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 „Patchen" (Nachbessern) behoben werden können, wenn sie – oft lange nach ihrer Entstehung – gefunden werden. Ganze Abteilungen und Firmen leben von solchen „Patchworks", 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 angedeuteten 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 Mikrocon-

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