1996?

A ProCoS-WG Working Group Final Report: ESPRIT Working Group 8694

Jonathan Bowen[1*] C.A.R. Hoare[2] Hans Langmaack[3]
Ernst-Rüdiger Olderog[4] Anders P. Ravn[5]

[1] The University of Reading, UK
[2] Oxford University, UK
[3] Christian-Albrechts-Universität Kiel, Germany
[4] University of Oldenburg, Germany
[5] Technical University of Denmark

URL: http://www.comlab.ox.ac.uk/archive/procos/procos-wg.html
Email: procos-request@comlab.ox.ac.uk

Abstract

An overview of the activities of the European collaborative ESPRIT **ProCoS-WG** Working Group (no. 8694) on "Provably Correct Systems" which ran from 1993 to 1997 is presented. This was a follow-on to the ESPRIT BRA **ProCoS I** project (no. 3104, 1989–1991) and **ProCoS II** project (no. 7071, 1992–1995), overlapping with the latter. A selected bibliography of publications, especially those involving the original project sites and collaboration between member sites, is included.

1 Introduction

The ESPRIT **ProCoS-WG** Working Group (no. 8694, 1993–1997) was formed as part of the activities of the **ProCoS II** Project (no. 7071, 1992–1995) [20] on "Provably Correct Systems", which itself was reformed after the original **ProCoS I** project (1989–1991). Its aim was to aid dissemination of the project's results. **ProCoS-WG** aimed to focus around rigorous techniques to improve dependability, reduce time-scales and cut development costs of construction for embedded systems, particularly in real-time and safety-critical applications. Its members used and developed the results of basic research into fundamental properties of interactive systems. Its interests included the development of embedded systems, ensuring correctness of all stages in the

*Department of Computer Science, University of Reading, Whiteknights, PO Box 225, Reading, Berkshire RG6 6AY, UK, since 1st October 1995. URL: http://www.cs.reading.ac.uk/people/jpb/ Email: J.P.Bowen@reading.ac.uk

development, from elicitation and analysis of requirements through design and implementation of programs down to compilation and execution on verified hardware.

The long term objective of the Working Group was to contribute to radical improvement in standards of professional practice in the design and implementation of information technology products, involving both hardware and software. The first target for improvement was in the area of safety-critical application; but we believe that much of the same technology will eventually spin off to improve quality and reduce life cycle costs of other products in widespread use.

Topics of interest to members of the Working Group include theories and methodology to handle the following levels of abstraction in the development of computer-based systems: (1) Requirements capture and analysis; (2) System specification and design; (3) Programming language processing and compilation; (4) Machine hardware, including hardware/software co-design; (5) Implementation in hardware down to gate level, especially using hardware compilation techniques.

2 Activities

Joint workshops with the ESPRIT **ProCoS II** project were held during the lifetime of that project (which ended in 1995) approximately every 6 months at project sites in Denmark, Germany and the UK.

A **ProCoS II** project meeting before the Working Group start was held in 1993 in Germany. Many prospective Working Group partners attended and gave presentations.

The official 1st Working Group meeting was held at Gentoft, Denmark in 18–20 January 1994, organized by Anders Ravn *et al.* of the Danish Technical University (DTU). The majority of Working Group members attended. In addition, a number of invited guests attended at their own expense. All Working Group members gave an overview of their activities relevant to **ProCoS**, and a number gave technical presentations as well. In addition, an overview of the **ProCoS II** project, and detailed technical talks on aspects of the project's research were presented by project members.

The major open event for the Working Group was a School and Symposium organized jointly with the existing Formal Techniques in Real-Time and Fault-Tolerant Systems series, held 19–23 September 1994 at Lübeck, Germany. A published proceedings is available [37]. Kiel were involved in the organization of the meeting and Prof. Hans Langmaack was a co-editor of the proceedings. A substantial **ProCoS** tutorial was presented.

