

Lecture Notes in Computer Science

1165

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Jean-Raymond Abrial Egon Börger
Hans Langmaack (Eds.)

Formal Methods for Industrial Applications

Specifying and Programming
the Steam Boiler Control



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Jean-Raymond Abrial

26, Rue des Plantes, F-75014 Paris, France

Egon Börger

Dipartimento di Informatica, Università di Pisa

Corso Italia 40, I-56125 Pisa, Italy

Hans Langmaack

Institut für Informatik und Praktische Mathematik, Universität Kiel

Preusserstr. 1-9, D-24105 Kiel, Germany

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal methods for industrial applications : specifying and programming the steam boiler control / Jean-Raymond Abrial ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996

(Lecture notes in computer science ; Vol. 1165)

ISBN 3-540-61929-1

NE: Abrial, Jean-Raymond [Hrsg.]; GT

CR Subject Classification (1991): D.1, D.2, D.3.1, F.3.1, K.6, C.2.4

ISSN 0302-9743

ISBN 3-540-61929-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10549218 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This book is the result of the collaborative effort of many persons and institutions, willing to contribute to a solution of the problem of finding means for a realistic evaluation of the practicality of formal methods for usage under industrial constraints. We would like to thank them all and will name them individually, in the chronological order of the help obtained.

We thank Schloß Dagstuhl for the opportunity to organize the workshop “Methods for Semantics and Specification” in June 1995, which was the starting point for our enterprise.

We thank Lt.-Col. J. C. Bauer from the Institute for Risk Research of the University of Waterloo, Ontario, Canada, for allowing us to use and modify his steam-boiler problem description for our own problem formulation, which was the basis for the specification competition reported in this book. We also thank the Institut de Protection et de Sureté Nucléaire, Fontenay-aux-Roses, France, through which we obtained J. C. Bauer’s text.

We thank Annette Lötzbeyer for the Karlsruhe steam-boiler simulator which allowed the participants to run and test their steam-boiler implementations through the internet.

We thank the authors of the submitted solutions for having accepted the challenge to work on a concrete, non-trivial, and non-academic specification problem coming from an application domain, and in particular for participating under the condition that during the whole competition period the full documentation of all the contributions be completely open to everybody who wanted to participate in the comparison effort.

We thank the participants of the Dagstuhl workshop for their open criticism in a friendly atmosphere which helped considerably to bring researchers from different communities together for a fruitful exchange of ideas.

We thank Martin Fränzle for the creation and maintenance of the steam-boiler [www](#) site at the University of Kiel, which made the transparency of the competition possible and added a world-wide dimension to the comparative research effort reported in this book. We thank Martin Fränzle also for his valuable technical assistance during the preparation of this volume.

We thank the following reviewers for their detailed study, in a relatively short period of time, of the 33 steam-boiler problem solutions submitted for this book: Sten Agerholm, Christoph Beierle, Jonathan Bowen, Reinhard Budde, Holger Busch, Jorge Cuellar, Werner Damm, Igor Đurđanović, Martin Fränzle, Uwe Glässer, Mats Heimdahl, Friedrich von Henke, Tom Henzinger, Mike Hinchey, Leszek Holenderski, Jozef Hooman, Martin Huber, Klaus Indermark, Burghard von Karger, Christoph Kreitz, Peter Gorm Larsen, Thomas Lindner, Peter Lucas, Andrea Masini, Jose Meseguer, Tobias Nipkow, Peter Päppinghaus, Anders P. Ravn, Elvinia Riccobene, Hans Rischel, Peter Ryan, Michael Schenke, Fritz

Vogt, Isolde Wildgruber, Thomas Wilke, Martin Wirsing, Howard Wong-Toi, Wolf Zimmermann.

We thank Springer-Verlag, the editors of the LNCS, and in particular Alfred Hofmann from Springer-Verlag for publishing this book in the series and for offering the experiment of the first LNCS volume to come out with a CD annex containing full details of all the contributions, including the executable programs and their documentation which could not be reported in print.

Our thanks also go to Vicky Hartonas-Garmhausen for commenting on the introduction.

