Preface

This volume contains the contributions presented at the *International Workshop on Current Trends in Applied Formal Methods* organized October 7-9, 1998, in Boppard, Germany.

The main objective of the workshop was to draw a map of the key issues facing the practical application of formal methods in industry. This appears to be particularly timely with safety and security issues becoming a real obstacle to industrial software and hardware development. As a consequence, almost all major companies have now set up departments or groups to work with formal methods and many European countries face a severe labour shortage in this new field. Tony Hoare's prediction of the art of software (and hardware) development becoming a proper engineering science with its own body of tools and techniques is now becoming a reality.

So the focus of this application oriented workshop was not so much on special academic topics but rather on the many practical aspects of this emerging new technology: verification and validation, and tool support and integration into the software life-cycle. By evaluating the state of the art with respect to industrial applications a discussion emerged among scientists, practising engineers, and members of regulatory and funding agencies about future needs and developments. This discussion lead to roadmaps with respect to the future of this field, to tool support, and potential application areas and promising market segments. The contributions of the participants from industry as well as from the respective national security bureaus were particularly valuable and highly appreciated.

The workshop program included four invited talks, 16 talks selected by the program committee, and six talks given during the application day. Apart from the regular papers, the proceedings contain two invited contributions by Egon Börger and Manfred Broy, three application papers, and eight tool papers.

Egon Börger gives a new comprehensive introduction to Abstract State Machines describing their use in the different design stages of software systems. Manfred Broy and Oscar Slotosch present a process model for the integration of formal methods into conventional software engineering. They discuss the mediating role of user-oriented description techniques. Contributions presented at the application day cover industrial applications of model-checking (an excellent survey of current industrial practice was presented in the invited talk by Wolfram Büttner, SIEMENS), hardware-design (paper by Masahiro Fujita, Sree P. Rajan, and Alan Hu), safety critical control systems (paper by Meine van der Meulen and Tim Clement), and security engineering (paper by Frank Koob, Markus Ullmann, and Stefan Wittmann, BSI). The tool papers provide a collection of the major current systems.

October 1998 Jörg H. Siekmann

Welcome Note

I welcome you cordially on behalf of the Federal Minister of the Interior and the Federal IT Security Agency at this international workshop, and I extend a special welcome to the many foreign guests and the invited speakers of the conference.

To look into the future and identify technological trends is a challenge that raises many questions. If one considers IT development in general, one comes to the conclusion that it is not unusual to talk about and handle technologies that have existed for fewer than 5 years now. Java and the World Wide Web are two illustrative examples. Their development and distribution is taking place at a breathtaking speed. I do not think that anybody would have predicted that these phenomena would take on such dimensions.

At the moment, technical systems in a wide range of fields are becoming ever more complex. Computer failures (breaking of access codes, T-online) and accidents (plane crashes, train disasters) arouse a latent feeling in society that technical systems are no longer fully controllable. The impression arises that against this background security will increasingly have to be discussed in its entirety, and that new promising procedures will have to be applied. We expect that it will be possible to achieve major improvements in terms of quality and security through *Formal Methods* (FM) in the field of software and hardware systems.

Yet new technologies alone are not enough. Those who make the laws must take action, too, in order to ensure that the technologies promising a higher level of security are used appropriately, and are not sacrificed for short-term economic profit. A high-level information technical security infrastructure is essential to ensure confidence in the flow of information on the data highways and acceptance of new technologies in politics, the economy, and society. The Digital Signature Act and Ordinance as well as the related detailed technical specifications have now created a basis in Germany for the development of a uniform security infrastructure. The high certification level of the components to be used means that the use of FM for digital signature components that comply with the law is mandatory.

The aim of the workshop, which starts today here at the Federal Academy, is, on the one hand, to provide information about current developments of IT, and to discuss and possibly orientate them towards the requirements of industry. On the other hand, you will exchange experience regarding the use of FM during the Application Day and thus encourage industrial companies to use FM in order to make a contribution to increasing security and safety.

I wish the workshop the best of success, which I combine with the hope that the workshop will give a clear signal for a wider applicability of formal methods.

October 1998

MinR Norbert Vogt
German Federal Ministry of the Interior

Workshop Organization

The *International Workshop on Current Trends in Applied formal Methods* (FM-Trends 98) was organized jointly by the DFKI GmbH (Deutsches Forschungszentrum für Künstliche Intelligenz, Saarbrücken), the BSI (Bundesamt für Sicherheit in der Informationstechnik, Bonn), the JRC (Joint Research Centre of the European Commission, Ispra) and the IRST (Istituto per la Ricerca Scientifica e Tecnologica, Trento).

Workshop Committee

F. Giunchiglia(Trento)
D. Hutter (Saarbrücken)
F. Koob (Bonn)
J.H. Siekmann (Saarbrücken)
W. Stephan (Saarbrücken)
P. Traverso (Trento)
M. Ullmann (Bonn)
H.P. Wagner (Bonn)
M. Wilikens (Ispra)

Advisory Board

E. Astesiano, (Genova)
K.R. Apt, (Amsterdam)
J. Bergstra, (Amsterdam)
V. Berzins, (Monterey)
D. Bjorner, (Lyngby, Denmark)
R. Bloomfield, (Adelard)
J. Bowen, (Berkshire)
B. Boyer, (Texas)
M. Broy, (Munich)
A. Bundy, (Edinburgh)
E. Clarke, (CMU, USA)
W. Damm, (Oldenburg)
J.W. de Bakker, (Amsterdam)
W.P. de Roever, (Kiel)
H.D. Ehrich, (Braunschweig)
E.A. Emerson, (Texas)
H. Ganzinger, (Saarbrücken)
M.C. Gaudel, (Paris)
J. Goguen, (Monterey)
D. Gries, (Ithaca, New York)
Y. Gurevich, (Michigan)
D. Harel, (Rehovot, Israel)
T. Henzinger, (Berkeley)
M. Hinchey, (New Jersey)
C.A.R. Hoare, (Oxford)
D. Howe, (Bell Labs, USA)
N. Jones, (Copenhagen)
D. Kapur, (New York)
H. Kirchner, (Rocquencourt, France)
H. Langmaack, (Kiel)
T. Maibaum, (London)
U. Martin, (St. Andrews)
U. Montanari, (Pisa)
J S. Moore, (Texas)
T. Nipkow, (Munich)
D. Parnas, (Hamilton)
L. Paulson, (Cambridge)
A. Ravn, (Lyngby, Denmark)
A. W. Roscoe, (Oxford)
J. Sifakis, (Paris)

External Referees

Massimo Benerecetti
Piergiorgio Bertoli
Alessandro Cimatti
Marco Daniele
Dominique Mery
Olaf Müller
Marco Roveri
Roberto Sebastiani
Oscar Slotosch
Adolfo Villafiorita

Acknowledgements

All submitted papers were refereed by advisory board members, workshop organizers, and external referees. This workshop would not have been possible without their voluntary and dedicated work.