The 2nd **ProCoS** meeting (for **ProCoS-WG** participants and invited guests only) was held on 10–12 January 1995 in Oxford, UK. An agenda including summaries of the talks is available on-line. Subjects included compilation proof of correctness, temporal compositionality, a logical framework for concurrent Objects, a modular codegenerator proof, digital abstraction of switching circuitry, the Sequential Calculus, refinement calculus with window inference, provably correct hardware/software partitioning, layering of real-time distributed processes, model checking and appropriate use of formal methods.

The 3rd **ProCoS-WG** meeting was held 21–23 August 1995 at the Hotel Marina, Vedbaek, near Copenhagen, Denmark. The local organizers were DTU. The theme for the workshop was "*Linking Theories*", ~~There are many~~ theories which can assist in the reliable design of real-time embedded computer systems. This workshop emphasized the interfaces between these theories as an important topic for theoretical research since it is always the combination of technologies that causes the most serious engineering problems.

The 4th **ProCoS-WG** meeting, was held 11–13 March 1996, in Oldenburg, Germany, organized by Prof. E.-R. Olderog. The main topics of the meeting were real-time and hybrid systems, linking different formal methods, and mechanical support of these methods. The highlight was a presentation of three German projects on formal methods for correct systems, namely the

ESPRESS, KORSYS and UNIFORM projects.

An associated **ProCoS-US** Hardware Synthesis and Verification Workshop was held at Cornell University, Ithaca, New York, USA, 14–16 August 1996. Members of the Working Group ~~will~~ an interest in provably correct hardware compilation attended and gave presentations. An informal proceedings was produced and issued to all participants.

The last major meeting was the 5th **ProCoS-WG** meeting, 7–9 April 1997, organized by Jonathan Bowen at the University of Reading, UK, in conjunction with ZUM'97 (see below). This was the final funded meeting of the Working Group. An academic day of more technical and research-oriented talks was held on the first day. A highlight was a presentation on *Unifying Theories for Parallel Systems* by Prof. Tony Hoare of Oxford University. On the second day some of the talks were more industrially and educationally oriented. The final day was an academic and business-oriented day in which plans for a follow-on Working Group were discussed.

The Working Group also supported the Z User Meeting series of conferences. The 8th Z User Meeting (ZUM'94) was held on 29–30 June 1994 at the University of Cambridge, UK [10]. The 9th International Conference of Z Users (ZUM'95) was held 7–9 September 1995 at the University of Limerick, Ireland [15]. The last meeting was ZUM'97 which was held at the University of Reading, UK, 3–4 April 1997 in conjunction with the final Working Group meeting [18]. All these meetings included contributions by **ProCoS-WG** members.

Further information on all these meetings is available on-line, linked from the Working Group's Web page (see end of report for URL).

3 Selected reports from ProCoS-WG sites

An integral part of the original **ProCoS II** project research plan was the formation of this Working Group. This section includes short reports from each of the original members of the **ProCoS II** project. Sample reports from a **ProCoS-WG** member and an affiliate are also included. Reports from all 25 members sites, and other individual affiliates, are not included due to lack of space. However this section is intended to give a flavour of the activities which the Working Group has helped foster at the various sites involved, both with other **ProCoS-WG** members and externally to the Working Group.

Oxford were the original proposers and coordinators for the Working Group. During the lifetime of the Working Group, Jonathan Bowen moved from a UK EPSRC funded project on *Provably Correct Hardware/Software Co-design* at Oxford, including explicit mention of European **ProCoS-WG** collaboration, to take up an appointment as a lecturer at the University of Reading, where more recent coordination of the group has been undertaken.

3.1 Oxford University, UK

For the last two years Prof. Tony Hoare and Prof. He Jifeng have been working on a UK EPSRC funded project for *Linking theories in Computer Science*. ~~The results have exceeded all our original hopes and expectation.~~ ~~We~~ have investigated a wide variety of computational paradigms, procedural and declarative, sequential and parallel, centralized and distributed, synchronized and asynchronous, even hardware and software. This work has fully confirmed a widely held conjecture that all paradigms can be embedded in the single mathematical theory of relations: and a number of projections have been discovered that maps the general theory to its more particular instances.

