so genannten System-on-Chip (SoC), integriert werden. So werden Verbesserungen bezüglich Fläche,

Stromverbrauch und Robustheit möglich, die Produktinnovationen quer durch alle Branchen treiben.

Die Charakterisierung dieser SoC ist eine Ansammlung von Superlativen: Ein solcher Chip enthält bis zu einige Hundert Millionen Transistoren und wird von Hunderten von Entwicklern in ca. 18 Monaten entwickelt. Die Umsatzerwartungen liegen jenseits von 500 Millionen Euro. Auch die Fehlerrisiken sind spektakulär: Die Suche nach Designfehlern verschlingt über 60 % des FuE-Budgets. Schwere Fehler, die nur beim Test erster Chips gefunden werden, erfordern oft mehrere „Respins“, die jeweils schon bald über 1 Million Euro kosten werden. Unterschätzte Verifikationsaufwände, die die Markteinführung um 3 Monate verzögern, können bis zu 25 % des erwarteten Umsatzes vernichten.

Selbst große Firmen können sich daher nur wenige solcher aufwändigen Entwicklungen zeitgleich leisten. Ihr Schicksal und erst recht das kleinerer Firmen hängt davon ab, die Risiken bezüglich Marketing, Entwicklung und gegebenenfalls der Produktion weniger großer Chips zu meistern. An die Stelle einer Risikoverteilung über viele kleine Chips tritt eine Auslese nach dem Prinzip „Alles oder Nichts“.

Zeit ist bei der Entwicklung eines SoC die knappste Ressource. Daher kann ein solcher Chip nicht vollständig neu entwickelt werden. Ein Großteil seiner Funktionalität muss aus vorgefertigten Designs häufig benötigter Bausteine – so genanntem Intellectual Property (IP), d. h. Designs von Prozessoren, Peripheriebausteinen, Speichern usw. – „zusammengesteckt“ werden. Das Zusammenwirken dieser IP gemäß einer hoch komplexen Kommunikationsstruktur erbringt dann die geforderte Systemfunktionalität. Die Anpassung des SoC an Besonderheiten von Kunden erfolgt über Software.

Abgesehen von der Beherrschung der weiteren Miniarisierung sind Mängel in der Designqualität (s. o.) das größte Risiko bei der Entwicklung eines SoC. Die Antwort der EDA-Industrie auf diese Probleme heißt vereinfacht „mehr Simulation, mehr Rechner und mehr Personal“. Dies ist nach Einschätzung der Projektpartner keine zukunftsfähige Lösung. Denn die prinzipiellen Grenzen der Simulation und die damit verbundenen Bedrohungsszenarien werden von der Fachwelt übereinstimmend anerkannt.

Vereinfacht gesagt, besteht ein SoC aus IP und einer hoch komplexen Kommunikationsstruktur. Technisches Ziel von HERKULES ist es, einen Großteil der bei der Verifikation der Kommunikationsstruktur anfallenden Aufgaben formal durchzuführen. Dabei wird auch hier wieder unter maximaler Nutzung der VALSE- und VALSE-XT-Ergebnisse versucht, höchste Qualität mit überlegener Produktivität zu koppeln und diese Qualität zu einem Produktvorteil zu machen. Sicherheitshalber sei betont: Für die Verifikation des Gesamtsystemkonzepts wird die simulationsbasierte Verifikation

weiterhin benötigt. Sie wird aber durch die VALSE- und HERKULES-Techniken von einer Fülle von Aufgaben der Codeverifikation entlastet.

In **HERKULES-1, „Basistechniken“**, werden die algorithmischen Grundlagen für das Vorhaben geschaffen: Diese Algorithmen automatisieren die in HERKULES-2 und -3 beschriebenen Verifikationsaufgaben zu großen Teilen.

In **HERKULES-2, „2-Punkt-Kommunikation“**, werden formale Verifikationslösungen für die Kommunikation von zwei Modulen entwickelt. Bedarf an solcher Integrationsverifikation besteht prinzipiell bei jedem Schaltungsentwurf und insbesondere in der Kommunikationstechnik mit ihren vielen aufeinander folgenden Blöcken zur Bearbeitung der Kommunikationsdaten. Die zu erforschenden Verfahren erleichtern die Fehlerlokalisierung, verlagern die Integrationsverifikation auf einen früheren Zeitpunkt und finden letztlich alle funktionalen Integrationsfehler. Der Austausch von Chips im Feld, die aufgrund solcher Fehler nicht funktionieren, wird damit komplett vermieden.

