SAVCBS'06:
5th Workshop on Specification and Verification of Component-Based Systems
A Workshop Proposal for SIGSOFT/FSE 2006

Theme and Goals

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.

We would like 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. 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 participants will 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. A web site that will be maintained after the workshop to act as a central clearinghouse for research in this area, and
4. A special issue of a journal that will invite revised and expanded versions of selected papers from the workshop.

Relevance

There has been an explosion of interest in applying formal techniques to the specification and verification of components. The success of applying formal tools to hardware systems, such as model checking, has led many investigators to extend these tools to software. At the same time, the world of component-based systems is crying out for an effective technique for consumers, both human and computer, to be able to evaluate the suitability of a binary component before either composing it into a larger system or utilizing its services directly. The combined push and pull of these two trends promises to have a profound impact on software engineering.

Every software engineering conference in the last few years has included several papers on this topic. The CAV conference contains many papers related to this issue. There are also several related workshops (PASTE, FTfJP at ECOOP, and the CBSE series of workshops formerly associated with
ICSE), which show the amount of interest in the area. However, these related events focus either on formal techniques or on components, but not both. SAVCBS fills an unaddressed gap between the formal methods community and the component-based systems community by focusing on how formal methods can be used to tackle critical CBSE problems. Additionally, the maturity of available research tools (Spec#, JML, LOOP, AsmL, ESC/Java) has already produced commercial usage and provoked further interest.

**Number of Participants**

The workshop will be limited to between 15 and 40 participants. If the workshop length allows, an invited keynote speaker will highlight key issues and problems. Participants will be selected based on an evaluation of submitted position papers. An ideal position paper would identify an emerging or critical research topic, problem, or technique related to formal methods in component-based software engineering. It should address the following questions.

- What is the problem (or topic or area) that is being described?
- What is the significance of the problem for component-based software?
- What theoretical or practical insights are needed to solve this problem?
- What related work is there about the problem and the theoretical approach? How does it compare?

**Pre-Workshop Activities**

All participants will be given (electronic) copies of accepted position papers in advance of the workshop date.

**Planned Workshop Activities**

The workshop format will be informal to allow free flow of information, combining selected short presentations in each area of interest with discussions. The number and duration of presentations will depend on the workshop duration (ideally two days); priority will be given to assigning sufficient time for discussion, to give the opportunity to all participants to actively exchange views about the topics of interest.

**Solicitation and Selection Process**

In addition to whatever ESEC/FSE publicity mechanisms can be used, we will advertise the workshop on relevant mailing lists (such as SEWORLD), web sites (individual and group), and by personal e-mail distribution. We will also distribute the call to the authors, participants, and program committee from previous SAVCBS workshops. The selection of position papers will be made by a program committee, which will be chaired by Prof. Jonathan Aldrich of Carnegie Mellon University. (We have started contacting the program committee, but do not yet have confirmations.)

**Organizer Background**

1. Dimitra Giannakopoulou is a Research Scientist with RIACS, working at NASA Ames Research Center. Her research focuses on scalable specification and verification techniques for NASA missions. She is particularly interested in modular verification based on system components and architectures. She received a PhD in March 1999, from the Dept. of Computing, Imperial College, University of London, where she was employed as a Research Associate from September 1994 to June 2000. Her research was funded by UK (EPSRC) and European Union (ESPRIT) projects. She has published extensively at international journals and conferences such as *Journal of Automated Software Engineering, TACAS, ICSE,*
ESEC/FSE. She has reviewed several submissions to international journals and conferences, such as IEEE Transactions on Software Engineering, ASE Journal, Requirements Engineering Journal, ICSE, ESEC/FSE, CAV, ASE and SPIN. She co-organized the OOPSLA 2001 workshop on Specification and Verification of Component-Based Systems.

