Ravishankar K. Iyer | Zbigniew T. Kalbarczyk
Nithin M. Nakka

Dependable Computing

Design and Assessment

with website

IEEE Press

IEEE computer society

WILEY

Dependable Computing

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

About IEEE Computer Society

IEEE Computer Society is the world's leading computing membership organization and the trusted information and career-development source for a global workforce of technology leaders including: professors, researchers, software engineers, IT professionals, employers, and students. The unmatched source for technology information, inspiration, and collaboration, the IEEE Computer Society is the source that computing professionals trust to provide high-quality, stage-of-the-art information on an on-demand basis. The Computer Society provides a wide range of forums for top minds to come together, including technical conferences, publication, and a comprehensive digital library, unique training webinars, professional training, and the Tech Leader Training Partner Program to help organizations increase their staff's technical knowledge and expertise, as well as the personalized information tool my Computer. To find out more about the community for technology leaders, visit http://www.computer.org.

IEEE/Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press authored book program to produce a number of exciting new titles in areas of computer science, computing, and networking with a special focus on software engineering. IEEE Computer Society members receive a 35% discount on Wiley titles by using their member discount code. Please contact IEEE Press for details.

To submit questions about the program or send proposals, please contact Mary Hatcher, Editor, Wiley-IEEE Press: Email: mhatcher@wiley.com, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774.

Dependable Computing

Design and Assessment

Ravishankar K. Iyer
Department of Electrical and Computer Engineering and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois, USA

Zbigniew T. Kalbarczyk
Department of Electrical and Computer Engineering and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois, USA

Nithin M. Nakka
Cisco Networking Engineering group
Cisco Systems, Inc.
San Jose, California, USA

IEEE computer society

IEEE Press

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data for:

Hardback ISBN: 9781118709443

Cover Design: Wiley
Cover Image: © Yuichiro Chino/Getty Images

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

This book is dedicated to my wife Pamela for her unwavering support and encouragement in my academic pursuits, from my PhD to the present day.
– For Ravishankar K. Iyer

This book is dedicated to my wife, whose unfailing support kept me moving forward to the completion of this work.
– For Zbigniew T. Kalbarczyk

This book is dedicated to my parents, whose sacrifices have shaped what I am.
– For Nithin M. Nakka

Contents

About the Authors

Professor Ravishankar K. Iyer is George and Ann Fisher Distinguished Professor of Engineering at the University of Illinois Urbana-Champaign. He holds joint appointments in the Departments of Electrical and Computer Engineering (ECE) and Computer Science, the Coordinated Science Laboratory (CSL), the National Center for Supercomputing Applications (NCSA), the Carle Illinois College of Medicine, and the Carl R. Woese Institute for Genomic Biology. He is also a faculty Research Affiliate at the Mayo Clinic. Professor Iyer was the founding Chief Scientist of the Information Trust Institute at UIUC – a campus-wide research center addressing security, reliability, and safety issues in critical infrastructures. He leads the DEPEND Group at CSL/ECE at Illinois, with a multidisciplinary focus on systems and software that combine deep measurement-driven analytics and machine learning with applications in two important domains: (i) management and control of large infrastructures including autonomous systems that span resilience, safety, and security and performance and (ii) health and personalized medicine that spans computational genomics and health analytics focused on neurological disorders, pharmacogenomics, and predicting cancer metastases. His group has developed a rich AI analytics framework that has been deployed on real-world applications in collaboration with industry, health providers, and government agencies including the National Science Foundation, the National Institutes of Health, the Department of Energy, the Defense Advanced Research Projects Agency, and the Department of Defense.

Professor Iyer is a Fellow of the American Association for the Advancement of Science (AAAS), the Institute of Electrical and Electronics Engineers (IEEE), and the Association for Computing Machinery (ACM). He has received several awards, including the Jean-Claude Laprie Award, IEEE Emanuel R. Piore Award, and the 2011 Outstanding Contributions Award by the Association of Computing Machinery. Professor Iyer is also the recipient of the degree of Doctor Honoris Causa from Toulouse Sabatier University in France.

