Fifth International Workshop on Specification and Verification of Component-Based Systems (SAVCBS 2006)

ACM SIGSOFT/FSE-14
14th ACM Symposium on the
Foundations of Software Engineering
Portland, Oregon, USA
November 10-11, 2006

Technical Report #06-29, Department of Computer Science, Iowa State University
226 Atanasoff Hall, Ames, IA 50011-1041, USA

SAVCBS 2006 PROCEEDINGS

Specification and Verification of Component-Based Systems

http://www.cs.iastate.edu/SAVCBS/

November 10-11, 2006
Portland, Oregon, USA

Workshop at ACM SIGSOFT/FSE-14
14th ACM Symposium on
Foundations of Software Engineering

Fifth International Workshop on Specification and Verification of Component-Based Systems (SAVCBS 2006), November 10-11, 2006, Portland, Oregon, USA.

SAVCBS 2006
TABLE OF CONTENTS

SAVCBS 2006
ORGANIZING COMMITTEE

Mike Barnett (Microsoft Research, USA)
Mike Barnett is a Research Software Design Engineer in the Foundations of Software Engineering group at Microsoft Research. His research interests include software specification and verification, especially the interplay of static and dynamic verification. He received his Ph.D. in computer science from the University of Texas at Austin in 1992.

Dimitra Giannakopoulou (RIACS/NASA Ames Research Center, USA)
Dimitra Giannakopoulou is a RIACS research scientist at the NASA Ames Research Center. Her research focuses on scalable specification and verification techniques for NASA systems. In particular, she is interested in incremental and compositional model checking based on software components and architectures. She received her Ph.D. in 1999 from the Imperial College, University of London.

Gary T. Leavens (Dept. of Computer Science, Iowa State University, USA)
Gary T. Leavens is a professor of Computer Science at Iowa State University. His research interests include programming and specification language design and semantics, program verification, and formal methods, with an emphasis on the object-oriented and aspect-oriented paradigms. He received his Ph.D. from MIT in 1989.

Natasha Sharygina (CMU and SEI, USA; Lugano, Switzerland)
Natasha Sharygina is a senior researcher at the Carnegie Mellon Software Engineering Institute and an adjunct assistant professor in the School of Computer Science at Carnegie Mellon University, and an assistant professor at the University of Lugano. Her research interests are in program verification, formal methods in system design and analysis, systems engineering, semantics of programming languages and logics, and automated tools for reasoning about computer systems. She received her Ph.D. from The University of Texas at Austin in 2002.

SAVCBS 2006
PROGRAM COMMITTEE

Jonathan Aldrich (School of Computer Science, Carnegie Mellon Univ., USA)
Jonathan Aldrich chaired the program committee for SAVCBS 2006. He is an assistant professor in the School of Computer Science at Carnegie Mellon University. His research interests are in lightweight software verification using programming language and program analysis techniques. He received his Ph.D. in Computer Science from the University of Washington in 2003.

Program Committee:
Jonathan Aldrich (Carnegie Mellon University), Program Committee Chair
Michael Barnett (Microsoft Research)
Patrice Chalin (Concordia University)
Robert Chatley (Kizoom, London)
David Coppit (The College of William and Mary)
Ivica Crnkovic (Mälardalen University)
Stephen Edwards (Virginia Tech)
Timothy J. Halloran (Air Force Institute of Technology)
Marieke Huisman (INRIA Sophia Antipolis)
Joseph Kiniry (University College Dublin)
Matthew Parkinson (Middlesex University)
Corina Pasareanu (QSS/NASA Ames Research Center)
Andreas Rausch (University of Kaiserslautern)
Robby (Kansas State)
Heinz Schmidt (Monash University)
Wolfram Schulte (Microsoft Research)
Natasha Sharygina (Lugano and Carnegie Mellon)
Tao Xie (North Carolina State)

Sponsors:

Microsoft® Research

SAVCBS 2006
WORKSHOP INTRODUCTION

This workshop is concerned with how formal (i.e., mathematical) techniques can be or should be used to establish a suitable foundation for the specification and verification of component-based systems. Component-based systems are a growing concern for the software engineering community. Specification and reasoning techniques are urgently needed to permit composition of systems from components. Component-based specification and verification is also vital for scaling advanced verification techniques such as extended static analysis and model checking to the size of real systems. The workshop will consider formalization of both functional and non-functional behavior, such as performance or reliability.

This workshop brings together researchers and practitioners in the areas of component-based software and formal methods to address the open problems in modular specification and verification of systems composed from components. We are interested in bridging the gap between principles and practice. The intent of bringing participants together at the workshop is to help form a community-oriented understanding of the relevant research problems and help steer formal methods research in a direction that will address the problems of component-based systems. For example, researchers in formal methods have only recently begun to study principles of object-oriented software specification and verification, but do not yet have a good handle on how inheritance can be exploited in specification and verification. Other issues are also important in the practice of component-based systems, such as concurrency, mechanization and scalability, performance (time and space), reusability, and understandability. The aim is to brainstorm about these and related topics to understand both the problems involved and how formal techniques may be useful in solving them.

The goals of the workshop are to produce:

1. An outline of collaborative research topics,
2. A list of areas for further exploration,
3. An initial taxonomy of the different dimensions along which research in the area can be categorized. For instance, static/dynamic verification, modular/whole program analysis, partial/complete specification, soundness/completeness of the analysis, are all continuums along which particular techniques can be placed, and
4. A web site that will be maintained after the workshop to act as a central clearinghouse for research in this area.

We enthusiastically thank the authors of submitted papers; their quality contributions and participation are what make a workshop like SAVCBS successful. We thank the program committee for their careful reading and reviewing of the submissions. Our PC members have expertise in a wide variety of sub-disciplines related to specification and verification of component-based systems; they include established research leaders and promising recent Ph.D.s; they come from both industry and academia, and hail from all over the world.

We received 13 submissions, of which 3 were withdrawn, leaving 10 to be reviewed. All papers were reviewed by 3 PC members, with PC member papers were reviewed by 4 PC members and held to a higher-confidence standard. Ultimately 8 papers were accepted, after PC discussions via email. As in previous years, we accepted additional submissions as poster presentations, reflecting the role of SAVCBS to promote discussion and incubation of new ideas for which a full paper may be premature.

This year our program also includes solutions to a specification and verification challenge problem posed to workshop attendees. The problem focused on the specification of iterators in collection libraries such as those in Java or C#. In these systems multiple iterators can be created over a collection, and can access that collection simultaneously as long as it is modified. However, if the collection is modified, all iterators are invalidated (except—for Java—the iterator through which the change was made, if any). While familiar to many programmers, this problem poses real challenges for specification and verification systems such as state aliased between the iterators and the collection. Four-page challenge problem solutions were each read and reviewed by two members of the program committee, to ensure quality and help the authors improve their presentation; we accepted all 5 submissions.

This year we also were pleased to have an invited presentation by Josh Berdine of Microsoft Research titled “Variance Analyses from Invariance Analyses.”

Jonathan Aldrich (Program Committee Chair)

Mike Barnett (Organizing Committee)
Dimitra Giannakopoulou (Organizing Committee)
Gary T. Leavens (Organizing Committee)
Natasha Sharygina (Organizing Committee)