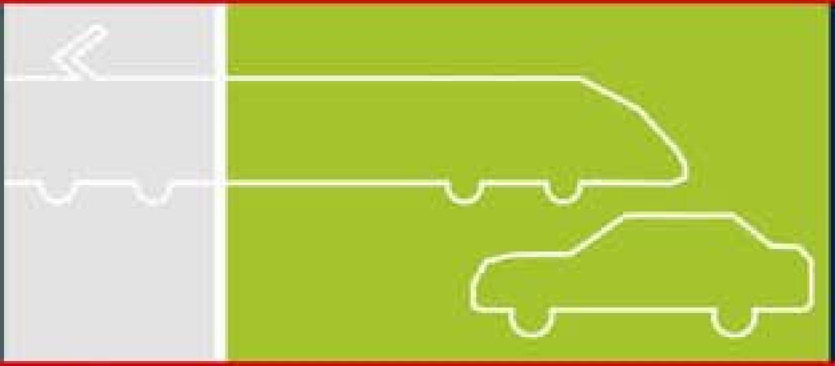
Eckehard Schnieder
Géza Tarnai
Editors



FORMS/FORMAT 2010

Formal Methods for Automation and Safety in Railway and Automotive Systems

Springer

FORMS/FORMAT 2010

Eckehard Schnieder · Géza Tarnai
Editors

FORMS/FORMAT 2010

Formal Methods for Automation and Safety in Railway and Automotive Systems

Springer

Editors

Eckehard Schnieder
Technische Universität Braunschweig
Institute for Traffic Safety
and Automation Engineering
Langer Kamp 8
D-38106 Braunschweig
Germany
e.schnieder@tu-braunschweig.de

Géza Tarnai
Budapest University of Technology
and Economics
Department of Control
and Transport Automation
Bertalan L. u. 2.
H-1111 Budapest
Hungary
tarnai.geza@mail.bme.hu

ISBN 978-3-642-14260-4 e-ISBN 978-3-642-14261-1
DOI 10.1007/978-3-642-14261-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011921311

Cover design: WMXDesign GmbH, Heidelberg

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Coping with the complexity of advanced automation- and safety systems both in railway and automotive applications will be more and more dominated by the use of formal means of description, formal methods, and tools. Altogether named Formal Techniques they provide next to the correctness and integrity checkups – especially in safety relevant systems – the possibility to prove the syntactic and semantic specification of the system as well as to simulate the system operation.

Formal methods – a comprehensive form for means of description and adjacent methodological concepts – gained by advanced and more and more professional tools supported by powerful computer technology emerge currently and find their benefits to lots of applications. Primarily, their promising power of clear description and symbolic patterns for modelling the real world including technological devices and human operators offers the chance for engineers to build up systems which can be designed in a correct way. With the quality of mathematical proofs they provide guaranteed conditions of dependability, the comprehensive term for availability, reliability, maintainability and safety and furthermore security, short RAMSS. In transportation, a high demand for RAMSS exists, especially under new European directives, regulation authorities, and standards on the one hand as well as expectations from the users' and operators' side on the other.

Requirements of the recently updated legal framework expressed by EU-Guidelines, IEC- and CENELEC-standards and establishing standards for automotive software which are based on formal techniques, particularly with regard to the handling of safety analysis, are to be treated in FORMS/FORMAT 2010. The main focus lies on topics facing formal techniques for railway applications and intelligent transportation systems as well as for automotive applications. Gained findings, experiences and also difficulties associated with the handling of the subject matter are to be shown.

Hence the meanwhile 8th Symposium of FORMS / FORMAT and its subtitle "Formal Methods for Automation and Safety in Railway and Automotive Systems" fully cover the broad joint approach for this challenging topic. Since transportation in its whole can profit from this theoretical approach for formal methods, the scope inside transportation has expanded for railway and road transportation, mainly tackled jointly by methodological approaches.

Supervised by an internationally highly ranked experts' program committee from America, Asia, and Europe some twenty contributions have been selected very critically for oral presentation and to be published in the proceedings of the 2010 symposium. The symposium will be framed by invited contributions by internationally leading experts from operators, assessors, and science.

The first part of the program starts with contributions about three different aspects of RAMSS. The first session covers both safety and security and their policy for application in the transportation domain. It is followed by the increasing influence of maintenance to operations and ends with its methods for evaluation and analysis of essential functions of railway operations systems as well as its infrastructure and vehicles.

The second part of the program covers general aspects. Beginning with remarks on legal framework and risk metrics, it is followed by methods for the development and simulation in the automotive domain. Theoretical contributions about the verification of programmable logic controllers (PLC) which become more and more attractive for the control in transportation together with tool chains for testing and development conclude the program.

The current proceedings include the papers of these different sessions of the Symposium FORMS/FORMAT 2010, which present novel research and practical results that have been reached since the previous symposium.

We would like to acknowledge the contribution of every attendant and the support of the program committee, and we hope for a prospering future of our common activity and also to widen the sphere of users again. We are convinced that our symposium will provide an invisible but nevertheless important contribution to safe transportation.

The editors thank all authors for their support, especially Geltmar von Buxhoeveden for his careful preparation of the symposium, and Springer Verlag for publishing the proceedings.

December 2010

Eckehard Schnieder, Géza Tarnai
Program Chairs
FORMS/FORMAT 2010

Conference Organization

Programme Chairs

Eckehard Schnieder, Géza Tarnai

Programme Committee

Marc Antoni	SNCF (F)
Joachim Axmann	Volkswagen AG (D)
Jens Braband	Siemens AG (D)
Henning Butz	Airbus Deutschland (D)
Werner Damm	Carl von Ossietzky Universität Oldenburg (D)
El-Miloudi El-Koursi	INRETS Lille (F)
Alessandro Fantechi	Università degli Studi di Firenze (I)
Martin Fränzle	Carl von Ossietzky Universität Oldenburg (D)
Peter Göhner	Universität Stuttgart (D)
Shigeto Hiraguri	RTRI - Railway Technical Research Institute (J)
Yuji Hirao	Nagaoka University of Technology (J)
Aleš Janota	University of Žilina (SK)
Karsten Lemmer	DLR Braunschweig (D)
István Majzik	Budapest University (HU)
Bin Ning	Beijing Jiaotong University (CN)
Jörn Pachl	Technische Universität Braunschweig (D)
Markos Papageorgiou	Technical University of Crete (GR)
Stefano Ricci	Università di Roma (I)
Bastian Schlich	RWTH Aachen (D)
Holger Schlingloff	Humboldt-Universität Berlin (D)
Roman Slovák	BAV - Bundesamt für Verkehr (CH)
Olaf Stursberg	Universität Kassel (D)
Aníbal Zanini	Universidad de Buenos Aires (AR)

Local Organization

Geltmar von Buxhoeveden, Christian Cholewa, Güler Gülec, Sylvia Glowania, Christine Jendritzka, Sofia Mouratidis, Sarah-Romina Pesenecker, Felix Reinbold, Arno G. Schielke, Sven Schulze, Nadine Schwarz, Andreas Siepmann, Akbar Shah, Regine Stegemann, Kevin Wieloch

External Reviewers

Lars Ebrecht, Matthias Grimm, Malte Hammerl, Christian Herde, Katrin Lüddecke, Michael Meyer zu Hörste, Markus Pelz

Table of Contents