

Formale Analyse des Zeitverhaltens Netzbasierter Automatisierungssysteme

Dipl.-Ing. Jürgen Andreas Greifeneder
geb. in Schwäbisch Hall

Vom Fachbereich Elektrotechnik und Informationstechnik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

genehmigte Dissertation

Eingereicht am: 19. September 2007
Tag der mündlichen Prüfung: 02. November 2007
Dekan des Fachbereichs: Prof. Dr.-Ing. Steven Liu

Promotionskommission
Vorsitzender: Prof. Dr. techn. Gerhard Fohler
Berichterstattende: Jun. Prof. Dr.-Ing. Georg Frey
Prof. Dr.-Ing. Birgit Vogel-Heuser

Berichte aus der Automatisierungstechnik

Jürgen Greifeneder

**Formale Analyse des Zeitverhaltens
Netzbasierter Automatisierungssysteme**

D 386 (Diss. Technische Universität Kaiserslautern)

Shaker Verlag
Aachen 2007

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Kaiserslautern, TU, Diss., 2007

Copyright Shaker Verlag 2007

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 978-3-8322-6835-0

ISSN 0945-4659

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • E-Mail: info@shaker.de

Kurzfassung

Die Architekturen vieler technischer Systeme sind derzeit im Umbruch. Der fortschreitende Einsatz von Netzwerken aus intelligenten rechnenden Knoten führt zu neuen Anforderungen an den Entwurf und die Analyse der resultierenden Systeme. Dabei spielt die Analyse des Zeitverhaltens mit seinen Bezügen zu Sicherheit und Performanz eine zentrale Rolle. Netzbasierte Automatisierungssysteme (NAS) unterscheiden sich hierbei von anderen verteilten Echtzeitsystemen durch ihr zyklisches Komponentenverhalten. Das aus der asynchronen Verknüpfung entstehende Gesamtverhalten ist mit klassischen Methoden kaum analysierbar. Zur Analyse von NAS wird deshalb der Einsatz der wahrscheinlichkeitsbasierten Modellverifikation (PMC) vorgeschlagen. PMC erlaubt detaillierte, quantitative Aussagen über das Systemverhalten. Für die dazu notwendige Modellierung des Systems auf Basis wahrscheinlichkeitsbasierter, zeitbewerteter Automaten wird die Beschreibungssprache DesLaNAS eingeführt. Exemplarisch werden der Einfluss verschiedener Komponenten und Verhaltensmodi auf die Antwortzeit eines NAS untersucht und die Ergebnisse mittels Labormessungen validiert.

Currently the architectures of many technical systems are undergoing considerable changes. The increasing use of networks connecting intelligent processor nodes leads to new requirements on the design and the analysis of the resulting systems. In this process, the analysis of temporal behavior with regards to safety and performance plays a central role. Networked Automation Systems (NAS) differ from other distributed real-time systems due to the cyclic behavior of their components. The overall behavior arising from the asynchronous composition of these components is hardly analyzable with traditional methods. Therefore, the use of Probabilistic Model Checking (PMC) is proposed for the analysis of NAS. PMC allows detailed quantitative statements about the overall system behavior. For the modeling task, which is based on the use of probabilistic timed automata, the description language DesLaNAS is introduced. As a case study, the influence of different components and behavior modes on the response time of a typical NAS is analyzed. The results are validated by measured values.

Meinen Eltern Helmut und Ingrid Greifeneder
in Würdigung der mir durch sie erschaffenen
Chance, dieses Bildungsniveau zu erreichen.

Wenn Du ein Schiff bauen willst, so trommle nicht Männer
zusammen, um Holz zu beschaffen, Werkzeuge vorzuberei-
ten, Aufgaben zu vergeben und die Arbeit einzuteilen, son-
dern lehre sie die Sehnsucht nach dem weiten endlosen Meer.

Antoine de Saint-Exupéry (zugeschrieben, Quelle unklar)

Danksagung

Wenn der Wanderer den Gipfel erreicht, erwartet ihn ein Gefühl der Freiheit und mit etwas Glück eine grandiose Aussicht. Zeit für ein Berg heil, Zeit, tief durchzuatmen, Zeit, zu danken. Jeder war in seiner Art wichtig und verdiente es, erwähnt zu sein. Doch möchte ich mich, stellvertretend für alle ungenannten, auf wenige beschränken.

Es waren François und Ursula Cellier, die mich zur Promotion ermutigten und stets nach meinen Fortschritten fragten. Es waren meine Eltern und Geschwister, auf deren Unterstützung ich jederzeit uneingeschränkt zählen konnte. Und es waren meine Freunde, deren wichtigste Aufgabe darin bestand, da zu sein. Auch waren da jene, die mir auf Konferenzen zuhörten und Anregung und Motivation gaben. Und Elke, Florian, Helmut, Kerstin, Matthias, Stephanie und Thomas, die mir beim Korrigieren halfen.

