Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany
Preface

Welcome to the proceedings of the 5th workshop on Software Engineering for Resilient Systems (SERENE 2013). We are very pleased that SERENE 2013 took place in the beautiful city of Kiev (Ukraine) during October 3–4, 2013.

The previous workshops of the SERENE series were held in Newcastle upon Tyne (2008), London (2010), Geneva (2011), and Pisa (2012). The workshop is supported by the ERCIM (European Research Consortium in Informatics and Mathematics) Working Group on Software Engineering for Resilient Systems, and brings together researchers and practitioners working on developing and applying advanced engineering techniques that help make complex systems resilient. The working group promotes the idea of resilient-explicit development that extends the traditional software engineering practice with theories, methods, and tools which explicitly support modelling, verification, and design of various facets of resilience.

The workshop covered topics related to all aspects of resilience engineering, including

Methodology:

- Relations between resilience, dependability, and quality attributes
- Requirements engineering and re-engineering for resilience
- Trustworthy and intrusion-safe systems
- Error fault and exception handling in the software life-cycle

Models & methods:

- Resilience prediction and experimental measurement
- Modelling of resilience properties: formal and semi-formal techniques
- Verification and validation of resilient systems
- Diversity and multi-version technologies for resilience

Tools & technologies:

- Frameworks, patterns, and software architectures for resilience
- Resilience at run-time: metadata, mechanisms, reasoning and adaptation
- CASE tools for developing resilient systems

Case studies & applications:

- Empirical studies in the domain of resilient systems
- Cloud computing and resilient service provisioning
- Resilience of software-hardware co-engineering
- Engineering of self-healing autonomic systems
- Resilience of cyber physical systems and infrastructures
- Global aspects of resilience engineering: education, training, and cooperation.
It is the SERENE tradition to explicitly invite contributions focusing on various aspects of research and development, and to call for submissions in five categories: technical papers, experience/industry papers, PhD forum papers, project papers, and tool papers.

SERENE 2013 attracted 21 submissions from 11 countries. 13 papers were accepted after a rigorous review process with every paper receiving at least 3 reviews. These include nine technical papers, two PhD students’ papers and two project papers.

Two prominent researchers working on resilience engineering, András Pataricza from BUTE (Hungary) and Robin Bloomfield from Adelard/City University (UK), kindly agreed to deliver keynote talks during the workshop. The volume includes reviewed and revised papers describing the research presented by the two keynote speakers.

We would like to thank the SERENE Steering Committee and the members of the SERENE working group for their hard work in publicising the event and contributing to the technical programme. We are grateful to the Programme Committee members and to the additional reviewers for all their efforts. We would like to acknowledge the help of the staff at Newcastle University and National Aerospace University (Kharkiv). But, first of all, our thanks go to all the contributors and the attendees of the workshop for making this workshop a success.

July 2013

Anatoliy Gorbenko
Alexander Romanovsky
Vyacheslav Kharchenko
Organization

General Chair

Vyacheslav Kharchenko  National Aerospace University, Ukraine

Program Chairs

Anatoliy Gorbenko  National Aerospace University, Ukraine
Alexander Romanovsky  Newcastle University, UK
Vyacheslav Kharchenko  National Aerospace University, Ukraine

Steering Committee

Henry Muccini  University of L’Aquila, Italy
Didier Buchs  University of Geneva, Switzerland
Patrizio Pelliccione  University of L’Aquila, Italy
Alexander Romanovsky  Newcastle University, UK
Elena Troubitsyna  Åbo Akademi University, Finland

SERENE WG Liaison

Nicolas Guelfi  University of Luxembourg, Luxembourg

Program Committee

Alessandro Garcia  PUC-Rio, Brazil
Andras Pataricza  BUTE, Hungary
Anthony Savidis  FORTH, Greece
Elena Troubitsyna  Åbo Akademi University, Finland
Felicita Di Giandomenico  ISTI-CNR, Italy
Felix Salfner  SAP Innovation Center, Germany
Finn Arve Aagesen  NTNU, Norway
Giovanna Di Marzo  Serugendo
Henry Muccini  University of L’Aquila, Italy
Holger Giese  University of Potsdam, Germany
Ivan Mistrik  Indep. Consultant, Germany
Ivica Crnkovic  Mälardalen University, Sweden
John Knight  University of Virginia, USA
Jörg Kienzle  McGill University, Canada
VIII Organization

