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

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

Die vorliegende Arbeit beschäftigt sich mit dem Einsatz formaler Methoden bei der Entwicklung von Steuerungsalgorithmen. Im Vergleich zu einer direkten Kodierung ermöglicht die Anwendung formaler Ansätze eine frühere Erkennung von Fehlern innerhalb des Enwicklungszyklus. Im Entwicklungsprozess werden zwei Teilschritte getrennt voneinander betrachtet: zum einen die Verifikation und Validierung, zum anderen die Implementierung..

Basierend auf dem formalen Ansatz Signal Interpretiertes Petri Netz (SIPN) wird eine systematische Methode entwickelt, um eine automatische Verifikation und Validierung zu ermöglichen. Das SIPN wird hierfür mit booleschen Funktionen kodiert. Zusammen mit den zu überprüfenden Anforderungen, die mittels temporaler Logik formuliert werden, entsteht ein Gesamtsystem von booleschen Funktionen, das mit einem Model Checking Tool, in dieser Arbeit SMV, ausgewertet wird. Diese Auswertung liefert eine Aussage, ob die jeweiligen Anforderungen erfüllt sind, und erzeugt gegebenenfalls ein Counterexample, falls dies nicht der Fall ist. Als Erweiterung wird untersucht, wie sich Prozessmodelle von unterschiedlichem Detailierungsgrad in den Verifikationsprozess integrieren lassen.

Große Bedeutung bei der Verifikation und Validierung hat die korrekte Spezifikation der Anforderungen. In der Arbeit wird argumentiert, dass bei einem korrekten Steuerungsalgorithmus zwei Aspekte berücksichtigt werden müssen: die Korrektheit des Formalismus und die Korrektheit der zu realisierenden Funktionalität. In der Arbeit werden die wichtigsten Kriterien vorgestellt.

Als zweiter Teilschritt bei der Entwicklung eines Steuerungsalgorithmus wird die Implementierung betrachtet. Um einen korrekten Steuerungsalgorithmus zu erhalten, muss neben der Korrektheit des Designs auch die Korrektheit der Implementierung, also der Umsetzung des Designs in den Code, sichergestellt werden. Hierzu wird ein verbesserter automatischer Kodierungsalgorithmus vorgeschlagen. Damit ist es möglich, einen Steuerungsalgorithmus, der als SIPN vorliegt, automatisch in eine der standardisierten Programmiersprachen in IEC 1131 umzusetzen.