Integration of Software Specification Techniques for Applications in Engineering

Priority Program SoftSpez of the German Research Foundation (DFG) Final Report
Preface

This volume is a documentation of the main results in the research area “Integration of Software Specification Techniques for Applications in Engineering”. On one hand it is based on the Priority Program “Integration von Techniken der Softwarespezifikation für ingenieurwissenschaftliche Anwendungen”, short Soft-Spez, of the German Research Council (DFG). On the other hand it contains new contributions of international experts in this research area, some of which were presented at the third international workshop INT 2004 on “Integration of Specification Techniques for Applications in Engineering”. INT 2004 was launched as a satellite event of ETAPS in Barcelona, the “European Joint Conferences on Theory and Practice of Software”.

The Priority Program SoftSpez was initiated by W. Brauer, M. Broy, H. Ehrig, H.J. Kreowski, H. Reichel, and H. Weber concerning different aspects from computer science, and by E. Schnieder and E. Westkämper concerning two main application areas in engineering, namely “Traffic Control Systems” and “Production Automation”. After acceptance of SoftSpez by the German Research Council for the period of 1998–2004 a call for specific projects within this priority program was launched, where 11 projects from about 75 project proposals were accepted for a period of two years. Since 1998 each year the main research proposals and results of the projects have been presented at an annual colloquium of the priority program, and every two years the projects have been evaluated by an independent group of referees appointed by the German Research Council. At this point we would like to thank A. Engelke and G. Sonntag, the responsible officers from the DFG, the group of referees, with chairman W. Brauer, and our colleagues mentioned above for setting up the initial proposal for SoftSpez.

The cooperation between the projects was organized into different subject areas, with several meetings since 1999. In addition to the annual colloquia and the subject area meetings on a national level, also three international workshops were organized by SoftSpez. The workshops INT 2000, 2002, and 2004 were launched in cooperation with the ETAPS conferences in order to present the concepts and results of SoftSpez to the international scientific community and to get feedback from international experts.

The contributions in this volume are organized according to the six different subject areas of SoftSpez, where the coordinators for the subject areas are the coeditors for the corresponding parts of this volume. All papers were carefully reviewed by national and international experts.

In addition to a general introduction to the research area of this volume there are also introductions for each subject area. They present an overview and a short introduction into each paper of the corresponding subject area, including contributions from the projects of SoftSpez and papers from international (non-German) experts in this area.
The organization of the priority program SoftSpez and of the six subject areas was coordinated during the program and for this documentation by the editor and the coeditors of this volume, respectively. For great support we would like to thank the following researchers of the project: M. Bengel, A. Braatz, B. Braatz, R. Geisler, H.M. Hanisch, L. Jansen, G. Juhás, M. Klar, M. Klein, J. Klose, R. Lorenz, G. Saake, Ch. Schaeffer, G. Schellhorn, G. Schröter, R. Slovak, A. Thums, and B. Westphal.

Finally let us thank all national and international reviewers and authors of the papers in this volume and Springer for a smooth publication.

We hope that this volume offers new insights and suggests new research topics and applications in various related areas of computer science and engineering.

July 2004

Hartmut Ehrig
Werner Damm
Jörg Desel
Martin Große-Rhode
Wolfgang Reif
Eckehard Schnieder
Engelbert Westkämper
# Table of Contents

Integration of Software Specification Techniques for Applications in Engineering: Introduction and Overview of Results .......................... 1
   *Hartmut Ehrig*

## Part I: Reference Case Study Production Automation

*Coordinator: Engelbert Westkämper*

- Basic Principles for Software Specification – Introduction to Subject Area Reference Case Study Production Automation .......... 9
  *Engelbert Westkämper, Matthias Bengel, Katja Fischer*

- Challenges of Next Generation Manufacturing Systems ................. 23
  *Paul Valckenaers*

- Development of Hierarchical Broadcasting Software Architectures Using UML 2.0 .................................................... 29
  *Ingolf Krüger, Wolfgang Prenninger, Robert Sandner, Manfred Broy*

- An Engineer’s Workstation to Support Integrated Development of Flexible Production Control Systems .......................... 48
  *Wilhelm Schäfer, Robert Wagner, Jürgen Gausemeier, Raimund Eckes*

- A Formal Component Concept for the Specification of Industrial Control Systems ....................................................... 69
  *Benjamin Braatz, Markus Klein, Gunnar Schröter, Matthias Bengel*

