



Research Report Series

Lehrstuhl für Rechnertechnik und
Rechnerorganisation (LRR-TUM)
Technische Universität München

<http://www.bode.in.tum.de/>

Editor: Prof. Dr. A. Bode

Vol. 28

Quantitative Bewertung hochverfügbarer Systeme

Max Walter

SHAKER
VERLAG

Aachen 2003

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Walter, Max:

Quantitative Bewertung hochverfügbarer Systeme/Max Walter.

Aachen: Shaker, 2003

(Research Report Series/Lehrstuhl für Rechnertechnik und Rechnerorganisation (LRR-TUM), Technische Universität München; Vol. 28)

Zugl.: München, Techn. Univ., Diss., 2002

ISBN 3-8322-1176-4

Copyright Shaker Verlag 2003

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

Printed in Germany.

ISBN 3-8322-1176-4

ISSN 1432-0169

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

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

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

Kurzfassung

Mit der zunehmenden Kommerzialisierung des Internets kommt der Zuverlässigkeit der dort eingesetzten Rechner eine immer größere Bedeutung zu. Zur Optimierung des Entwurfs kostengünstiger, hochverfügbarer Systeme werden stochastische Modelle herangezogen.

Aus der Literatur sind zwei Klassen von Modellierungsmethoden für hochverfügbare Systeme bekannt. *Boolesche Methoden*, auch als *kombinatorische Methoden* bezeichnet, kommen im industriellen Umfeld am häufigsten zum Einsatz. Sie haben den Vorteil einer leichten Handhabbarkeit, können allerdings stochastische Abhängigkeiten zwischen dem Ausfall- und Reparaturverhalten der einzelnen Komponenten des Systems nicht berücksichtigen.

Gründe für diese stochastischen Abhängigkeiten können beispielsweise gemeinsame Fehlerquellen, Fehlerfortpflanzungen, überlastetes Reparaturpersonal, nicht-perfekte Fehlererkennungsmechanismen oder die Umschaltzeit zwischen dynamisch-redundanten Komponenten des Systems sein. Eine Vernachlässigung dieser Systemeigenschaften führt zu überoptimistischen Ergebnissen bei der Ermittlung der Zuverlässigkeit, weshalb die Verwendung Boolescher Methoden zu einer Unterschätzung der durch Ausfälle entstehenden Kosten führt.

Genauere Ergebnisse liefert die Verwendung sogenannter *Zustandsraum-basierter Methoden*, welche aber eine relativ hohe Einarbeitungszeit voraussetzen und zu schwer handhabbaren Modellen führen. *Zustandsraum-basierte Methoden* finden deshalb in der Praxis nur selten Anwendung.

Um die Vorteile beider Methoden zu vereinen, wird im Rahmen der vorliegenden Dissertation eine neuartige Methode vorgestellt, die die Erstellung von leicht handhabbaren Modellen erlaubt, ohne auf die relevanten stochastischen Abhängigkeiten zwischen den Komponenten verzichten zu müssen. Dies wird durch die Verwendung von zwei Modellen erreicht. Dem Modellierer des Systems steht eine Sammlung von leicht handhabbaren, aber auch sehr mächtigen Diagrammart und Tabellen zur Verfügung. Im Unterschied zu anderen Diagrammart kann dieses Eingabemodell jedoch nicht direkt ausgewertet werden, sondern wird mit Hilfe einer ebenfalls in dieser Arbeit vorgestellten Methode in ein semantisch äquivalentes Zustandsraum-basiertes Modell umgewandelt. Dieses zweite Modell kann anschließend unter Verwendung eines herkömmlichen Werkzeugs analysiert werden.

Die Arbeit enthält außerdem eine Beschreibung der Implementierung dieser Methode im Werkzeug OpenSESAME (Simple but Extensive Structured Availability Modeling Environment). Die praktische Anwendbarkeit des Werkzeugs wird anhand von zwei industriell relevanten Beispielen aufgezeigt. Das erste Beispiel enthält ein Modell eines typischen verteilten, hochverfügbaren Webservers. Als zweites Beispiel dient ein sogenannter *Adjunct Processor*, wie er im intelligenten Telefonnetz eingesetzt wird, um beispielsweise virtuelle Telefonnummern in physikalische Telefonnummern umzuwandeln.