We are confident that the collaborative effort of the persons and institutions cited above will be rewarded by the positive contribution the material presented in this book will make to the discussion on the use of formal methods in practical applications.

September 1996

Jean-Raymond Abrial
Egon Börger
Hans Langmaack

Table of Contents

ABL: The Steam Boiler Case Study: Competition of Formal Program Specification and Development Methods	1
<i>Jean-Raymond Abrial, Egon Börger, Hans Langmaack</i>	
AT: Structural Synthesis of Programs from Refined User Requirements (Programming Boiler Control in NUT)	13
<i>Mattin Addibpour, Enn Tyugu</i>	
AL: Using FOCUS, LUSTRE, and Probability Theory for the Design of a Reliable Control Program	35
<i>Christoph Andriessens, Thomas Lindner</i>	
BBDGR: Refining Abstract Machine Specifications of the Steam Boiler Control to Well Documented Executable Code	52
<i>Christoph Beierle, Egon Börger, Igor Đurđanović, Uwe Glässer, Elvinia Riccobene</i>	
BCPR: An Algebraic Specification of the Steam-Boiler Control System ..	79
<i>Michel Bidoit, Claude Chevenier, Christine Pellen, Jérôme Ryckbosch</i>	
BW: A Steam-Boiler Control Specification with Statecharts and Z	109
<i>Robert Büssow, Matthias Weber</i>	
BSS: An Action System Approach to the Steam Boiler Problem	129
<i>Michael Butler, Emil Sekerinski, Kaisa Sere</i>	
CD: The Steam-Boiler Problem in Lustre	149
<i>Thierry Cattel, Gregory Duval</i>	
CW1: The Steam Boiler Problem - A TLT Solution	165
<i>Jorge Cuéllar, Isolde Wildgruber</i>	
CW2: The Real-Time Behavior of the Steam Boiler	184
<i>Jorge Cuéllar, Isolde Wildgruber</i>	
DC: Specifying and Verifying the Steam-Boiler Problem with SPIN	203
<i>Gregory Duval, Thierry Cattel</i>	
GM: TRIO Specification of a Steam Boiler Controller	218
<i>Angelo Gargantini, Angelo Morzenti</i>	
GDK: A Formal Specification of the Steam-Boiler Control Problem by Algebraic Specifications with Implicit State	233
<i>Marie-Claude Gaudel, Pierre Dauchy, Carole Khouiry</i>	

HW: Using HyTech to Synthesize Control Parameters for a Steam Boiler .	265
<i>Thomas A. Henzinger, Howard Wong-Toi</i>	
LP: A VDM Specification of the Steam-Boiler Problem	283
<i>Yves Ledru, Marie-Laure Potet</i>	
LL: Proving Safety Properties of the Steam Boiler Controller	318
<i>Gunter Leeb, Nancy Lynch</i>	
LM: Steam Boiler Control Specification Problem: A TLA Solution	339
<i>Frank Lesske, Stephan Merz</i>	
LW: Specifying Optimal Design of a Steam-Boiler System	359
<i>Li XiaoShan, Wang JuAn</i>	
OKW: An Object-Oriented Algebraic Steam-Boiler Control Specification .	379
<i>Peter Csaba Ölveczky, Piotr Kosiuczenko, Martin Wirsing</i>	
SR: Refinement from a Control Problem to Programs	403
<i>Michael Schenke, Anders P. Ravn</i>	
S: VDM Specification of the Steam-Boiler Control Using RSL Notation ..	428
<i>Christian P. Schinagl</i>	
VH: Assertional Specification and Verification Using PVS of the Steam Boiler Control System	453
<i>Jan Vitt, Jozef Hooman</i>	
WS: Specifying and Verifying the Steam-Boiler Control System with Time Extended LOTOS	473
<i>Andreas Willig, Ina Schieferdecker</i>	
L: Simulation of a Steam-Boiler	493
<i>Annette Lötzbeyer</i>	
A: Steam-Boiler Control Specification Problem	500
<i>Jean-Raymond Abrial</i>	
Author Index	511