Leszek Kotulski 
AGH University of Science and Technology, Poland

Mohamed Kaaniche 
LAAS-CNRS, France

Nicolas Guelfi 
University of Luxembourg, Luxembourg

Paris Avgeriou 
University of Groningen, The Netherlands

Patrizio Pelliccione 
University of L’Aquila, Italy

Peter Schneider-Kamp 
University of Southern Denmark, Denmark

Raffaela Mirandola 
Politecnico di Milano, Italy

Schahram Dustdar 
Vienna University of Technology, Austria

Stefania Gnesi 
ISTI-CNR, Italy

Stefano Russo 
University of Naples Federico II, Italy

Tudor Dumitras 
Symantec, USA

Valerie Issarny 
Inria, France

Vincenzo Grassi 
University of Rome Tor Vergata, Italy

Vladimir Hahanov 
National University of Radioelectronics, Ukraine

Willi Hasselbring 
Kiel University, Germany

Reviewers

Anton Tarasyuk 
Åbo Akademi University, Finland

Apostolis Ampatzoglou 
University of Groningen, The Netherlands

Gregor Berg 
Hasso Plattner Institute, Germany

Imre Kocsis 
BUTE, Hungary

Maciej Koutny 
Newcastle University, UK

Rui Miguel Lopes 
Critical Software, Portugal

Yuliya Prokhorova 
Åbo Akademi University, Finland
# Table of Contents

## Keynote Talks

Empirical Assessment of Resilience ................................. 1  
   András Pataricza, Imre Kocsis, Ágnes Salánki, and László Gónczy

Security-Informed Safety: If It’s Not Secure, It’s Not Safe ........ 17  
   Robin Bloomfield, Kateryna Netkachova, and Robert Stroud

## Resilient Software and Design

Engineering a Platform for Mission Planning of Autonomous and Resilient Quadrotors ............................................. 33  
   Davide Di Ruscio, Ivano Malavolta, and Patrizio Pelliccione

Towards Agile Development of Critical Software .................. 48  
   Janusz Górski and Katarzyna Lukasiewicz

Supporting the Evolution of Free and Open Source Software Distributions ...................................................... 56  
   Davide Di Ruscio and Patrizio Pelliccione

## Rigorous Reasoning

Optimizing Verification of Structurally Evolving Algebraic Petri Nets... 64  
   Yasir Imtiaz Khan

A Case Study in Refinement-Based Modelling of a Resilient Control System .......................................................... 79  
   Yuliya Prokhorova, Elena Troubitsyna, and Linas Laibinis

Synthesis of Resilient Choreographies ................................. 94  
   Marco Autili, Amleto Di Salle, and Massimo Tivoli

## Applications

Formal Development and Quantitative Assessment of a Resilient Multi-robotic System ............................................... 109  
   Anton Tarasyuk, Inna Pereverzeva, Elena Troubitsyna, and Linas Laibinis

The SafeCap Project on Railway Safety Verification and Capacity Simulation .............................................................. 125  
   Alexei Iliasov, Ilya Lopatkin, and Alexander Romanovsky
Modeling of Autonomous Vehicle Operation in Intelligent Transportation Systems ........................................... 133  
Mark Woodard and Sahra Sedigh

Concepts

Preliminary Contributions Towards Auto-resilience ....................... 141  
Vincenzo De Florio

A New Approach to Software Reliability ........................................... 156  
Dmitry A. Maevsky

Analysis

Static Analysis Approach for Defect Detection in Multithreaded C/C++ Programs ............................................. 169  
Mikhail Moiseev

Stochastic Model-Based Analysis of Railway Operation to Support Traffic Planning .................................................. 184  
Felicia Di Giandomenico, Alessandro Fantechi, Stefania Gnesi, and Massimiliano Leone Itria

Author Index ................................................................. 199