

Formal Specifications of Computer-Based Systems

Miroslav Sveda
Brno University of Technology
Czech Republic
sveda@fit.vutbr.cz

Charles Rattray
University of Stirling
Scotland
cr@cs.stir.ac.uk

Jerzy Rozenblit
University of Arizona
Tucson, Arizona
jr@ece.arizona.edu

Origins

The IFIP TC10 Working Group 10.1 "Computer Aided Systems Theory" Committee Meeting at the Vienna University of Technology on the 30th September 1999, resulted in a resolution to support a joint workshop with the IEEE Computer Society TC-ECBS on *Formal Specifications of Computer-Based Systems* (FS CBS). Owing to a substantial overlap in this research domain, Franz Pichler, the founder of the IFIP WG10.1, and Charles Rattray, the IFIP WG10.1 chair, delegated Miroslav Sveda, a member of both WG10.1 and TC-ECBS, to act as a contact person in this activity.

The ECBS Executive Committee has welcomed and greatly supported the initiation and implementation of the IEEE/IFIP Joint Workshops on FS CBS as *Formal Specifications Working Group Sessions* following annual ECBS Conferences.

1st Joint Workshop 2000

The first IEEE/IFIP Joint Workshop on Formal Specifications of Computer-Based Systems, sponsored by both IEEE TC-ECBS and IFIP WG10.1, has been organized by Miroslav Sveda and Charles Rattray and held in Edinburgh, Scotland, 6-7 April 2000. It created a forum for researchers and practitioners from industry and academia, in which discussions focused on completed work as well as work-in-progress related to FS CBS.

The following seventeen accepted contributions were published in the Workshop Proceedings 2000 [1] and presented at the workshop.

Y. Dong, S. A. Smolka, E.W. Stark, S. White: Practical Considerations in Protocol Verification: The E-2C Case Study

G. Karsai: Towards two-level Formal Modeling of Computer-Based Systems

D. Beyer, H. Rust: Modular Modelling and Verification with Cottbus Timed Automata

S. Maharaj, C. Shankland: A Survey of Formal Methods applied to IEEE 1394

I. Traore: An Outline of PVS Semantics for UML Statecharts

R.G. Clark: Use of E-LOTOS in Adding Formality to UML

J. Mullins: Non-deterministic Admissible Interference

W. Kuchlin: Hardware Representation Using Gröbner Bases

T. Kelsey: Formal Specification of Computer Algebra

J.R. Blow, A.J. Galloway, J.A. McDermid, M.G. Dowding, T.J. Cockram: The Industrial Use of a Formal Method in a Gas Turbine Engine Electronic Control System

N.J. Rizk: Irregular Problem Design under BSP Model

A. Fuchs, J. Kreslikova: Toward a Unified Formal Models of CBS

L. Allain, P. Yim: Modeling Information System Behavior with Dynamic Relation Nets

M. Urbasek, M. Ceska: Reasoning about Categories of Petri Nets

P. Matousek, J. Rab, P. Vysek: Protocol Proving and Model Checking

M. Jankovsky, M. Sveda: From TLA Specifications to Real-Time Unix Applications

M. Sveda, R. Vrba: Executable Specifications for Embedded Distributed Systems

2nd Joint Workshop 2001

The second IEEE/IFIP Joint Workshop on Formal Specifications of Computer-Based Systems, sponsored by both IEEE TC-ECBS and IFIP WG10.1, has been organized by Charles Rattray, Miroslav Sveda and Jerzy Rozenblit and held in Washington, D.C., 20 April 2001. The following 21 accepted contributions were published in the Workshop Proceedings 2001 [2] and presented at the workshop.

P. Alexander, C. Kong: Heterogeneous Computer-Based System Specification

S. Einer, A. Grau: Integrating Petri Nets and TROLL in the Modeling of Engineering Systems

A. Ledeczi, G. Nordstrom, G. Karsai, P. Volgyesi, M. Maroti: On Metamodel Composition

M. Au. Fortes da Cruz: Assertive Modeling Framework

V.S. Alagar, G. Haidar, V. Srinivasan: A Formal Approach to Designing Software for Ease of Extension and Retraction

I. Traore: A Framework for Rigorous Testing of Object-oriented Programs

P. Krishnamurthy, P.A.G. Sivilotti: Object Protocols for Distributed Systems

D. Gray, G. Hamilton, J. Powers, D. Sinclair: A Specification of TCP/IP using Mixed Intuitionistic Linear Logic

C.H. Cap, N. Ioustinova: Algebraic and Transitional Techniques for Requirements Specification of Distributed Systems

