FACS 2007 Christmas Workshop: Formal Methods in Industry

BCS London, UK
17 December 2007

Editors:
Paul Boca
Jonathan Bowen
Peter Gorm Larsen
Abstract

This Electronic Workshop in Computing (eWiC) proceedings contains selected papers from the workshop on Formal Methods in Industry, held in London, UK, and organised under the auspices of the BCS Formal Aspects of Computing Science (FACS) Specialist Group. The workshop, organised by Paul Boca, Jonathan Bowen and Peter Gorm Larsen, was inspired by the very successful and well-attended Industry Day event at the FM05 conference. The FACS workshop dovetails well with the subsequent Industry Day at FM08, which Peter Gorm Larsen is also co-chairing.

This conference was sponsored by:

Google
BCS FACS
FM Europe
EPSRC VSR-net network
BCS Engineering Technology Forum
This Electronic Workshop in Computing (eWiC) proceedings contains selected papers from the workshop on Formal Methods in Industry [1], held in London, UK, and organized under the auspices of the BCS Formal Aspects of Computing Science (FACS) Specialist Group [2]. The workshop, organized by Paul Boca, Jonathan Bowen and Peter Gorm Larsen, was inspired by the very successful and well-attended Industry Day event at the FM05 conference [3]. The FACS workshop dovetails well with the subsequent Industry Day at FM08 [4], which Peter Gorm Larsen is also co-chairing.

The workshop attracted 50 participants, mainly from the UK and other parts of Europe; two attendees travelled nearly 6,000 miles from Japan to attend. The programme consisted of two invited contributions - one from Jim Woodcock, University of York, UK and the other from Peter Gorm Larsen, Engineering College of Aarhus, Denmark - and eight peer-reviewed papers. Tony Hoare, Microsoft, had been invited to give a talk at the workshop, but unfortunately was unwell and could not attend.

Woodcock's talk focused on the verified file store, one of the case studies in the Grand Challenges 6 initiative to produce a repository of verified software. A workshop devoted to the verified file store problem took place the day after the Christmas workshop, once again hosted by the BCS.

Larsen's talk, which was co-authored with John Fitzgerald, was more pragmatic, focusing on experiences of using VDM in Japan. In particular, uses of VDM in three projects covering different application areas were presented and compared: trading, railway, mobile chip. Larsen illustrated how VDM had benefited and continues to benefit these projects.

A number of the regular papers contained in this eWiC indicate how different formalisms (such as Communicating Sequential Processes, VDM, Event-B) and tools (such as the B-tool, FDR) can be used to model, test, improve our understanding of and reason about industrial-scale examples. There is evidence too that formal methods can be viable in industry, saving time and money if used appropriately.

The presentations from RAL and Newcastle University (NU) both deal with formal aspects of information shared across different organizations. The RAL contribution presented by Aziz focused on formalizing the security aspects of grid computing. The NU contribution presented by Fitzgerald demonstrated how information flow in virtual organizations can be validated. The presentation given by Hallerstede provided insight in the RODIN tool supporting Event-B whereas the presentation from Rezazadeh demonstrated how this tool can be used in the redevelopment of the CDIS system. Oliver demonstrated how Nokia saved 3 man months of effort using Alloy. Lawrence presented how IBM use CSP to analyse deadlocks in Java classloaders. Finally Treharne presented initial ideas of a new collaborative industrial project with AWE. Papers based on Woodcock's and O'Halloran's talks are not included in these proceedings, but their presentations can be found at the event website along with those of the other presenters:


We hope that these eWiC proceedings will be of interest to readers and will demonstrate that formal methods can be used effectively in industry.

The event was sponsored by the BCS Engineering and Technology Forum [5], Formal Methods Europe [6], FACS [2], Google [7] and the EPSRC VSR-net network [8]. The organizers would like to thank all of the sponsors for their generosity. This event could not have taken place without their
support. Finally, the organizers give a special thank you to Gemma Liddiard and Rachel Browning from the BCS for running the registration desk, printing the badges and proceedings, and ensuring that there were no problems on the day, despite a change to the venue at the very last minute!


Paul Boca
Jonathan Bowen
Peter Gorm Larsen
Editors

This conference was edited by:

Paul Boca - Programming Research Ltd, UK, Paul Boca's Webpage


Peter Gorm Larsen - Engineering College of Aarhus, Denmark, Peter Gorm Larsen's Webpage
Papers:

Benjamin Aziz, Alvaro Arenas, Juan Bicarregui, Brian Matthews, Erica Yang  A Formal Security Requirements Model for a Grid-based Operating System  
http://dx.doi.org/10.14236/ewic/FMI2007.1

Michael Butler and Stefan Hallerstede  The Rodin Formal Modelling Tool  
http://dx.doi.org/10.14236/ewic/FMI2007.2

http://dx.doi.org/10.14236/ewic/FMI2007.3

Ian Oliver  Experiences of Formal Methods in 'Conventional' Software and Systems Design  
http://dx.doi.org/10.14236/ewic/FMI2007.4

Jonathan Lawrence  Analyzing Java Classloader Deadlocks Using CSP and FDR  
http://dx.doi.org/10.14236/ewic/FMI2007.5

Abdolbaghi Rezazadeh, Neil Evans and Michael Butler  Redevelopment of an Industrial Case Study Using Event-B and Rodin  
http://dx.doi.org/10.14236/ewic/FMI2007.6

Edward Turner, Helen Treharne, Neil Evans  An overview of the SystemB collaborative project  
http://dx.doi.org/10.14236/ewic/FMI2007.7

Peter Gorm Larsen and John Fitzgerald  Recent Industrial Applications of VDM in Japan  
http://dx.doi.org/10.14236/ewic/FMI2007.8