This means that a single model-based specification language like Z or VDM will serve at the highest level of abstraction to specify all systems, without concern for the technology or mixture of technologies in which they will be implemented. The notations of each programming language are definable as extensions to the schema calculus of Z, and powerful algebraic laws are provided

to assist in subsequent design. As a result, all paradigms are susceptible of the same design methodology, with proofs based on familiar techniques of calculational refinement, assertion and weakest precondition.

These ideas have been highly influenced by experience of collaboration with **ProCoS** partners. In turn, it is hoped that the concepts will also have future influence on **ProCoS** members through the regular **ProCoS-WG** meetings we have attended, and further afield through existing and planned publications [29, 35, 36].

3.2 Christian-Albrechts-Universität Kiel, Germany

After completion of the **ProCoS** projects, the Kiel group (headed by Prof. Hans Langmaack [42]) continued research on the broad scope of topics that the **ProCoS** projects had sparked. These topics, involving algebraic models of reactive systems [2, 3, 56, 57, 58, 59], real-time model-checking and controller synthesis [23, 24, 25], and compiler design and verification [26, 50], may seem diverse, yet they are closely linked within the **ProCoS** approach.

Setting up a consistent set of formalisms and methods for the variety of abstraction levels that arise during embedded system design requires a firm grasp of all of them. However, the scientific subjects involved are nevertheless diverse, and no single research group would be able to substantially further all of them without being linked to other, particularly more specialized, groups. Being broader in scope than the scientific contacts that a single site can set up, the **ProCoS** Working Group proved to be an excellent basis for the required kind of scientific exchange. Its meetings provided an indispensable forum for presenting and discussing the work in various stages, and finally became an important means for teaching the newly developed techniques to other personnel.

It is just now that it becomes apparent how successful these information dissemination activities were: The compiler verification activities of the **ProCoS** project led to a German compiler verification project called Verifix (Verifizierte Compiler, verified compilers) [28, 41, 43] that builds upon the ProCoS techniques [49]. The project is supported by the Deutsche Forschungsgemeinschaft (DFG). The other project partners – Prof. Goos at the University of Karlsruhe, Germany, and Prof. v. Henke at the University of Ulm, Germany – were a member and an affiliate member of the **ProCoS** Working Group respectively.

Furthermore, **ProCoS** researchers from Kiel have been hired by other universities: Markus Müller-Olm, whose extensive case study of applying the **ProCoS** compiling verification techniques onto the translation of a prototypic hard-real time programming language to an actual processor (the Inmos Transputer) is documented in the PhD thesis [48] that appeared recently as a monograph in the LNCS series of Springer-Verlag [50], moved to the University of Dortmund, Germany. Martin Fränzle, who has been concerned with real-time model-checking and hardware synthesis from temporal logic [24, 25, 23], is now at the University of Oldenburg, Germany – another **ProCoS** Working Group site – responsible for synthesis of VHDL designs from temporal logic specifications. Bettina Buth is now employed at the University of Bremen, Germany.

3.3 Universität Oldenburg, Germany

ProCoS-WG has enabled us to maintain contacts and collaboration between DTU, Denmark and Oldenburg on the use of Duration Calculus and programming specification language SL developed during the **ProCoS** project. This is documented by two case studies [51, 55].

It has also enabled exchange of ideas between the University of Twente, The Netherlands (J. Zwiers) and Oldenburg on specification formalisms mixing communication and state transition aspects. A separate two day meeting took place in Autumn 1996.

Personnel exchange between Oxford University, UK and Oldenburg, Germany took place by

Michael Schenke from Oldenburg visiting Oxford for one year (1996/97) and applying ideas from **ProCoS** in a UK EPSRC funded project [54].

