

Verification and Validation of Logic Control Algorithms by Model Checking

Vom Fachbereich Elektrotechnik und Informationstechnik
der Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Ingenieurwissenschaften (Dr.-Ing.)
genehmigte Dissertation

von
M.Sc. Xiyang Weng

D 386

Eingereicht am:	27. November 2002
Tag der mündlichen Prüfung:	23. Mai 2003
Dekan des Fachbereichs:	Prof. Dr.-Ing. G. Huth
Promotionskommission:	
Vorsitzender:	Prof. Dr.-Ing. W. Kunz
Berichterstattende:	Prof. Dr.-Ing. habil. L. Litz Prof. Dr.-Ing. J. Lunze

Berichte aus der Automatisierungstechnik

Xiying Weng

**Verification and Validation
of Logic Control Algorithms
by Model Checking**

Verifikation und Validierung
von Steuerungsalgorithmen
mittels Model Checking

D 386 (Diss. Universität Kaiserslautern)

Shaker Verlag
Aachen 2003

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at <http://dnb.ddb.de>.

Zugl.: Kaiserslautern, Univ., Diss., 2003

Copyright Shaker Verlag 2003

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 3-8322-2242-1

ISSN 0945-4659

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen

Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9

Internet: www.shaker.de • eMail: info@shaker.de

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als Doktorandin bei Herrn Prof. Dr.-Ing. habil. L. Litz am Lehrstuhl für Automatisierungstechnik, Fachbereich Elektrotechnik und Informationstechnik, an der Universität Kaiserslautern. Ich möchte mich ganz herzlich bei allen Kollegen am Lehrstuhl für die angenehme Zusammenarbeit bedanken.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. habil. L. Litz für die Anregung und Betreuung meiner Arbeit. Seine stetige Unterstützung und Förderung, ergänzt durch zahlreiche Hinweise und Ratschläge, haben entscheidend zum Gelingen dieser Arbeit beigetragen. Vor allem bin ich ihm für seine sehr freundliche und hilfsbereite Art herzlich dankbar.

Herrn Prof. Dr.-Ing. J. Lunze danke ich für das Interesse an meiner Arbeit und für die Übernahme des Korreferats. Ebenso danke ich dem Vorsitzenden der Promotionskommission, Herrn Prof. Dr.-Ing. W. Kunz.

Mein Dank gilt auch der Hanns-Seidel Stiftung für die zweijährige finanzielle Unterstützung dieser Arbeit.

Schließlich danke ich in besonderer Weise meiner Familie, die mich stets darin unterstützt hat, meine Ziele zu erreichen.

Eschborn, im August 2003

Xiying Weng

Contents

1	Introduction	1
1.1	Demand on formal methods for developing logic control software.....	1
1.1.1	Conventional implementation-oriented approach.....	1
1.1.2	Formal approach for developing logic control software	2
1.2	Thesis objectives and important contributions	3
1.3	Organization and contents of the thesis.....	6
2	Formal Specification for logic control design: SIPN.....	8
2.1	Introductory remarks	8
2.2	Interpreted Petri net based framework: SIPN	10
2.3	Formal properties of an SIPN specification.....	15
2.3.1	Basic properties of an SIPN design	15
2.3.2	Specific properties of an SIPN design.....	17
2.4	Graph based analysis and verification of SIPN	22
3	Temporal logic model checking approach to software verification	25
3.1	Introductory remarks	25
3.2	Temporal logic	26
3.3	Brief description of TL model checking methodology	30
3.3.1	Explicit model checking.....	30
3.3.2	Symbolic model checking.....	32
3.3.2.1	Boolean representation of a finite state system.....	32
3.3.2.2	OBDD manipulation of Boolean functions.....	32
3.3.2.3	Fixpoint characterization of CTL operators.....	34
3.3.3	The model checking tool SMV	38
3.4	Symbolic encoding of SIPN.....	39
4	The realization of model checking of an SIPN design.....	47
4.1	Introductory remarks	47
4.2	General approach to the verification of an SIPN design using model checking.....	47
4.3	Modeling the dynamic behavior of an SIPN design	49
4.3.1	Modeling of SIPN elements	49
4.3.2	Modeling with stability check	56
4.3.3	Modeling of time	58
4.3.4	Modeling of hierarchical structures.....	59
4.3.5	Summary.....	60

4.4	Correctness criteria for an SIPN design	61
4.4.1	From informal to formal requirement specification	61
4.4.2	Temporal logic specification of the correctness criteria	63
4.5	Process model for the verification purpose	68
4.5.1	Verification with process model.....	68
4.5.2	Modeling process behavior using temporal logic forms	70
4.5.3	Modular modeling of the uncontrolled process	70
4.5.4	PIPN process model for verification	72
4.6	Discussion	72
5	Towards generating a correct implementation	73
5.1	Introduction	73
5.2	The problem of the current implementation method	73
5.3	A new implementation algorithm.....	76
6	Experiments on complex applications	83
6.1	Introduction	83
6.2	Air compressor control system.....	83
6.2.1	Verification of design 1 without applying a process model	85
6.2.2	Verification of design 1 with process model	96
6.2.3	The verification of design 2	99
6.3	A flexible manufacturing line	101
6.4	A turning-plate	113
6.5	Discussion	124
7	Concluding remarks and future research	125
7.1	Summary and conclusions	125
7.2	Suggestions for future research.....	126
7.3	Kurzfassung in deutscher Sprache	127
	List of often used symbols and abbreviations	132
	Reference.....	135