Composition of Embedded Systems

Scientific and Industrial Issues

13th Monterey Workshop 2006
Paris, France, October 16-18, 2006
Revised Selected Papers

Springer
Preface

Composition of Embedded Systems:
Scientific and Industrial Issues

The Monterey Workshops series was initiated in 1992 by David Hislop with the purpose of exploring the critical problems associated with cost-effective development of high-quality software systems. During its 14-year history, the Monterey Workshops have brought together scientists that share a common interest in software development research serving practical advances in next-generation software-intensive systems. Each year is dedicated to a particular topic of critical importance. In the past years, workshop topics were "Networked Systems: Realization of Reliable Systems on Unreliable Networked Platforms" (2005 in Laguna Beach, California), "Software Engineering Tools: Compatibility and Integration" (2004 in Vienna), "Engineering for Embedded Systems: From Requirements to Implementation" (2003 in Chicago), "Radical Innovations of Software and Systems Engineering in the Future" (2002 in Venice), "Engineering Automation for Software Intensive System Integration" (2001 in Monterey).

The 14th Monterey Workshop was held in Paris, France, during October 16–18, 2006.

Context of the 2006 Monterey Workshop

Distributed real-time embedded (DRE) systems are notoriously hard to design, implement, and validate. The complexity of a typical system found in many critical applications in civil and military aviation, transportation systems, and medical devices exceeds the capabilities of existing development and verification technologies. Companies spend enormous amounts of time and resources on verification and validation of DRE systems they develop and yet, despite their best efforts, hard-to-find errors show up in deployed products.

More and more, large DRE systems are built from components developed by third-party suppliers in an attempt to reduce development costs. But integration of DRE components presents its own set of problems: components that appear correct in isolation fail to function properly when put together. Research on DRE composition aims to develop techniques for designing DRE components and integrating them into larger systems in such a way that emphasizes safety and reliability of the integrated systems.

The 14th Monterey Workshop on "Composition of Embedded Systems: Scientific and Industrial Issues" focused on new, promising directions for achieving high software and system reliability in DRE systems while minimizing design, verification, and validation efforts and time to market.

All presentations at the workshop were by invitation upon the advice of the Program Committee.
Invited Speakers

Juan Colmenares  University of California at Irvine, USA
David Corman  Boeing, USA
Gregory Haik  Thales, France
Jérôme Hugues  Telecom-Paris, France
Xenofon Koutsoukos  Vanderbilt University, USA
Ingolf Krueger  UC San Diego, USA
Radu Grosu  Stony Brook University, USA
Gabor Karsai  Vanderbilt University, USA
Christoph Kirsch  University of Salzburg, Austria
Francois Laroussinie  ENS Cachan, France
Klaus Müller-Glaser  FZI, Germany
Rick Schantz  BBN Technologies, USA
Manuel Rodriguez  Naval Postgraduate School, USA
Roman Obermaisser  TU Vienna, Austria
Francois Terrier  CEA-LIST, France
Joseph Sifakis  Verimag, France

Papers included in this volume were selected among the submissions from the workshop’s discussions.

Workshop Topics

Our society is increasingly reliant on embedded systems for many critical day-to-day activities. In many application domains, such as automotive and avionics industries, satellite communications, and medical devices, embedded software is the major driving force. Development of embedded software has come to dominate design effort, time, and costs. Despite massive development efforts, software is now a significant cause of failure in embedded devices. Advances in embedded software development technologies are therefore fundamental to the economic success, scientific and technical progress, as well as national security of our society.

Development of embedded software-intensive systems is always a hard task due to a multitude of stringent constraints that these systems have to satisfy, including stringent timing, memory footprint, and other resource requirements. In recent years, the problem has become even more complicated due to the advent of DRE systems, which need to interact with each other in a timely and predictable fashion, while still satisfying their individual requirements. The increased complexity of DRE systems has rendered existing development technologies inadequate for the demands of today’s applications.

Composition is a possible approach for conquering the complexity of modern embedded systems design. In this approach, the components of the system can be developed in isolation and then integrated together in a property-preserving way. Compositional development for embedded systems is an active research area, but much remains to be done to keep up with the needs of industry and society.
The workshop discussed a range of challenges in embedded systems design that require further major advances in software and systems composition technology:

- **Model-driven development for DRE systems.** Modeling and model-driven development (MDD) are of particular importance for DRE systems, because of their dependence on continuously evolving environments and strict requirements that need to be specified precisely for testing and verification.

- **Balancing cost and assurance in DRE systems.** High assurance comes at a high cost. System developers need to balance development costs and assurance levels depending on the criticality of particular system aspects. This area has not received enough attention from the research community and system developers lack proper tools to reason about such trade-offs.

- **Domain-specific languages for DRE systems.** Domain-specific languages (DSL) allow designers to represent systems directly using concepts from their application domains. Because of this, models and designs are easier to understand and validate, increasing confidence in the system. Research on DSL has been very active recently, yet many open questions remain, including semantic definitions for DSLs and correctness of model transformations with respect to the language semantics.

