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

http://wwwbode.in.tum.de/

Editor: Prof. Dr. A. Bode

Vol. 34

Application-oriented evaluation of fault-tolerant systems

Max Walter

SHAKER
VERLAG
Aachen 2009

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: München, Techn. Univ., Habil.-Schr., 2008

Printed in Germany.

ISBN 978-3-8322-8227-1
ISSN 1432-0169

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Max Walter: ***Application-oriented evaluation of fault-tolerant systems***

Abstract

In fault-tolerant systems, redundancy in terms of hardware, software, repeated computations, or additional information is used to increase dependability. As redundancy is costly and might influence performance in a negative way, stochastic dependability models are used for a quantitative assessment of attributes like reliability, safety, and availability.

The thesis first summarizes the existing modeling concepts for fault tolerant systems, namely combinational methods (e.g. fault trees and reliability block diagrams), state-based models (e.g. Markov chains, stochastic Petri nets, and models based on a stochastic process algebra), as well as hybrid methods, which combine different kind of modeling paradigms.

Furthermore, it describes a novel, application-oriented approach for the evaluation of fault-tolerant systems. In this approach, the system is modeled using a high-level, application specific input model, which is automatically transformed into a lower-level formal model. Using existing software packages, the formal model is in turn transformed into a mathematical model which can be analyzed numerically. The results of this evaluation are presented within the scope of the high-level input model, though.

The novel approach is able to calculate the overall system's dependability from information given on the components it is built of, including information on the components themselves (e.g. MTTF- and MTTR-values), information on which combination of component failures imply a system failure (i.e. the redundancy structure of the system), as well as information on inter-component dependencies like failures with a common cause, failure propagation, different kind of redundancy strategies, non-dedicated repairmen and so on.

After first describing the basic design principles, the thesis also describes four specific tools which have been implemented according to these principles. The Simple but Extensive, Structured Availability Modeling Environment (OpenSESAME) was developed for the evaluation of High-Availability systems, The Safety Modeling Environment (SafeME) is tailored towards safety-critical systems, Information Flow Diagrams (IFD) are used to model emergency shutdown systems, and The Copula-BAsed Reliability and Availability Modeling Environment (COBAREA) is intended for the analysis of fault-tolerant digital circuits.

In general, the evaluation of stochastic dependability models is very demanding in terms of CPU-time and memory. To alleviate this problem, the thesis also presents a novel divide-and-conquer algorithm allowing to divide large dependability models into independent parts which can be analyzed separately. The algorithm was applied in the tools mentioned above, but could be reused in similar evaluation approaches, as well.