RESPONSIVE COMPUTER SYSTEMS: STEPS TOWARD FAULT-TOLERANT REAL-TIME SYSTEMS

THE KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE

REAL-TIME SYSTEMS

Consulting Editor
John A. Stankovic

IMPRECISE AND APPROXIMATE COMPUTATION, by Swaminathan Natarajan, ISBN: 0-7923-9579-4
FOUNDATIONS OF DEPENDABLE COMPUTING: *System Implementation*, edited by Gary M. Koob and Clifford G. Lau, ISBN: 0-7923-9486-0
FOUNDATIONS OF DEPENDABLE COMPUTING: *Paradigms for Dependable Applications*, edited by Gary M. Koob and Clifford G. Lau, ISBN: 0-7923-9485-2
FOUNDATIONS OF DEPENDABLE COMPUTING: *Models and Frameworks for Dependable Systems*, edited by Gary M. Koob and Clifford G. Lau, ISBN: 0-7923-9484-4
THE TESTABILITY OF DISTRIBUTED REAL-TIME SYSTEMS, Werner Schütz; ISBN: 0-7923-9386-4
A PRACTITIONER'S HANDBOOK FOR REAL-TIME ANALYSIS: *Guide to Rate Monotonic Analysis for Real-Time Systems,* Carnegie Mellon University (Mark Klein, Thomas Ralya, Bill Pollak, Ray Obenza, Michale González Harbour); ISBN: 0-7923-9361-9
FORMAL TECHNIQUES IN REAL-TIME FAULT-TOLERANT SYSTEMS, J. Vytopil; ISBN: 0-7923-9332-5
SYNCHRONOUS PROGRAMMING OF REACTIVE SYSTEMS, N. Halbwachs; ISBN: 0-7923-9311-2
REAL-TIME SYSTEMS ENGINEERING AND APPLICATIONS, M. Schiebe, S. Pferrer; ISBN: 0-7923-9196-9
SYNCHRONIZATION IN REAL-TIME SYSTEMS: *A Priority Inheritance Approach,* R. Rajkumar; ISBN: 0-7923-9211-6
CONSTRUCTING PREDICTABLE REAL TIME SYSTEMS, W. A. Halang, A. D. Stoyenko; ISBN: 0-7923-9202-7
FOUNDATIONS OF REAL-TIME COMPUTING: *Formal Specifications and Methods,* A. M. van Tilborg, G. M. Koob; ISBN: 0-7923-9167-5
FOUNDATIONS OF REAL-TIME COMPUTING: *Scheduling and Resource Management,* A. M. van Tilborg, G. M. Koob; ISBN: 0-7923-9166-7
REAL-TIME UNIX SYSTEMS: *Design and Application Guide,* B. Furht, D. Grostick, D. Gluch, G. Rabbat, J. Parker, M. McRoberts, ISBN: 0-7923-9099-7

RESPONSIVE COMPUTER SYSTEMS: STEPS TOWARD FAULT-TOLERANT REAL-TIME SYSTEMS

edited by

Donald S. Fussell

The University of Texas at Austin
Austin, Texas, USA

Miroslaw Malek

Humboldt-Universität
Berlin, Germany

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

ISBN 978-0-7923-9563-8 ISBN 978-1-4615-2271-3 (eBook)
DOI 10.1007/978-1-4615-2271-3

Printed on acid-free paper.

CONTENTS

LIST OF FIGURES

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

LIST OF TABLES

Chapter 12

PREFACE

Modern computer systems are rapidly evolving into a highly integrated global network which serves as the repository of ever larger amounts of information critical to the social infrastructure. At the same time, a increasing fraction of the general public is becoming familiar with, and dependent upon, computers in the home. As this evolution continues, there is a growing need for computing environments that can be relied upon to provide timely responses to demands for information and service.

For some time now, a great deal of attention has been paid to the design of fault-tolerant computers for special, mission-critical applications. In parallel, much research has been devoted to methods for designing real-time systems, which again are usually intended for specialized applications. While some of these applications demand highly reliable real-time service guarantees, for the most part research on the design of real-time computer systems and fault-tolerant computers has progressed independently. However, with increasing societal dependence on computers for everyday operation, the integration of fault-tolerance and real-time capabilities into new generations of computer systems has become a significantly more important issue in systems design. We believe that the time has come for the development of a discipline of *responsive systems* design, by which we mean the design of systems optimized to meet demands for reliable and timely service.