- **Composition of real-time components.** Timing and resource constraints, prevalent in DRE system development, make composition much more difficult. Component interfaces that are the basis for system integration now have to expose not only the input and output behaviors of the component, but also its resource demands. Formalisms that are used to reason about composition need to be able to capture the notion of resources and resource scheduling.

- **Fault tolerance for DRE.** Dealing with emergency situations is a major part of the DRE operation. The handling of faults and other abnormal events consumes a major portion of the system development efforts and represents the vast majority of code in a system implementation. At the same time, most model-driven approaches concentrate on the functional aspects of system behavior and the nominal environment.

The papers presented at the workshop and collected in this volume discuss recent advances in addressing the above challenges, and outline directions of future research necessary to conquer them. The papers are organized into the following three groups:

- The first group addresses the problem of MDD for DRE systems. Papers in this group address model-level composition of functional and non-functional properties, as well as correctness of property-preserving model transformations that are key to the MDD process.

- The second group of papers is devoted to software engineering and analysis for component-based DRE systems.

- Finally, the last group of papers discuss component implementation and integration technologies that address the composition on a more concrete level, while making full use of modeling and software engineering approaches considered in the first two groups.
Acknowledgements

We are grateful to the Steering Committee, the Local Organizing Committee, and the invited speakers for making the workshop a success. We acknowledge generous sponsorship from the Army Research Office (David Hislop) and from the National Science Foundation (Helen Gill).

September 2007

Fabrice Kordon
Oleg Sokolsky
Organization

Executive Committee

Program Chairs
- Fabrice Kordon (Université Pierre & Marie Curie, France)
- Oleg Sokolsky (University of Pennsylvania, USA)

Local Organization
- Fabrice Kordon (Université Pierre & Marie Curie, France)

Technical Program Committee

Beatrice Berard
- Université Paris-Dauphine, France

Valdis Berzins
- Naval Postgraduate School, USA

Juan de la Puente
- Universidad Politecnica de Madrid, Spain

Gabor Karsai
- Vanderbilt University, USA

Insup Lee
- Pennsylvania University, USA

Edward Lee
- University of California at Berkeley, USA

Tom Maibaum
- King’s College, London, UK

Joseph Sifakis
- Verimag, France

Henny Sipma
- Stanford University, USA

Francois Terrier
- CEA-LIST, France
# Table of Contents

## Model Driven Development and Embedded Systems

- **On the Correctness of Model Transformations in the Development of Embedded Systems** ................................................................. 1  
  *Gabor Karsai and Anantha Narayanan*

- **Supporting System Level Design of Distributed Real Time Systems for Automotive Applications** ................................................. 19  
  *Klaus D. Müller-Glaser, Clemens Reichmann, and Markus Kuehl*

- **From MDD to Full Industrial Process: Building Distributed Real-Time Embedded Systems for the High-Integrity Domain** ........... 35  
  *Jérôme Hugues, Laurent Pautet, and Bechir Zalila*

- **Model-Based Failure Management for Distributed Reactive Systems** .... 53  
  *Vina Ermagan, Ingolf Krüger, and Massimiliano Menarini*

## Software Engineering for Embedded Systems

- **A Methodology and Supporting Tools for the Development of Component-Based Embedded Systems** ............................................ 75  
  *Marc Poulhiès, Jacques Pulou, Christophe Rippert, and Joseph Sifakis*

- **Industrial Challenges in the Composition of Embedded Systems** ..... 97  
  *David Corman and James Paunicka*

- **Deep Random Search for Efficient Model Checking of Timed Automata** ................................................................. 111  
  *Radu Grosu, Xiaowen Huang, Scott A. Smolka, Wenkai Tan, and Stavros Tripakis*

- **OASiS: A Service-Oriented Architecture for Ambient-Aware Sensor Networks** ................................................................. 125  
  *Xenofon Koutsoukos, Manish Kushwaha, Isaac Amundson, Sandeep Neema, and Janos Sztipanovits*

## Composition Technologies

- **Composing and Decomposing QoS Attributes for Distributed Real-Time Systems: Experience to Date and Hard Problems Going Forward** .... 150  
  *Richard Schantz and Joseph Loyall*
Recent Additions on the Application Programming Interface of the TMO Support Middleware ........................................ 168
  K.H. (Kane) Kim, Juan A. Colmenares, Liangchen Zheng,
  Sheng Liu, Qian Zhou, and Moon-Cheol Kim

Integrating Automotive Applications Using Overlay Networks on Top of a Time-Triggered Protocol ........................................ 187
  Roman Obermaisser

Reliability Properties of Models for Flexible Design and Run-Time Analysis ................................................................. 207
  Luqi, Valdis Berzins, and P.M. Musial

Author Index ........................................................................... 221