Guest Editorial for the Special Issue on the 2005 IEEE/IFIP Conference on Dependable Systems and Networks, including the Dependable Computing and Communications and Performance and Dependability Symposia

Jean Arlat, *Member*, *IEEE*, Andrea Bondavalli, *Member*, *IEEE*,
Boudewijn Haverkort, *Senior Member*, *IEEE*, and Paulo Veríssimo, *Senior Member*, *IEEE*

Now more than ever, dependable computing systems, along with secure networking and communication infrastructures, are essential to critical applications and services. This is due, in particular, to the emergence of very large-scale systems made up of myriads of ever-evolving and often mobile computerized devices with numerous and complex interactions and interdependencies. Moreover, the increasingly broad spectrum of threats—physical or human-made, accidental or malevolent—to these various layers and interfaces adds another difficult facet to the challenge.

The people in charge of designing intricate computing systems are concerned with developing and implementing resilient components, architectures, networks, protocols, software algorithms, and applications. In addition, topics related to the assessment of the properties achieved both during the development process and in operation are also critical. Verification (proving and testing) and evaluation, including analytical modeling, simulation, field measurements, and controlled experiments, are necessary for the successful exploitation and monitoring of these systems.

This special issue aims to serve researchers, designers, and implementers of dependable and secure systems and infrastructures. It includes a set of papers presented at the Dependable Computing and Communication Symposium (DCCS) and the Performance and Dependability Symposium (PDS) that were part of the sixth edition of the annual IEEE/IFIP Dependable Systems and Networks (DSN) Conference held in Yokohama, Japan, in 2005. The technical program of DSN-2005 included 77 regular papers covering a wide range of relevant issues and showing the depth and breadth of our community's research efforts. This collection was the result of the tough and thorough selection process that characterizes this conference in both symposia. For DCCS, from the 205 submissions, with contributions originating from 35 countries from all continents, 50 regular papers were accepted by the program committee based on a total of 846 reviews with an average of 4.13 reviews per paper. PDS received 94 submissions from 19 countries from all continents and 27 papers were accepted by the PC based on a total of 435 reviews with an average of 4.63 reviews per paper.

Two subcommittees were formed to select a small number of papers from each symposium to form this DSN special issue. We want to thank the members of these subcommittees, chaired by the guest editors: for DCCS, Christian Cachin, Farnam Jahanian, Carl Landwehr, Raimundo Macedo and Nirmal Saxena, and, for PDS, Nuno Neves, Aad van Moorsel, and Markus Siegle. Their dedication in carrying out this selection on a tight schedule was outstanding. Out of a total of 77 regular papers, six papers were selected from DCCS and three from PDS and the authors were invited to submit properly extended versions of their contributions. Each paper went through another two rounds of review by qualified experts, some of them already familiar with these papers because they had been reviewers for DSN and others specifically invited to perform this review. In the end, seven papers successfully went through this selection process and will be archived in *TDSC* as a sample of the excellent program of DSN-2005. These papers cover a broad subset of the symposia themes. They include contributions on architecting systems, devising procedures and protocols, modeling and measuring systems, covering hardware and software layers, and coping with threats ranging from accidental to malicious faults.

- *J. Arlat is with LAAS-CNRS, University of Toulouse, 7 Avenue du Colonel Roche, 31077 Toulouse Cedex 4, France. E-mail: jean.arlat@laas.fr.*
- *A. Bondavalli is with the Department of Systems and Informatics, University of Florence, Viale Morgagni, 65, 50134 Firenze, Italy. E-mail: bondavalli@unifi.it.*
- *B. Haverkort is with the University of Twente, Faculty for Electrical Engineering, Mathematics and Computer Science, PO Box 217, 7500 AE Enschede, The Netherlands. E-mail: brh@cs.utwente.nl.*
- *P. Veríssimo is with the Department of Informatica, FC/UL, Universidade de Lisboa, Bloco C6.3.10, Campo Grande, 1700 Lisboa, Portugal. E-mail: pjv@di.fc.ul.pt.*

For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org.