While many approaches to the design of reliable systems have been developed, all of them share one characteristic in common — they rely on replication of resources in some way to achieve high reliability. Thus, the advent of widespread parallel and distributed computing has been greeted as the basis of a new generation of computing systems which use redundancy to achieve high reliability. To date, however, the reality in most parallel and distributed systems has been quite the reverse of this hope. The typical user of a distributed client-server environment actually experiences less reliable service than was provided by a time-shared mainframe or minicomputer in previous years. This is because each user of such a system typically relies on a reasonably large number of individual computers for his overall service needs. In many current environments, the failure of any one of these machines brings down the user's environment. While each machine may be more robust than its counterparts of previous generations, with overall system designs which ignore fault-tolerance, the probability that the user sees a functional system declines exponentially with the number of machines on which he is dependent.

A similar situation exists with respect to the use of parallelism in the design of high-performance machines to meet severe real-time constraints. A parallel system may in principle be able to provide a performance level necessary to the achievement of a real-time constraint beyond the performance limits of any sequential system. Since parallel systems are significantly more complex and harder to program than sequential systems, however, it is harder to realize their performance potential in practice. Moreover, there is a significantly greater opportunity for asynchronous, non-deterministic, or other unpredictable behavior in parallel or distributed computing systems, which makes it much harder to guarantee that a real-time constraint will always be met.

Thus we have the situation at present that, while the technology of parallel and distributed computing contains within it precisely the raw material needed for the design of responsive systems, it is most often the case in current system designs that responsiveness is actually harder to achieve than in sequential systems in spite of this potential. It is a significant challenge to convert the potential of modern, parallel and distributed computing environments into realized responsive computing systems. Developing a discipline of responsive systems design will require integrating the theory and practice of real-time systems, fault-tolerant computing, and parallel and distributed processing into a whole which is more than the sum of its parts.

In order to take the first steps in this direction, we must begin with a clearer understanding of the goal and the costs of achieving it. Much of the reason that current distributed systems for non-critical applications are so unreliable is that they have been designed to maximize raw benchmark speeds while minimizing the cost of storage and processing power. Thus, disks are not used to hold replicated copies of data; processors are not employed to back up the functions of others. The cost to the user of downtime is not usually considered in the design of these systems; hence efforts to minimize costs can adversely affect reliability. Any use of redundancy that might entail performance costs is considered harmful using this metric. Thus, if we are to undertake a discipline of responsive systems design, we must begin by recognizing the value of system availability and finding a way to measure it against the values of other system capabilities such as performance level and storage capacity.

We must in the same vein modify our notion of how to evaluate performance. Raw benchmark speed must be deemphasized and replaced with a valuation based on the expectation of the timeliness of the responses that a system will typically provide to its users. System resources beyond those required to provide timely responses should preferentially be used for greater system reliability or availability then for increasing raw performance as is typically the case today. Overall, then, we need a measure of system value in terms of responsiveness that lets us make design decisions regarding how system resources are to be used to provide the highest level of responsiveness at a given cost level, or alternatively the lowest cost for a given level of responsiveness. We then need to develop methodologies for designing systems and algorithms that will allow us to satisfy reliability and timeliness requirements in a flexible and efficient way.

Given the complexity of modern computing systems and the ambitious goals of responsive systems design, a wide variety of issues will need to be resolved before these goals can be achieved. For example, how can we meet high level specifications with respect to fault tolerance and timeliness, or, in fact, how do we even specify these requirements? How do we express and estimate bounds on computation time? What models should be used to desribe the system? What methods should be used to prove that a design or an implementation meet a responsiveness specification? What language, operating system and architecture paradigms would be most appropriate? How do we design algorithms and programs that behave responsively?

In the present volume, which contains twelve papers selected from the Second International Workshop on Responsive Computer Systems that took place in Lincoln, New Hampshire on September 28-30, 1993, you will find some initial steps toward answering these and related questions.

Donald S. Fussell
Miroslaw Malek