Dr. Zbigniew T. Kalbarczyk is Research Professor at the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory of the UIUC. Dr. Kalbarczyk's research interests are in the design and validation of reliable and secure computing systems. His current work explores: (i) emerging computing technologies, such as resource virtualization to provide redundancy and assure system resiliency to accidental errors and malicious attacks; (ii) machine learning-based methods for early detection of security attacks, including defense against smart malware; (ii) analysis of data on failures and security attacks in large computing systems to characterize system resiliency and guide development of methods for rapid diagnosis and runtime detection of problems; and (iv) development of techniques for automated validation and benchmarking of dependable and secure computing systems using formal (e.g., model checking) and experimental methods (e.g., fault/attack injection). Dr. Kalbarczyk led the design and commercialization of (i) ARMOR high-availability software middleware to support resilient distributed applications and (ii) NFTAPE software framework to support fault injection-based resiliency assessment. He served as a program chair of Dependable Computing and Communication Symposium (DCCS), a track of the International Conference on Dependable Systems and Networks (DSN) 2007, and Program Co-Chair of Computer Performance and Dependability Symposium, a track of the DSN 2002. He was Associate Editor of IEEE Transactions on Dependable and Secure Computing. He has published over 230 technical papers and is regularly invited to give tutorials and lectures on issues related to the design and assessment of complex computing systems. He is a member of the IEEE, the IEEE Computer Society, and IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance.

Dr. Nithin M. Nakka received his BTech (hons.) degree from the Indian Institute of Technology, Kharagpur and his MS and PhD degrees at the University of Illinois at UIUC. Currently, he is Technical Leader at Cisco Systems. While at Cisco, he has worked on most layers of the networking software stack, from network data-plane hardware, control plane at Layer-2 and Layer-3, network controllers, up to and including network fabric monitoring. This along with doing what he enjoys – sharing his expertise through mentoring many incoming employees. He has been leading the development of solutions for network day-2 operations to monitor fabrics and analyze, understand, troubleshoot network issues, and possibly predict impending network failures. His innovative approximation heuristics in Algorithms for Memory Array Redundancy Analysis during his work at Nextest Systems Corporation brought the company to world-class excellence in this niche computational problem domain, generally known to be NP-complete. He also worked for Motorola's mobile devices group, on pioneering efforts in Bluetooth stereo audio transmission (A2DP) and Bluetooth security. His areas of research interest include systems reliability, network telemetry, and hardware implemented fault tolerance. Dr. Nakka has previously held positions as a research faculty in UIUC, and Northwestern University in Evanston, Illinois, and contributed to the area of dependability in high-performance computing systems.

Preface

Dependability of systems has transitioned over the years from a feature to a necessity for end users, and from an add-on to a core design principle for those who are designing and implementing computing or computer-based systems. The need for dependability has grown not just in its breadth in terms of the areas where it is applicable but also in depth. Given any one of the many systems where dependability techniques are applied, their relevance is seen in every layer of the system stack. The aim of this book is to help readers navigate through the evolution of dependability, from taxonomy, mathematical concepts, and fundamental theory to design, implementation, validation, deployment, measurement, and monitoring. Finally, the book brings its audience right up to the modernity of the field by looking at critical societal applications such as autonomous vehicles, large-scale clouds, and engineering solutions for healthcare, illustrating the emerging challenges faced in making artificial intelligence (AI) and its applications dependable and trustworthy.

Sections of the book are intensely pedantic and technical. However, with the support of practical case studies and use cases from both academia and real-world deployments, we have attempted to guide our audience through their journey in fathoming the developments in this ever-growing field. For a beginner, a systematic study from the beginning will help in building strong foundations, but we encourage all readers to whet their appetite with any of the case studies that spark their interest. For seasoned designers and academicians in the area, we attempt to provide a near-current reference for dependability research and development.