"Dependability through Assured Reconfiguration in Embedded System Software," by Elisabeth A. Strunk and John C. Knight, advocates that assuring properties over a simple subset of a system can provide assurance of critical properties over the entire system. The paper proposes an approach to system construction that ensures dependability properties by guaranteeing critical functional and reconfiguration properties. Systems designed this way can dependably be reconfigured by degrading to some simpler function rather than assuring the full functionality. Reconfiguration thus controls the effective complexity of the system without forcing that system to sacrifice desired, but nonassurable, capabilities.

"ReStore: Symptom-Based Soft Error Detection in Microprocessors," by Nicholas J. Wang and Sanjay J. Patel, deals with soft errors in microprocessors. So far, parity and ECC have been sufficient to stem the growing soft-error tide, but this will not be the case for long. The authors propose the ReStore architecture, which leverages existing performance-enhancing check-pointing hardware to recover from soft-error events in a low-cost fashion.

"Fast Byzantine Consensus," by Jean-Philippe Martin and Lorenzo Alvisi, presents the first protocol that reaches asynchronous Byzantine consensus in two communication steps in the common case. The protocol is optimal in terms of both the number of communication steps and the number of processes for 2-step consensus. The protocol can be used to build a replicated state machine that requires only three communication steps per request in the common case.

"System Call Monitoring Using Authenticated System Calls," by Mohan Rajagopalan, Matti A. Hiltunen, Trevor Jim, and Richard D. Schlichting, addresses the problem of detecting and controlling compromised applications using runtime checks. It introduces a new approach for preventing malicious actions from exploiting the system-call interface. The proposed scheme implements system-call monitoring via authenticated system calls, i.e., system calls augmented with extra information. The paper presents the approach, describes a prototype implementation, and gives experimental results suggesting that the approach is effective in protecting against compromised applications at modest cost.

"Detecting and Isolating Malicious Routers," by Alper Tugay Mızrak, Yu-Chung Cheng, Keith Marzullo, and Stefan Savage, advances the ability to tolerate attacks on key network infrastructure components. Routers with incorrect packet-forwarding behavior are detected and the paper presents a concrete protocol efficient enough to be implemented. A description of a prototype system, called Faith, which implements this approach on a PC router, concludes the paper.

In the paper "A Novel Approach for Phase-Type Fitting with the EM Algorithm," Axel Thümmler, Peter Buchholz, and Miklós Telek, address the important task of fitting measurement traces to distributions. In particular, they propose using mixtures of Erlang distributions to fit to, in combination with the estimation-maximization (EM) fitting approach. This combination is shown to lead to a very efficient and accurate fitting technique. The paper describes the technique in detail, and shows the applicability by addressing the fitting to six synthetic benchmark traces, to two real traces, as well as by studying queuing performance. The proposed method shows excellent performance throughput the experiments.

In "Combining Response Surface Methodology with Numerical Models for Optimization of Class-Based Queueing Systems," Peter Kemper, Dennis Müller, and Axel Thümmler address the issue of parameter optimization in complex Markovian queuing models. They do use the response surface method (RSM) for this purpose, however, they do so in combination with the methods used to solve the Markovian queuing network models. In this way, the required accuracy for the next step to be taken in the RSM optimization procedure may control the accuracy for the numerical solution of the Markovian models, thus leading to the optimal parameter setting in the quickest possible time. The paper developed the required theoretical framework, presents an algorithm, and evaluates the approach using a number of examples, in particular, a class-based scheduling strategy for sharing network link capacity.

Finally, we would like to thank all the reviewers for DCCS and PDS, as well as those involved in the selection and reviewing process for this special issue for their dedication and timeless efforts.