2. Gary Leavens is a Professor in the Dept. of Computer Science at Iowa State University. He received his Ph. D. from MIT in 1989 and has taught at Iowa State University ever since. He has written for such journals as ACM TOSEM, ACM TOPLAS, Theoretical Computer Science, Acta Informatica, and Theory and Practice of Object Systems. He has served on the program committees of conferences such as ESEC/FSE (1999), ICSE (2000), OOPSLA (several times including 2006), AOSD (2003), ECOOP (2003), POPL (2006), Formal Methods 2006. His research on the Java Modeling Language (JML), a formal specification language tailored to Java, is funded by the National Science Foundation. In addition to co-organizing a workshop on Foundations of Component Based Systems with Murali Sitaraman, Leavens has also co-organized a workshop on Formal Techniques for Java-like Programs (FTfJP) at ECOOP every year since 2000. He has also co-organized the Foundations of Aspect Oriented Languages (FOAL) workshops at every AOSD since 2002. He co-organized the OOPSLA 2001 workshop on Specification and Verification of Component-Based Systems. He was a coeditor (with Susan Eisenbach) of a special issue of Concurrency, Practice and Experience devoted to papers from the 2000 ECOOP workshop. He is an assistant editor of the journal Software and Systems Modeling. He is a member of IFIP Working Group 2.3.

3. Mike Barnett has been a Research Software Design Engineer at Microsoft Research since 1995. He received his PhD from The University of Texas at Austin in 1992. From 1992—1995 he was an Assistant Professor at the University of Idaho. His current research centers on the modular verification of object-oriented programs. He works on the Spec# project based at Microsoft Research.

4. Natasha Sharygina is a senior researcher at Carnegie Mellon University and the Software Engineering Institute, and is also an Adjunct Assistant Professor in the School of Computer Science at at Carnegie Mellon University. She received her Ph. D. from the University of Texas at Austin in 2002. She has written for such journals as the Formal Methods in System Design Journal, and highly competitive conferences and workshops such as CAV, TACAS, and the SPIN workshop. She has been a co-organizer of the SAVCBS workshop since 2003 and also its program committee chair (in 2004). She co-organized the CMU/SEI symposium on software model checking.

**Preliminary Call for Position Papers**

SAVCBS is focused on using formal (i.e., mathematical) techniques to establish a foundation for the specification and verification of component-based systems. Specification techniques are urgently needed to support effective reasoning about systems composed from components. Component-based approaches also underscore the need 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). Suggested research topics of interest include (but are not limited to):

- Techniques for component-based verification or reasoning
- Component-based specification languages
- Static analysis of components and component compositions
- Verification-oriented design methodologies for components
- Dynamic checking techniques, including run-time assertion or property checking
• Specification and verification of non-functional component behavior (performance, memory, concurrency, etc.)
• Unifying formal descriptions of concurrency properties with model-based behavioral descriptions of components
• Balancing tradeoffs (automatic/manual verification, soundness/completeness, static/dynamic verification, testing/formal verification, scalability, etc.)
• Theories of component composition
• Industrial experience with formal techniques for component-based systems
• Case studies of applying formal techniques to component based systems
• Educational experience or tactics for formal approaches to component-based systems

We are soliciting position papers from researchers and practitioners in the areas of component-based software engineering and formal methods. Submissions should outline the current state of research or practice, describe the most pressing shortcomings, and formulate goals for future development. Submissions must not exceed seven (7) pages.

The workshop objective is to bring together scientists from both academia and industry to discuss their experiences, forge collaborative relationships, and form a more cohesive research agenda in the community. Papers will be selected in each area of interest for short presentations to catalyze discussions. The number and duration of presentations will depend on the workshop duration (ideally two days); priority will be given to assigning sufficient time for discussion. To make discussions effective, the workshop will not accept more than 40 participants.

Scheduling

The last two meeting of this workshop were two-day events, which allowed for generous discussions, an invited talk, and a poster session. The poster session is valuable for encouraging participation from students and others whose papers are not accepted for presentation. Further, at the last one day workshop, participants indicated a desire for a 2 day format. As a result, we would prefer to have 2 days (e.g., 10 and 11 November). If only a 1 or 1.5 day format is available, however, we feel that the event will still provide a valuable forum for the participants.

Our plan for the important dates for SAVCBS is as follows:

- Submission deadline: August 15
- Notification: September 15
- Final versions: October 15

Organizational Details

The workshop requires a room large enough to hold 40 people, chairs for all participants, a projection screen, a projection system that can accommodate various PC platforms, and an overhead projector for transparencies. No sound amplification is needed.

Information from Past Workshops

See http://www.cs.iastate.edu/SAVCBS/ for information from past workshops, including proceedings, program committees, etc.