3.4 Danish Technical University, Denmark

The **ProCoS-WG** Working Group has enabled us to stay in touch with **ProCoS** partners and associates; in particular, collaborative research with the University of Oldenburg, Germany has been undertaken, as documented in the joint papers [51, 55]. Another direct outcome has been the collaboration with Siemens Research resulting in [52]. Furthermore, we have a new collaboration with Turku, Finland [53] and have discussed functional programming with the University of Reading, UK.

3.5 Report from a ProCoS-WG member site

The Intellectics Laboratory of the Department of Computer Science at the Technische Universität Darmstadt, Germany has profited in substantial ways from the interaction with other members in the **ProCoS-WG**. Our approach to provably correct systems, briefly spoken, consists in extracting programs, or systems, from interactively obtained proofs of their specifications (considered as theorems in some theory formalized in some constructive logic).

The interaction with the **ProCoS-WG** has kept us focusing on the reality of software engineering and remaining on firm practical grounds. We attended three **ProCoS** meetings (Gentofte 1994, Lübeck 1994, Vedbaek 1995), usually with two members from our laboratory, and presented talks at two of them. In addition we stayed in contact with individual members of the Working Group. Our group played also a linking role between **ProCoS** and a German national project on automated deduction which is coordinated by the laboratory's leader (W. Bibel).

Although there is no joint paper with one of these individual members completed, the **ProCoS** influence can be recognized in many of our own papers. In fact, the **ProCoS**-related research in our lab (which has several other interests beyond **ProCoS** such as pure theorem proving, knowledge representation, stochastic search etc.) has been extremely successful during the period of the last three years as can be seen from the selected list of publications [5, 38, 39, 40]. This work has brought theorem proving techniques closer to system development practice and altogether resulted in the system MAPS [4] meant to be useful exactly for this purpose.

4 ProCoS affiliates

During the course of the Working Group, it was noticed that a number of participants not included in the original proposal were keen to participate at many of the meetings. These people were invited to become "**ProCoS** affiliates" and were subsequently invited to attend **ProCoS** meetings, but at their own expense. As a result, a significant amount of the European collaboration fostered by the Working Group was with European sites not directly funded by **ProCoS-WG**. Many of the **ProCoS-WG** affiliates are involved in the proposed follow-on Working Group. Feedback from two **ProCoS** affiliates is included below.

Sample reports

Prof. Egon Börger of the University of Pisa, Italy, has participated at many **ProCoS-WG** meetings, largely at his own expense. He was an invited speaker at ZUM'97 [7] and organized, with Prof. Hans Langmaack of the University of Kiel, an important set of case studies formalizing a Steam Boiler problem in a variety of notations [1], including a number of contributions by **ProCoS-WG** members. He reports:

> The **ProCoS** meetings have been for me a very useful occasion for fruitful exchange of ideas and methods related to the application of formal methods. In particular I appreciate the occasion I had to present my work on the correctness theorem for a general compilation scheme for compiling Occam programs to Transputer code. This work appeared in [6].
>
> Furthermore I appreciated the chance to present the Abstract State Machine (ASM) method to **ProCoS-WG** members.

Dr. Ben Moszkowski of the Department of Electrical and Electronic Engineering, University of Newcastle; Newcastle upon Tyne, UK has also participated in an unfunded affiliate capacity since the initial meeting. He has been working on Interval Temporal Logic (ITL) and compositionality [22, 46, 47, 45], and writes:

> I have found the **ProCoS** Working Group to be very beneficial as a framework for relatively informal meetings with others in both academia and industry who have a serious interest in formal methods. The five **ProCoS**-related meetings I have been to since 1994 have always had stimulating exchanges of ideas. Besides learning about other groups' ongoing activities, I have had an opportunity to get comments on my own work and to discuss research grant proposals. Jonathan Bowen's maintenance of the Formal Methods Web pages is an invaluable part of **ProCoS-WG**'s mission of disseminating information about formal methods. My own participation in the **ProCoS-WG** even lead indirectly to a very successful international symposium on compositionality entitled COMPOS'97. In closing, I hope that **ProCoS-WG** continues to serve its useful role.

