Seventh International Workshop on Specification and Verification of Component-Based Systems (SAVCBS 2008)

SIGSOFT 2008/FSE 16
16th ACM SIGSOFT Symposium on the Foundations of Software Engineering
Atlanta, Georgia, USA
November 9-10, 2008

Technical Report CS-TR-08-07,
School of Electrical Engineering and Computer Science, University of Central Florida,
4000 Central Florida Blvd., Orlando, Florida, 32816-2362 USA

SAVCBS 2008 PROCEEDINGS

Specification and Verification of Component-Based Systems

http://www.eecs.ucf.edu/SAVCBS/

November 9-10, 2008
Atlanta, Georgia, USA

Workshop at SIGSOFT 2008/FSE 16
16th ACM SIGSOFT Symposium on the
Foundations of Software Engineering

SAVCBS 2008
TABLE OF CONTENTS

SAVCBS 2008
ORGANIZING COMMITTEE

Jonathan Aldrich (Carnegie Mellon University, USA)
Jonathan Aldrich is an assistant professor in the School of Computer Science at Carnegie Mellon University. His research contributions include techniques for verifying object interaction protocols and architectures, modular reasoning techniques for aspects and stateful programs, and new object-oriented language models. He received his Ph.D. from the University of Washington in 2003.

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 (School of EECS, University of Central Florida, USA)
Gary T. Leavens is a professor in the School of Electrical Engineering and Computer Science at the University of Central Florida. He moved to Orlando in Fall 2007. Previously he was 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 2008
PROGRAM COMMITTEE

Robby (Department of Computing and Information Sciences, Kansas State University, USA)
Robby chaired the program committee for SAVCBS 2008. He is an assistant professor in the Department of Computing and Information Sciences, Kansas State University. His research interests are in software specification, analysis, transformation, and model-driven software development. He received his Ph.D. in Computer Science from Kansas State University in 2004.

Workshop Program Committee:
Patrice Chalin (Concordia University, Canada)
Ivica Crnkovic (Mälardalen University, Sweden)
Cormac Flanagan (University of California, Santa Cruz, USA)
Alex Groce (Jet Propulsion Laboratory, USA)
Joseph Kiniry (University College Dublin, Ireland)
Eric Madelaine (INRIA, Sophia Antipolis, France)
Rupak Majumdar (UCLA, USA)
Darko Marinov (University of Illinois at Urbana-Champaign, USA)
Marius Minea ("Politehnica" University of Timisoara, Romania)
Mauro Pezzè (University of Lugano, Switzerland)
Arnd Poetzsch-Heffter (University of Kaiserlautern, Germany)
Andreas Rausch (T.U. Clausthal, Germany)
Natarajan Shankar (SRI, USA)
Yannis Smaragdakis (University of Oregon, USA)
Nigamanth Sridhar (Cleveland State University, USA)
Serdar Tasiran (Koc University, Turkey)

SAVCBS 2008
WORKSHOP INTRODUCTION

This volume contains the proceedings of the *Seventh Workshop on Specification and Verification of Component-Based Systems (SAVCBS 2008),* affiliated with the *Sixteenth ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2008)*. *SAVCBS 2008* took place in Atlanta, Georgia, USA on November 9-10, 2008.

SAVCBS is a venue for discussing 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 considers formalization of both functional and non-functional behavior, such as performance or reliability.

SAVCBS aims to bring 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. The workshop seeks to bridge the gap between principles and practice on this research area. The intent of bringing participants together at the workshop is to help form a community-oriented understanding of the relevant research problems and to 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. *SAVCBS* aims to provide a venue 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. Contacts and discussion among researchers and practitioners, and
2. 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 academia and esteemed research institutes, and hail from all over the world.

We received 15 research paper submissions. All papers were reviewed by 3 PC members, with PC member papers reviewed by 4 PC members. After PC discussions, 6 papers were accepted. As in previous years, we accepted additional submissions as short and 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, we accepted 3 papers for short presentations and 4 papers for poster presentations. Two of the accepted poster presentations were withdrawn. Among all of the 15 papers submitted, 2 submissions were rejected.

This year's program also includes a solution to a specification and verification challenge problem based on the "composite pattern". A composite object is one that organizes objects into a tree structure in order to represent a part-whole hierarchy. The point of the pattern is that clients have a uniform interface whether they have a reference to a sub-tree (i.e., a composite object) or a leaf (a single object). The focus of the challenge problem is to specify and verify an invariant that relates each composite node to its children. This invariant is broken when a new child is added, and it remains broken until all the transitive parents of the new node are traversed and adapted. The main challenge is to give a concise specification, especially for the operation that re-establishes the invariant. After the reviewing process, we accepted all 4 submissions to the challenge problem.

This year, we are pleased to have an invited presentation by Wolfgang Emerich of University College London titled "Verification Challenges for Components in Federated Distributed Systems".

Robby (Program Committee Chair)

Jonathan Aldrich (Organizing Committee)
Mike Barnett (Organizing Committee, Challenge Problems Chair)
Dimitra Giannakopoulou (Organizing Committee)
Gary T. Leavens (Organizing Committee)
Natasha Sharygina (Organizing Committee)