## Part II: Reference Case Study Traffic Control Systems

*Coordinator: Eckehard Schnieder*

- Specification Methodology, Case Studies, and Experiments – An Introduction to the Subject Area of Traffic Control Systems .......... 89
  *Eckehard Schnieder*

- Reference Case Study “Traffic Control Systems” for Comparison and Validation of Formal Specifications Using a Railway Model Demonstrator ............................................... 96
  *Frank Hänsel, Jan Poliak, Roman Slovák, Eckehard Schnieder*
## Table of Contents

### Part III: Petri Nets and Related Approaches in Engineering

**Coordinator: Jörg Desel**

**Process Description Languages and Methods:**

**Introduction to the Chapter**

*Petri Nets and Related Approaches in Engineering* ........................................ 199

*Jörg Desel*

**Specification and Formal Verification of Temporal Properties**

of Production Automation Systems ......................................................... 206

*Stephan Flake, Wolfgang Müller, Ulrich Pape, Jürgen Ruf*

**STOP – Specification Technique of Operational Processes** ................. 227

*Stefan Einer*

**Specification and Validation of an Edge Router Discovery Protocol**

for Mobile Ad Hoc Networks ................................................................. 248

*Lars Michael Kristensen, Kurt Jensen*

**A Guide to Modelling and Control with Modules of Signal Nets** .......... 270

*Jörg Desel, Hans-Michael Hanisch, Gabriel Juhás, Robert Lorenz, Christian Neumair*

**Conceptual Design of an Engineering Model**

for Product and Plant Automation .......................................................... 301

*K. Fischer, P. Göhner, F. Gutbrodt, U. Katzke, B. Vogel-Heuser*

### Part IV: Charts

**Coordinator: Werner Damm**

**Introduction to Subject Area “Charts”** .............................................. 322

*Werner Damm, Bernd Westphal*
# Table of Contents

**The Rhapsody Semantics of Statecharts** ........................................ 325  
*David Harel, Hillel Kugler*

**Interactive Verification of Statecharts** ........................................ 355  
*Andreas Thums, Gerhard Schellhorn, Frank Ortmeier, Wolfgang Reif*

**Live Sequence Charts** .................................................................. 374  
*Matthias Brill, Werner Damm, Jochen Klose, Bernd Westphal, Hartmut Wittke*

**A Unifying Semantics for Sequential Function Charts** ..................... 400  
*Nanette Bauer, Ralf Huuck, Ben Lukoschus, Sebastian Engell*

## Part V: Verification

*Coordinator: Wolfgang Reif*

**Introduction to Subject Area “Verification”** .................................. 419  
*Frank Ortmeier, Wolfgang Reif, Gerhard Schellhorn*

**“UML–ising” Formal Techniques** .................................................. 423  
*Dines Bjørner, Chris W. George, Anne E. Haxthausen, Christian Krog Madsen, Steffen Holmslykke, Martin Pěnička*

**Model Based Formal Verification of Distributed Production Control Systems** .................................................. 451  
*Martin Kardos, Franz-J. Rammig*

**Combining Formal Methods and Safety Analysis – The ForMoSA Approach** ................................................................. 474  
*Frank Ortmeier, Andreas Thums, Gerhard Schellhorn, Wolfgang Reif*

**Formal Verification of LSCs in the Development Process** ............ 494  
*Matthias Brill, Ralf Buschermöhle, Werner Damm, Jochen Klose, Bernd Westphal, Hartmut Wittke*

**Verification of PLC Programs Given as Sequential Function Charts**  517  
*Nanette Bauer, Sebastian Engell, Ralf Huuck, Sven Lohmann, Ben Lukoschus, Manuel Remelhe, Olaf Stursberg*

**Modeling and Formal Verification of Production Automation Systems**  541  
*Jürgen Ruf, Roland J. Weiss, Thomas Kropf, Wolfgang Rosenstiel*
Part VI: Integration Modeling

Coordinator: Martin Große-Rhode

On Model Integration and Integration Modelling –
Introduction to the Subject Area Integration Modelling .......................... 567
  Martin Große-Rhode

On the Integration of Modular Heterogeneous Specifications ............... 582
  Fernando Orejas, Elvira Pino

Semantical Integration
of Object-Oriented Viewpoint Specification Techniques ........................ 602
  Benjamin Braatz, Markus Klein, Gunnar Schröter

Author Index ......................................................................................... 627