P. Cheng, D. Wijesekera: Hierarchical and Modular Model Checking of Finite State Machines

J. Mullins: Two Proof Methods for Fully Bisimulation-based Non-deterministic Admissible Interference

D. Zhou, P.E. Black: Formal Specification of Operating System Operations

D. Beyer, H. Rust: Cottbus Timed Automata: Formal Definition and Semantics

D. Beyer, A. Heinig: Different Strategies for BDD-based Reachability Analysis of Timed Automata

J. Guo: An Integrated Formal Framework in the Development of Safety Critical Software Systems

A. Galloway, J. Blow: Multi-layered Domain Specific Formal Languages

J. Baillie: From CSP to Java: A Rough Guide

S. Nyambaa, I. Tseren-Onolt, R. Moore: Formal Specification of a Management System for University Teaching

D.W. Bustard, P.J. Lundy: Low-cost Formal Support for Business Analysis: A Case Study in Methods Integration

M. Satpathy, R. Harrison, C. Snook, M. Butler: A Comparative Study of Formal and Informal Specifications through an Industrial Case Study

M. Sveda, F. Zezulka, R. Vrba: A Case-Based Reasoning Approach to Reuse of CBS Specifications

3rd Joint Workshop 2002

The third IEEE/IFIP Joint Workshop on Formal Specifications of Computer-Based Systems, sponsored by both IEEE TC-ECBS and IFIP WG10.1, has been organized by Jerzy Rozenblit, Miroslav Sveda, and Charles Rattray and held in Lund, Sweden, 10-11 April 2002. The following twelve contributions were published in the Workshop Proceedings 2002 [3] and presented at the workshop.

C. Kong, P. Alexander: Modeling Model of Computation Ontologies in Rosetta

Y.M. Liu, I. Traore: PVS Proof Patterns for UML-Based Verification

S. Lafrance, J. Mullins: A Generic Enemy for the Analysis of Cryptographic Protocols

T. Sivertsen: Algebraic Specification of an Inductive Theorem Prover

- R.G. Crespo: The Semantics of Feature Execution Trees
- S. Nadjm-Tehrani: Synchronous Languages for Heterogeneous Models of Embedded Systems
- A. Fernandez Vilas, J.J. Pazos Arians, R.P. Diaz Redondo: Incremental Synthesis of Timed Models from Many-valued Temporal Logic
- V. Dvorak: Executable System-Level Specifications of HW/SW Architecture for Embedded Multiprocessor Systems
- J. Staroba, V. Dvorak: Design Space Exploration of Parallel Embedded Applications Based on Performance-Oriented Specifications
- J. Kotzian, V. Srovnal: Using Formal Methods for Designing Embedded Control Systems
- A. Manzer, A. Dogru: Formal Modeling for the Composition of Virtual Enterprises
- P. Kucera, F. Zezulka, M. Sveda, R. Vrba: Executable Specifications for Process Automation and Microelectronics

Full-Length Papers

Participants of the First Workshop had the possibility to extend their submissions to full papers and resubmit them for journal publication. The program committee consisting of Vaclav Dvorak, Charles Rattray, Jerzy Rozenblit and Miroslav Sveda reviewed nine full-length papers. The best 6 of them passed the reviewing process by and appeared in the special issue of the electronic Journal of Universal Computer Science [4]:

- Gabor Karsai: Towards two-level Formal Modeling of Computer-Based Systems
http://www.jucs.org/jucs_6_11/towards_two_level_formal
- Savi Maharaj, Carron Shankland: A Survey of Formal Methods applied to IEEE 1394
http://www.jucs.org/jucs_6_11/a_survey_of_formal
- Issa Traore: An Outline of PVS Semantics for UML Statecharts
http://www.jucs.org/jucs_6_11/an_outline_of_pvs
- Robert G. Clark: Use of E-LOTOS in Adding Formality to UML
http://www.jucs.org/jucs_6_11/use_of_e_lotos

- John Mullins: Non-deterministic Admissible Interference
http://www.jucs.org/jucs_6_11/nondeterministic_admissible_interference

- Laurent Allain, Pascal Yim: Modeling Information System Behavior with Dynamic Relation Nets
http://www.jucs.org/jucs_6_11/modeling_information_system_behavior

Also authors of the Second and the Third Workshop had the possibility to extend their submissions to full papers and resubmit them, in this case, for a "paper" journal publication. The program committee consisting of Jerzy Rozenblit, Charles Rattray and Miroslav Sveda is striving to complete negotiation and reviewing process for a journal publication of the following 17 full-lengths from the year 2001 and 5 full-lengths from the year 2002:

- P. Krishnamurthy, P.A.G. Sivilotti: Object Protocols for Distributed Systems
- J. Mullins: Two Proof Methods for Fully Bisimulation-based Non-deterministic Admissible Interference
- P. Alexander, Cindy Kong: Heterogeneous Computer-Based System Specification
- D. Zhou, P.E Black: Formal Specification of Operating Systems
- M. Sveda, F. Zezulka, R. Vrba: A Case-Based Reasoning Approach to Reuse of CBS Specifications
- D. Gray, G. Hamilton, J. Power, D. Sinclair: A Specification of TCP/IP using Mixed Intuitionistic Linear Logic
- A. Ledeczi, G. Nordstrom, G. Karsai, P. Volgyesi: On Metamodel Composition
- D.W Bustard, P.J Lundy: Low-cost Support for Business Analysis: A Case Study in Methods Integration
- M. Satpathy, C. Snook, R. Harrison, M. Butler: A Comparative Study of Formal and Informal Specifications through an Industrial Case Study
- J. Baillie, J. Malcolm: From CSP to Java: A Rough Guide
- D. Beyer, A. Heinig: Different Strategies for BDD-based Reachability Analysis of Timed Automata
- A. Galloway, J. Blow: Multi-layered Domain Specific Formal Languages

- V.S. Alagar, G. Haidar, V. Srinivasan: A Formal Approach to Designing Software for Ease of Extension and Retraction
- J. Guo: An Integrated Formal Framework in the Development of Safety Critical Software Systems
- D. Beyer, H. Rust: Cottbus Timed Automata: Formal Definitions and Semantics
- P. Chen, D. Wijesekera: Hierarchical and Modular Model Checking of Finite State Machines
- I. Traore: A Framework for Rigorous Testing of Object-oriented Programs
- R.G. Crespo: The Semantics of Feature Execution Trees
- A. Fernandez Vilas, J.J. Pazos Arias, R.P. Diaz Redondo: Incremental Synthesis of Timed Models from Many-valued Temporal Logic
- J. Kotzian, V. Srovnal: Using Formal Methods for Designing Embedded Control Systems
- T. Sivertsen: Algebraic Specification of an Inductive Theorem Prover
- P. Kucera, F. Zezulka, M. Sveda, R. Vrba: Executable Specifications for Process Automation and Microelectronics

4th Joint Workshop 2003

The goal of this workshop, following the IEEE ECBS'2003 Conference, is to provide a forum for researchers and practitioners from industry and academia to discuss both completed work and work-in-progress related to formal specifications of computer-based systems, software, hardware and hardware/software applications. The co-chairs of this workshop Miroslav Sveda, Charles Rattray and Jerzy Rozenblit, encouraged, in particular, studies focusing on integrating formal techniques into systems design and implementation and on various application case studies.

The FS CBS Call for Papers, distributed through e-mail lists among IEEE ECBS and IFIP TC10 communities, asked to submit 5-8 page extended abstracts for publishing in the Preprints Proceedings. The authors will have an opportunity to present a 20-minute talk on their work. The final papers, based on presented extended abstracts and selected from the refereed full-length papers are to be published in a special issue of the electronic Journal of Universal Computer Science (Springer).

Acknowledgements

The authors would like to thank their colleagues, namely Byron Purves, Ted Bapty, Perry Alexander, Stephanie White, Vaclav Dvorak and all submitting authors for their valuable contributions to the initiation and implementation of this Workshop.

References

- [1] Rattray C., Sveda M. (Editors): *Proceedings of the IEEE TC-ECBS + TF RE and IFIP WG10.1 Joint Workshop on Formal Specifications of Computer-Based Systems*. Edinburgh, Scotland, April 6-7, 2000. Produced by University of Stirling, UK, 2000, pp.iii+85.
- [2] Rattray C., Sveda M., Rozenblit J. (Editors): *Proceedings of the IEEE TC-ECBS and IFIP WG10.1 Joint Workshop on Formal Specifications of Computer-Based Systems*. Washington, D.C., USA, April 20, 2001. Produced by University of Stirling, UK, 2001, pp.iii+150.
- [3] Rattray C., Sveda M., Rozenblit J. (Editors): *Proceedings of the IEEE TC-ECBS and IFIP WG10.1 Joint Workshop on Formal Specifications of Computer-Based Systems*. Lund, Sweden, April 10-11, 2002. Produced by University of Stirling, UK, 2002, pp.iii+98.
- [4] Dvorak V.: Special Issue on Formal Specifications of Computer-Based Systems. *Journal of Universal Computer Science*, Springer, Vol.6., No.11., 2000.
http://www.jucs.org/jucs_6_11