Diss. ETH Nr. 11'916

Rapid-Prototyping eingebetteter Systeme

ABHANDLUNG
zur Erlangung des Titels
DOKTOR DER TECHNISCHEN WISSENSCHAFTEN
der
EIDGENÖSSISCHEN TECHNISCHEN HOCHSCHULE ZÜRICH

vorgelegt von
Rudolf Eugen Mattmann
Dipl. El.-Ing. ETH

geboren am 5. Juli 1960
von Luzern

Angenommen auf Antrag von:
Prof. Dr. A. Kündig, Referent
Prof. Dr. D. Hogrefe, Korreferent

1996

Kurzfassung

Die vorliegende Arbeit präsentiert eine neue Entwicklungsmethode für eingebettete Systeme, die sich auf eine formale grafische Notation abstützt, und stellt dazu die systematische Definition eines durchgehenden Rapid-Prototyping-Werkzeuges vor.

Die Arbeit definiert die neu entwickelte Spezifikationssprache der Specs-(Petri)-Netze, die zugehörige seiteneffektfreie Netzbeschriftungssprache SpecsLingua und stellt den in Smalltalk programmierten objekt-orientierten Compiler vor. Die formale Analysierbarkeit der Modelle zum Zwecke einer Korrektheitsanalyse wird anhand der Konflikt- und Invarianten-Analyse aufgezeigt. Weiter wird die Entwicklung eines parallelen Simulationsalgorithmus' vorgestellt, mit dem sich Specs-Netze auf einem Parallelrechner mit verteilter Architektur effizient simulieren lassen. Ebenso wird gezeigt, wie sich mittels 'simulated annealing', einem bekannten Optimierungsverfahren, dieses parallele Simulationsprogramm automatisch auf einen frei konfigurierbaren Parallelrechner, bestehend aus Transputern, abbilden lässt. Als Implementierungssprache wird Occam-2 verwendet. Mit Hilfe dieses parallelen Simulators lassen sich Spezifikationen von reaktiven Systemen in ihrer realen Umgebung in Echtzeit ausführen und testen. Die Arbeit stellt zudem eine integrierte Entwicklungsumgebung für Specs-Netze vor, erläutert zwei Beispielanwendungen und zieht einen Vergleich zu einem Smalltalk-erweiterten Petri-Netz-Werkzeug und zu SDL.

Das hier vorgestellte Rapid-Prototyping-Werkzeug verwendet eine modellbasierte Spezifikationssprache, unterstützt die formale Verifikation von Verhaltenseigenschaften, erlaubt die Validierung eines modellierten Echtzeitsystems in Feldtests und ermöglicht die automatische Transformation einer Spezifikation in eine Software- oder Hardware-Implementierung.

Abstract

The development of embedded systems with semi-formal diagramming techniques and handcoding is time consuming and error prone. A more efficient development methodology will, therefore, be presented that uses a formal method based on a graphical notation. A new rapid-prototyping tool will also be defined that supports all development processes from specification to implementation.

The tool is used to specify the functional behaviour of the system under development by graphically modelling the system, its environment and its user interface. The graphical specification language used, Specs nets, is a new high level Petri nets class. It provides a firm mathematical basis allowing the formal analysis of Specs (Petri) nets and the detection of errors in the specification. Specs nets represent an executable specification language such that specification models can be simulated. For Specs (Petri) nets a new distributed simulation algorithm has been developed for scaling up the simulation speed on a parallel computer. This allows the real time simulation of a Specs nets model, which can then be used as a system prototype. The Specs nets method further allows the automatic transformation of specifications into software and hardware implementations.

The thesis defines Specs (Petri) nets, a new class of high level Petri nets. It also defines the accompanying side-effect-free net inscription language SpecsLingua, and presents the object-oriented Specs nets compiler written in Smalltalk. Specs nets are shown to be formally analysable by conflict and invariant analysis. The systematic development of a distributed simulation algorithm is presented in several stages. The method and the tool are applied to different real world applications and compared with SDL and PACE, another high-level Petri net tool.