The prerequisites for the content of this book are a basic understanding of statistical concepts, computer systems and organization, and, preferably, a course on distributed systems. Above all, a keen interest in delving into this exciting field to unravel and possibly discover new techniques will maintain a reader's enthusiasm, as it has done ours over the past years. Certainly, well-written texts are already available in this area. However, the authors felt that we lacked a single compendium spanning the myriad areas in which dependability has been applied, providing theoretical concepts and applied knowledge with content that would excite a beginner yet rigor that would satisfy an expert. That feeling led us to embark on the long journey of bringing forth this book.

Chapters 1 and 2 describe dependability taxonomy and briefly compare and contrast classical techniques with their modern counterparts or extensions. Chapters 3–7 help the readers walk up the system stack, from the hardware logic via operating systems up to software applications, with respect to how those layers are hardened for dependability. Chapters 8–12 expand into the domain of distributed systems to explore the techniques and applications therein. Those chapters also delve a great deal into a measurement-based understanding of the systems being studied, an aspect that the authors feel honored to have had the opportunity to significantly contribute. Chapter 13 focuses on the most recent and upcoming trends that are shaping developments in dependability. Finally, looking into the future, Chapter 14 delves deeper into the novel challenges that are being faced in making AI systems dependable and trustworthy.

In summary, with the support of practical case studies and use cases from both academia and real-world deployments, we guide our audience through a journey of developments, including the impact of AI and machine learning on this ever-growing field.

Acknowledgments

In writing this book, we were inspired by Professor Dan Siewiorek's groundbreaking research and the unmatched book *The Theory and Practice of Reliable System Design* by Siewiorek and Swarz, now in its third edition, as well as the foundational work of Professors Ed McCluskey and Al Avižienis, which continues to impact the field today.

We are indebted to many of our current and former students, postdoctoral associates, and academic and industry colleagues whose research contributed in important ways to material in this book, including Karthik Pattabiraman, Lelio DiMartino, Bob Horst, Saurabh Bagchi, Homa Alemzadeh, Long Wang, Tim Tsai, Saurabh Jha, Phuong Cao, Keywhan Chung, Shengkun Cui, and Archit Patke. Some of our colleagues have also adopted a draft version of this book in teaching dependability courses to graduate and senior students in their respective institutions, which has bolstered our confidence in the usefulness of this content. The administrative and technical proofreading staff members, including, Carol Bosley, Heidi Leerkamp, Jenny Applequist, and Kathleen Atchley, have contributed immensely to this effort by their critical linguistic polish of this technical content and also by their logistical work in keeping the authors and publishers in synchrony to accomplish this massive task. We are grateful to all of them as well as many others who shared their insights.

Special thanks to our colleagues at the University of Illinois Urbana-Champaign who provided a rich, supportive environment that allowed us to pursue this project.

The research presented in this book was supported by numerous funding agencies and industry partners, including NSF, NIH, NASA, DoD, DARPA, DOE, IBM, Sandia National Lab, Nvidia, the Mayo Clinic, Infosys, and Xilinx.

Apart from the immense technical support we have received, we are very grateful to our families, who have been ever so patient in supporting us. They have transformed their "Are we there yet?" to "Looks like we are getting close" to keep our enthusiasm alive on an emotional front while we gave all we could to tame this mammoth. In spite of all the support that we have received both professionally and personally, added to our over 100 years of combined experience in this area, we feel that our attempts to gather all that we could in this ever-expanding and interesting field may have fallen short in some application domains, not given enough justice to some, or even at times made unintentional errors in comprehending and explaining the content. A significant portion of our time was spent in making sure that we kept the content current and relevant for our audience. However, as the field is growing at the rate that it is, we had to reconcile ourselves to the hope that we may offer more in a future edition! We invite readers to send us their feedback on the content or any errors that may have escaped our scrutinous efforts to maintain relevance and correctness.