FMICS'05

Proceedings of the

Tenth International Workshop on Formal Methods for Industrial Critical Systems

September 5-6, 2005 • Lisbon, Portugal
Co-located with ESEC/FSE'05

Editors

Tiziana Margaria & Mieke Massink

Sponsored by

ACM SIGSOFT

The Association for Computing Machinery
1515 Broadway
New York, New York 10036

ISBN: 1-59593-148-1

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 11405
New York, NY 10286-1405

Phone: 1-800-342-6626
(US and Canada)
+1-212-626-0500
(all other countries)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org

ACM Order Number 592055
Printed in the USA

Foreword

This 10th edition of the *International Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, a series of workshops organised by the homonimous ERCIM Working Group, is a good occasion for re-examining ten years of best practises of the use of formal methods in industry and to outline a promising way forward for the next decade. Since ten years the FMICS workshops strive to promote research on and support the improvement of formal methods and tools for industrial critical applications. They are meant to provide a common forum for the exchange of experiences of scientists as well as industrial professionals that are involved in the development and application of formal methods for industrial applications. The FMICS Working Group has achieved a broad public visibility and actively aims at interaction with the wider scientific community.The ERCIM board of directors recognised these merits and granted the FMICS Working Group the ERCIM award for the most successful Working Group of 2002.

Previous workshops were held in Oxford (March 1996), Cesena (July 1997), Amsterdam (May 1998), Trento (July 1999), Berlin (April 2000), Paris (July 2000), Malaga (July 2002), Trondheim (July 2003) and Linz (September 2004). This year the FMICS workshop is co-located with the European Software Engineering Conference (ESEC) and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE) which are an internationally renowned forum for researchers, practitioners and educators in the field of software engineering and which is held in the beautiful city of Lisbon in Portugal.

Fourteen contributions have been selected, out of 27 good quality submissions, covering both industrially relevant theoretical topics as well as industrial case studies.

We are also pleased to welcome two invited speakers:

- Luis Andrade from ATX Software SA, Lisbon, who gives a presentation on the experience of ATX with the application of formal and rigorous techniques and methods in real projects, and
- Christel Baier from the University of Bonn, who gives a presentation on the most recent developments on the quantitative analysis of distributed randomized protocols.

On occasion of the tenth edition of the workshop a special session has been arranged for the presentation of the follow-up of the much cited and widely discussed *article*

- *"Ten Commandments of Formal Methods"* by Jonathan P. Bowen and Michael G. Hinchey

which was published ten years ago. Both authors join the workshop to present a ten-year perspective on the industrial application of formal methods and set the stage for another lively discussion on the way ahead for formal methods for industry in the decade to come. We are very happy that both authors chose the FMICS workshop as the forum where to present their new ideas. A best paper award will be granted also this year with the support of the European Association of Software Science and Technology (EASST).

We thank all the members of the programme committee and all the additional referees for their careful and timely evaluation of the submitted papers. We are also grateful to the organisers of the ESEC/FSE conference for hosting our workshop and taking care of many organisational aspects, to ACM SIGSOFT for their sponsorship and ERCIM for its financial support of the workshop. Additionally, we thank EASST (European Association of Software Science and Technology), ATX Software, and our home institutions CNR-ISTI and the University of Göttingen for their support to this event.

We hope that you will find this program interesting and thought-provoking and that the symposium will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

Tiziana Margaria
Universität Göttingen
FMICS'05 Co-Chair

Mieke Massink
CNR-ISTI
FMICS'05 Co-Chair

Table of Contents

FMICS 2005 Workshop Organization

Co-Chairs: Tiziana Margaria *(Universität Göttingen, Germany)*
Mieke Massink *(CNR-ISTI, Italy)*

Program Committee: Alvaro Arenas *(CCLRC/RAL, UK)*
Lubos Brim *(Masaryk Univ. CZ)*
Andrew Butterfield *(Dublin Univ., IRL)*
Marsha Chechik *(Univ. of Toronto, CAN)*
Alessandro Fantechi *(Univ. of Florence, IT)*
Mike Hinchey *(NASA GSFC, US)*
Leszek Holenderski *(Philips, NL)*
Michaela Huhn *(Clausthal Tech. Univ., D)*
Hardi Hungar *(Univ. Oldenburg, D)*
Diego Latella *(CNR/ISTI Pisa, I)*
Radu Mateescu *(INRIA Rhone-Alpes, F)*
Jaco van de Pol *(CWI, NL)*
Ina Schieferdecker *(Fraunhofer FOKUS, D)*

Additional reviewers: Michele Banci
Maurice ter Beek
Juan Bicarregui
Bastian Florentz
Julian Gallop
Stefania Gnesi
Denis Gracanin
Arie Gurfinkel
Gabriele Lenzini
Giovanni Mainetto
Brian Matthews
Franco Mazzanti
Tilo Mücke
Emilio Spinicci

Sponsor:

ACM Special Interest Group on
Software Engineering

Supporters:

Council of European Professional
Informatics Societies

CNR-ISTI Institute for Computer
Science and Technology

Universität Göttingen