Journal of Universal Computer Science, vol. 6, no. 11 (2000), 1052-1053
submitted: 1/10/00, accepted: 23/10/00, appeared: 28/11/00 © Springer Pub. Co.

J.UCS Special Issue on Formal Specifications of Computer-Based Systems

Vaclav Dvorak
(Brno University of Technology, Czech Republic
dvorak@dcse.fee.vutbr.cz)

Formal methods referring to mathematical modeling techniques applicable to computer design, software and hardware, are as old as computer science itself. They have gone a long way before becoming an indispensable tool in a wide spectrum of applications, from chip design to information system modeling. The domain of computer-based systems (CBS) brings new challenges to formal specification methods and tools because of complexity of CBS, which include distributed/parallel, hard RT, safety critical and mixed SW/HW systems.

Since complete formal specification, modeling and verification of large complex systems is impractical at this time, using formal methods only for the most critical portions of a system is a pragmatic and useful strategy. The Formal Specifications Working Group within the IEEE Computer Society TC-ECBS aims at the use of formal notations to describe assumptions, requirements and a design of CBS. The first Workshop on Formal Specifications of CBS (FS-CBS) has been organized by Charles Rattray (UK) and Miroslav Sveda (CZ) 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, software, hardware and hardware/software applications. Authors of 17 presented contributions from Europe and North America extended their submissions to full papers, out of which the best 6 passed the reviewing process and appear in this special issue of J.UCS.

The paper "*Nondeterministic Admissible Interference*" by J. Mullins addresses the issue of confidentiality and information security, important for applications such as electronic banking. Admissible information flow between levels of multi-level security architecture is modeled using the extended transition system DTS and completeness of such characterization is formally proved. The follow-up research is to be oriented into computer-aided verification methods and tools for admissible interference.

Two papers deal with aspects of Unified Modeling Language (UML), a standard notation used in the object-oriented analysis and design phase. The paper entitled "*Use of E-LOTOS in Adding Formality to UML"* by R. Clark and A. Moreira describes mappings from UML constructs to the formal language E-LOTOS, which then provides executable specifications. In obtaining a formal model this way, authors were even able to identify inconsistencies in UML models. Rapid prototyping tools are suggested for validation purposes. The other paper on UML, "*An Outline of PVS Semantics for UML Statecharts*" by I.Traore presents an approach for formalization of one of the multiple diagrams of UML, namely statechart diagrams. That is achieved by using PVS Specification Language as formal semantics domain. Formal analysis using the PVS model-checker makes also use of this approach.

Information system specification and design are a central problem of information processing today. Besides UML, there are other methods to specify data, events and processing. The paper "*Modeling Information System Behavior with Dynamic Relation Nets*" by L. Allain and P.Yim introduces a model closely related to high-level Petri Nets – Dynamic Relation Nets (DRN). The power of DRN approach is in the integration of both static and dynamic aspects of an information system. The computational part of an active DBMS-based application can be generated automatically from the DRN specification. However, consistent design tools, dedicated to processing specifications and based on presented ideas, are yet to be developed.

The paper "*Towards Two-Level Formal Modeling of Computer-Based Systems*" by G. Karsai, G. Nordstrom, A. Ledeczi and J. Sztipanovits argue that there is no single modeling language, which would satisfy the requirements of all CBS. The authors therefore propose a two-level approach, where area-specific modeling tools are used for creating domain-specific models, and these tools are represented in terms of (and built from) a higher-level meta-model. The method proved itself during years of its practical use.

The last paper "*A Survey of Formal Methods Applied to Leader Election in IEEE 1394*" by S. Maharaj and C. Shankland is a comparative study. A variety of formalisms (E-LOTOS, I/O Automata, μCRL) have been used to specify and analyze the same real-life benchmark: IEEE 1394 FireWire multimedia serial bus and particularly the network Leader Election (LE) protocol specification. Specifications are judged according to their expressiveness, readability, standardization and the kinds of analysis possible. Comparison is by all means instructive and stimulating.

We hope that readers will benefit from the most recent work in formal specifications and that they will get interested in formal methods generally, and in formal specifications of CBS specifically. Enjoyable reading!

Vaclav Dvorak, Guest Editor
Brno University of Technology, Czech Republic
dvorak@dcse.fee.vutbr.cz