Jean Arlat
Andrea Bondavalli
Boudewijn Haverkort
Paulo Veríssimo
Guest Editors

Jean Arlat (M'80) is Directeur de Recherche of CNRS, the French National Organization of Scientific Research, and currently leads the research group on dependable computing and fault tolerance at LAAS-CNRS (www.laas.fr). His research interests focus on the design and assessment of hardware-and-software fault-tolerant systems and the dependability characterization of off-the-shelf software executives, including both analytical modeling and fault injection approaches, topics on which he authored or coauthored more than 100 papers and three books. He has led the industry-research cooperative actions set between LAAS and five leading companies (Airbus, Astrium, Électricité de France, Technicatome, and Thales): LIS (1997-2000: Laboratory for Dependability Engineering–www.laas.fr/LIS) and RIS (2001-2004: Network for dependability Engineering–www.ris.prd.fr). He is currently a member of the editorial board for the *IEEE Transactions on Dependable and Secure Computing*. Dr. Arlat is a member of the ACM, the IEEE, the IFIP WG 10.4, and the French SEE Working Group on Dependable Computing.

Andrea Bondavalli (M'96) is a professor in the Department of Systems and Informatics at the University of Florence. Previously, he was a researcher at the Italian National Research Council, working at the CNUCE Institute in Pisa. His research activity and interest are focused on the design and validation of critical systems and infrastructures, in particular, the design of fault-tolerant architectures, mechanisms and protocols and their evaluation in terms of dependability attributes such as reliability, availability, and performability. He is an author of more than 110 refereed publications in international journals and conferences. He has been PI in many projects funded by the European Community, acted in several occasions as an expert for the European community, and served as program chair of the most important conferences in the area. Professor Bondavalli is a member of the IEEE, the IFIP W.G. 10.4 on "Dependable Computing and Fault-Tolerance," ENCRESS Club Italy, and the AICA Working Group on Dependability in Computer Systems.

Boudewijn Haverkort received the engineering and the PhD degree in computer science, both from the University of Twente, in 1986 and 1991, respectively. Since 2003, he has held the chair for Design and Analysis of Communication Systems at the University of Twente, The Netherlands. Prior to that, he was a professor for performance evaluation and distributed systems at the RWTH Aachen, Germany, a lecturer in computer science at the University of Twente, The Netherlands, and visiting researcher in the Teletraffic Research Centre at the University of Adelaide, Australia. His research interests encompass the design and performance and dependability evaluation of computer-communication systems, model checking, parallel and distributed computing, and fault-tolerant computer systems. He has published more than 75 papers in international journals and conference proceedings, edited several books and conference proceedings, and written monographs on model-based performance evaluation of computer and communication systems and on performability modeling and evaluation. He is a member of the ACM, the German GI, and the IFIP Working Groups 6.3 (Performance of Communication Systems) and 7.3 (Computer Performance Modeling and Analysis), and a senior member of the IEEE.

Paulo Veríssimo is currently a professor in the Department of Informatics (DI) at the University of Lisboa Faculty of Sciences (http://www.di.fc.ul.pt/~pjv), and director of LASIGE, a research laboratory of the DI (http://lasige.di.fc.ul.pt). He belongs to the European Security & Dependability Advisory Board and is an associate editor of the *IEEE Transactions on Dependable and Secure Computing*. He is past chair of the IEEE Technical Committee on Fault-Tolerant Computing and of the steering committee of the DSN conference and belonged to the executive board of the CaberNet European Network of Excellence. He was coordinator of the CORTEX IST/FET project (http://cortex.di.fc.ul.pt). He is a senior member of the IEEE. Dr. Veríssimo leads the Navigators Research Group of LASIGE and is currently interested in: architecture, middleware and protocols for distributed, pervasive and embedded systems, in the facets of real-time adaptability, and fault/intrusion tolerance. He is the author of more than 130 refereed publications in international scientific conferences and journals in the area and coauthor of five books (example, http://www.navigators.di.fc.ul.pt/dssa/).