Diese Dissertation schreiben zu dürfen war eine Herausforderung, aber auch ein Privileg, für dessen Finanzierung ich der Stiftung der Deutschen Wirtschaft (sdw), meinen Eltern und der Technischen Universität Kaiserslautern danken möchte.

Danken möchte ich auch jenen, mit denen ich im Rahmen verschiedenster Aktivitäten einen Ausgleich zur Forschungsarbeit finden durfte. Danken möchte ich den Entwicklern der Software PRISM, die sich viel Zeit für Diskussionen nahmen, sowie den Forscherteams des LURPA der ENS Cachan (F) und des Departamento de Engenharia Elétrica der Universidade de Brasília (BR) für deren Gastfreundschaft. Danken möchte ich aber auch der kompletten Kaiserslauterer Arbeitsgruppe, in deren Mitte nicht nur die Arbeit Spaß machte, sondern ich auch viele schöne Ausflüge und andere Aktivitäten erleben durfte.

Frau Prof. Dr.-Ing. Birgit Vogel-Heuser und Herrn Jun. Prof. Dr.-Ing. Georg Frey möchte ich für das Interesse an meiner Arbeit und all die Zeit und Mühe, die sie in die Begutachtung investiert haben, danken. Gleiches gilt für den Vorsitzenden der Promotionskommission, Herrn Prof. Dr. techn. Gerhard Fohler.

Schlussendlich gilt mein Dank meinem Doktorvater Georg Frey für die wissenschaftliche und menschliche Begleitung meines akademischen Weges.

Inhaltsverzeichnis

Kurzfassung	
Vorwort / Danksagungen	v
1 Einleitung	1
2 Netzbasierte Automatisierungssysteme (NAS)	5
2.1 Verlässlichkeit und Qualität	7
2.2 Antwortzeitanalyse	9
2.3 Anforderungen an die Analysemethodik	12
2.4 Antwortzeitanalysemethoden	13
3 Probabilistic Model Checking (PMC)	21
3.1 Kurze Einführung in PRISM	24
3.1.1 PRISM-Programmiersprache	25
3.1.2 Formulierung der Eigenschaften in PCTL	26
3.2 PMC-Ablauf	29
3.2.1 Entwurfsprozess	29
3.2.2 Terminierungsnotwendigkeit	30
3.2.3 Ermittlung des Anfangszustands	33
3.3 Mathematische Grundlagen	35
3.3.1 Pfadwahrscheinlichkeiten und Kosten in DTMC	35
3.3.2 <code>Until</code> -Operator	37

4	Problem des Initialzustands	41
4.1	Repetitive Prozesse	41
4.2	Verkopplung mehrerer repetitiver Prozesse	44
4.3	Signal-Tracking (Signalbeobachtung)	46
4.4	Modellierung des Ereigniseintritts	48
4.4.1	Nicht-repetitive Prozesse mit stochastischer Durchlaufzeit	49
4.4.2	Zugriffskonflikte	52
4.4.3	Informationsverlust	53
4.5	Fazit	54
4.6	Implementierungsmöglichkeiten in PRISM	54
4.6.1	Einschrittwertzuweisung	55
4.6.2	Serielle Wertzuweisung	56
5	Modellierungsansatz	59
5.1	Beschreibungssprache DesLaNAS	60
5.2	Klassifizierung	65
5.3	Zeitkontinuierlicher Automat	69
5.4	Zeitdiskreter Automat	76
5.5	Diskretisierung	82
5.5.1	Prozessaggregation	82
5.5.2	Zeitschrittweite	84
5.5.3	Schrittweiten-Modell-Interdependenz	85
5.5.4	Übergang vom kontinuierlichen zum diskreten Automaten	85
5.6	Transformation nach PRISM	89
5.7	Multischrittweitensteuerung	91

6 Anwendungsbeispiel	95
6.1 Analyse des Komponentenverhaltens	95
6.1.1 Grundmodule	96
6.1.2 Antwortzeitanalyse	98
6.1.3 Relative Anteile der Verhaltenseigenschaften	100
6.2 Stochastische Übergangszeiten	101
6.2.1 Variable Netzlaufzeit	101
6.2.2 Variabler SPS-Zyklus	103
6.3 Stochastische und parallele Funktionsweisen	104
6.3.1 Fehler	104
6.3.2 Zugriffskonflikte	108
6.4 Weiterführende Anwendungsmöglichkeiten	111
6.4.1 Beispiel zur Konfigurationsanalyse	112
6.4.2 Beispiel zur Komponentenanforderungsanalyse	114
6.5 Vergleich mit Messungen	115
7 Zusammenfassung und Ausblick	117

Verzeichnisse

Definitionen und Begriffe	119
Symbole	121
Abkürzungen	123
Tabellen	125
Abbildungen	127
Literatur	131
Normen	141