In diesem Arbeitspaket sind auch die Leitanwendung der HERKULES-Technik auf Kommunikationsbausteine für Datenübertragungsnetze und die Verifikation eines LIN-Knotens platziert:

Die SDH-Protokolle (Synchrone Digitale Hierarchie) wenden statisches (leitungsorientiertes) Routing an, um die Wege der Rahmen im optischen Netz festzulegen. Die neuesten Systeme verbinden die statische Wegwahl des SDH-Standards mit der dynamischen, paketerorientierten Wegwahl wie beispielsweise im Internet Protokoll (IP). Diese Verbindung von dynamischen und statischen Routing-Protokollen hat einen erhöhten Maintenance- und Monitoring-Aufwand seitens der Netzbetreiber zur Folge. Es müssen z. B. komplizierte Quality-of-Service- (QoS) Abfragen in ASICs implementiert werden, die in den zugrunde liegenden Standards nicht bis in jede Einzelheit definiert wurden. Angesichts dieser „weichen“ Standards simulativ die nötige Verifikationssicherheit zu erlangen, ist mit immensem Zeitaufwand verbunden.

Daher werden die o. g. dynamischen Routingprotokolle einschließlich ihrer QoS-Abfragen häufig mit FPGAs implementiert, um so aufwandsarm im System nachbessern zu können. FPGAs sind jedoch in ihrem Durchsatz und in ihrer Größe limitiert und auch das Nachbessern „im Feld“ ist dem Image des Systemherstellers abträglich. Die formale Aufarbeitung der Standards und die Bereitstellung von Bibliotheken von formalen Verifikationskomponenten (FVC) für die neuen Datenübertragungsprotokolle steigern die Verifikationssicherheit um Größenordnungen und verkürzen die Entwicklungszeit.

In **HERKULES-3, „Mehrpunkt-kommunikation“**, wird die Korrektheit von Bussystemen adressiert. Solche Systeme sind das Rückgrat von SoCs, und Fehlerfunktionen in diesem Bereich haben oft gravierende Auswirkungen. Die geplante Aktivität soll fehlerfreie Kommunikation sichern und die Fehlerfindung auf die Phase der Modulverifikation vorverlegen, wo die Fehlerlokalisierung vergleichsweise einfach und die Fehlerkorrekturen kostengünstig sind. Zusätzlich soll der Aufwand in der Systemsimulation deutlich sinken, weil anders als in der heutigen Praxis keine Kommunikationsfehler mehr zu identifizieren und zu beheben sind.

In **HERKULES-4, „Methodik“**, sollen die in VALSE-XT und HERKULES entwickelten technischen Verfahren methodisch so aufbereitet werden, dass sie sowohl für Anbieter von integrierten Schaltungen als auch deren Anwender bzw. Integratoren insbesondere unter dem hohen Qualitätserfordernis „Null-Fehler-Design“ einsetzbar werden. Dabei sollen verschiedene Sichtweisen auf die Verifikationsaufgabe berücksichtigt werden. Neben der rein technischen Betrachtung wird beschrieben werden, wie Verifikationsprojekte unter Einbeziehung von HERKULES-/VALSE-XT-Technologie zu planen und zu überwachen sind. Für die administrative Ebene technischer Überwachung insbesondere sicherheitskritischer Anwendungen soll am Beispiel der Automobilelektronik eine geeignete Zertifizierungsmethodik entwickelt werden, die mit Hilfe der HERKULES-Technologie geltende Qualitätsstandards bzw. Normen erfüllt.

**Kont@kt (HERKULES):**

Hans Sahn

Alcatel Lucent Deutschland AG  
O-TH14 Optical Networking  
Thurn- und Taxisstr. 10  
90411 Nürnberg  
fon: (09 11) 5 26-26 38  
hsahm@alcatel-lucent.com

Weitere Informationen sind  
unter [http://www.edacentrum.de/  
herkules/](http://www.edacentrum.de/herkules/) zu finden.