Lecture Notes in Computer Science 7527

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Paris Avgeriou (Ed.)

Software Engineering for Resilient Systems

4th International Workshop, SERENE 2012
Pisa, Italy, September 27-28, 2012
Proceedings

Springer

Volume Editor

Paris Avgeriou
University of Groningen
Nijenborgh 9
9747 AG Groningen, The Netherlands
E-mail: paris@cs.rug.nl

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-33175-6 e-ISBN 978-3-642-33176-3
DOI 10.1007/978-3-642-33176-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012945542

CR Subject Classification (1998): D.4.5, D.2.1-2, D.2.4-5, D.2.11, C.2.4, H.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The unprecedented level of complexity of modern software makes it difficult to ensure its resilience - the ability of the system to persistently deliver its services in a trustworthy way even when facing changes. Yet, we are observing the increasingly pervasive use of software in such critical infrastructures as transportation, health care, energy production etc. This trend urges the research community to develop powerful methods for assuring resilience of software-intensive systems. The SERENE workshop was established as a means of disseminating such research results and fostering discussion and cooperation between the growing resilience research community.

This volume contains the proceedings of the 4th International Workshop on Software Engineering for Resilient Systems (SERENE 2012). SERENE 2012 took place in Pisa, Italy, during September 27–28, 2012. The SERENE workshop is an annual event that brings together researchers and practitioners working on the various aspects of the software engineering life-cycle for resilient systems, especially design, verification, and assessment. In particular it covers such areas as:

- Modelling of resilience properties: formal and semi-formal techniques
- Requirements engineering and re-engineering for resilience
- Verification and validation of resilient systems
- Resilience prediction and experimental measurement
- Error, fault, and exception handling in the software life-cycle
- Empirical studies in the domain of resilient systems
- Relations between resilience and other system quality attributes
- Frameworks, patterns, and software architectures for resilience
- Resilience at run-time: metadata, mechanisms, reasoning, and adaptation
- Engineering of self-healing autonomic systems
- Quantitative approaches to ensuring resilience
- CASE tools for developing resilient systems

SERENE 2012 featured two invited speakers: Andrea Zisman and Nuno Ferreira Neves. Andrea Zisman is professor at the City University London (UK) and is considered a leading expert in service engineering in combination with resilience. She has worked, among others, in verification of service-based systems, consistency management and traceability of software artifacts, design and verification of secure software systems, and identification and composition of trusted services as well as development of trust framework for cloud infrastructures. Nuno Ferreira Neves is associate professor at the University of Lisbon (Portugal) and is a distinguished researcher in the area of fault and intrusion tolerance. He has worked on a range of topics, including security information and events management, critical infrastructure protection, dependable cloud computing, and intrusion-tolerant sensor networks.

The workshop was established by the members of the ERCIM working group SERENE. The group promotes the idea of resilient-centric development processes. It stresses the importance of extending the traditional software engineering practice with theories and tools supporting modelling and verification of various aspects of resilience. We would like to thank the SERENE working group for their hard work in publicizing the event and contributing to its technical program.

All submitted papers received at least three rigorous reviews. The accepted set, consisting of 12 high-quality submissions, allowed us to build a technically strong program that inspired lively discussion and future collaboration in the resilience community. We would like to express our gratitude to the Program Committee members and the additional reviewers who actively participated in reviewing and discussing the submissions. Of course, we would like to gratefully acknowledge and thank all the authors for their effort in submitting papers.

The organization of such a workshop is challenging. We would like to acknowledge the help of technical and administrative staff of CNR-ISTI, Newcastle University, and University of L'Aquila. SERENE 2012 was supported by ERCIM (European Research Consortium in Informatics and Mathematics), CNR-ISTI (Istituto di Scienza e Tecnologie dell'Informazione), and LASSY (Laboratory for Advanced Software Systems, University of Luxembourg).

July 2012

Paris Avgeriou
Program Chair

Felicita Di Giandomenico
General Chair

Organization

General Chair

Felicita Di Giandomenico	CNR-ISTI, Italy

Program Chair

Paris Avgeriou	University of Groningen, The Netherlands

Autumn School Director

Elena Troubitsyna	Åbo Akademi University, Finland

Steering Committee

Didier Buchs	University of Geneva, Switzerland
Henry Muccini	University of L'Aquila, Italy
Patrizio Pelliccione	University of L'Aquila, Italy
Alexander Romanovsky	Newcastle University, UK

Program Committee

Finn Arve Aagesen	NTNU, Norway
Mehmet Aksit	University of Twente, The Netherlands
Giovanna Di Marzo Serugendo	University of Geneva, Switzerland
Xavier Franch	Universitat Politècnica de Catalunya, Spain
Vincenzo Grassi	University of Rome Tor Vergata, Italy
Brahim Hamid	IRIT, France
Valerie Issarny	INRIA, France
Mohamed Kaaniche	LAAS-CNRS, France
Vyacheslav Kharchenko	National Aerospace University, Ukraine
Linas Laibinis	Åbo Akademi University, Finland
Tom Maibaum	McMaster University, Canada
Jose Carlos Maldonado	University of Sao Paulo, Brazil
Eda Marchetti	CNR, Italy
Raffaela Mirandola	Politecnico di Milano, Italy
Ivan Mistrik	Indep. Consultant, Germany
Henry Muccini	University of L'Aquila, Italy
Flavio Oquendo	European University of Brittany/IRISA-UBS, France

Andras Pataricza	BUTE, Hungary
Patrizio Pelliccione	University of L'Aquila, Italy
Anthony Savidis	FORTH, Greece
Peter Schneider-Kamp	University of Southern Denmark
Francis Tam	Nokia, Finland
Elena Troubitsyna	Åbo Akademi University, Finland
Apostolos Zarras	University of Ioannina, Greece

Subreviewers

Maurice H. Ter Beek
Silverio Martinez-Fernandez
Somayeh Malakuti
Nicolas Desnos
Pasqualina Potena

Table of Contents

Fault Tolerance and Exception Handling

Implementing Reusable Exception Handling Patterns with Compile-Time Metaprogramming 1
Yannis Lilis and Anthony Savidis

A Case Study in Formal Development of a Fault Tolerant Multi-robotic System 16
Inna Pereverzeva, Elena Troubitsyna, and Linas Laibinis

Fault-Tolerant Interactive Cockpits for Critical Applications: Overall Approach 32
Camille Fayollas, Jean-Charles Fabre, David Navarre, Philippe Palanque, and Yannick Deleris

Safety Modeling

Linking Modelling in Event-B with Safety Cases 47
Yuliya Prokhorova and Elena Troubitsyna

Safety Lifecycle Development Process Modeling for Embedded Systems – Example of Railway Domain 63
Brahim Hamid, Jacob Geisel, Adel Ziani, and David Gonzalez

Supporting Evolution

Language Enrichment for Resilient MDE 76
Yasir Imtiaz Khan and Matteo Risoldi

Assume-Guarantee Testing of Evolving Software Product Line Architectures 91
Maurice H. ter Beek, Henry Muccini, and Patrizio Pelliccione

Resilience in Service-Oriented Computing

FAS: Introducing a Service for Avoiding Faults in Composite Services 106
Koray Gülcü, Hasan Sözer, and Barış Aktemur

Dependability of Service-Oriented Computing: Time-Probabilistic Failure Modelling 121
Anatoliy Gorbenko, Alexander Romanovsky, Vyacheslav Kharchenko, and Olga Tarasyuk

Monitoring Service Choreographies from Multiple Sources 134
Amira Ben Hamida, Antonia Bertolino, Antonello Calabrò, Guglielmo De Angelis, Nelson Lago, and Julien Lesbegueries

Applying Formal Methods in Case Studies

Supporting Field Investigators with PVS: A Case Study in the Healthcare Domain 150
Paolo Masci, Dominic Furniss, Paul Curzon, Michael D. Harrison, and Ann Blandford

Model-Based Evaluation of the Availability of a CBTC System 165
Alessio Ferrari, Massimiliano L. Itria, Silvano Chiaradonna, and Giorgio O. Spagnolo

Author Index 181