5 Dissemination

A major open conference was held in conjunction with an existing related conference series, *Formal Techniques in Real-Time and Fault-Tolerance Systems* (FTRTFT) [44]. Many **ProCoS-WG** Working Group members attended. An extended **ProCoS** tutorial was presented [19, 30]. A **ProCoS** tutorial [31] was also presented at FME'96 in Oxford [27].

Related EC "Keep In Touch" (KIT) initiatives with Augusto Sampaio in Brazil and Zhou Chaochen in Macau have allowed continuing contact with former project members. An associated ESPRIT/NSF initiative allows reciprocal funding of visits between Cornell University in the US and **ProCoS** partners in the area of provably correct hardware compilation. A workshop was held in August 1996 at Cornell University, USA.

Contact with the Z User Group has been maintained by supporting attendance at Z User Meetings [10, 15, 18] using **ProCoS-WG** Working Group funds when appropriate. A journal special issue on Z has been produced [14] and a Z bibliography maintained [8, 21].

A book of industrial applications of formal methods has been produced [32]. This includes a number of chapters contributed by members of the Working Group. Two associated articles have been produced as guides to industrial users of formal methods [12, 13] with the aim of facilitating the technology transfer of formal methods. These have been translated into Dutch (*Management [Select]*, December 1996) and Russian (*PC World Russia*, September/October 1997) respectively for further dissemination. Material has been published specifically for technology transfer especially with respect to standards and safety-critical systems [9, 11, 16, 17]. Further books are in the course of preparation [33, 34].

Information on all **ProCoS** activities, including the Working Group, has been maintained on-line, together with an associated repository of formal methods and safety-critical systems information (see locations at the end of the report). These resources have been remarkably

successful and attract several hundred users each day. An electronic mailing list for messages relating to **ProCoS** activities, especially notices of meetings, has also been maintained. This has included personnel at all Working Group sites with email access, **ProCoS** affiliates, and anyone with an interest in **ProCoS** on request to `procos-list-request@comlab.ox.ac.uk`.

Bibliographies of relevant publications by **ProCoS** members have been created and maintained on-line for easy accessibility and convenient searching. This report includes a selection of **ProCoS-WG**-related publications, especial those where collaboration between Working Group sites has been involved.

6 Lessons learned

The Working Group has been extremely successful as a mechanism to ensure contact between academic members. Meetings have been well attended, although some sites have participated considerably more than others. **ProCoS-WG** has been less successful in maintaining direct contact with industrial sites. However, it has been inspirational in generating technology transfer information in the form of articles, books and on-line Web-based information.

Members with good network access have benefited most from the Working Group as far as direct information dissemination is concerned. Essential information, especially concerning meetings, has been sent by fax or post to the (small number of) members who were not contactable via electronic mail. However these members have in general participated less at meetings; they are also the more industrially oriented sites.

Sites where existing ties have been in place have participated most in the Working Group. Generating new ties through the Working Group has not been completely successful; much more success has been found when building on and continuing existing ties.

These lessons have been taken on board for a proposed follow-on Working Group. All the proposed new members have existing links with at least one other member, and/or have expressed proactive interest in joining the group. This was not necessarily the case for all partners in the initial Working Group reported here.

7 Conclusion

Overall, the Working Group is deemed to have been a success. The original core of **ProCoS II** project sites have maintained a high degree of *esprit de corps*, and this has engendered enthusiasm in other participants at Working Group meetings. We have also gained from having a variety of ideas and approaches presented at meetings. Certainly there is enough continued enthusiasm from the majority of the original **ProCoS-WG** members to form a consortium for a follow-on proposal, together with a number of new members, mainly due to personnel moves between sites together with the inclusion of previous **ProCoS** affiliates and collaborators.

On-line information

Much fuller on-line information on the activities and achievements of the **ProCoS-WG** Working Group is available under the following URL (Universal Resource Locator):

`http://www.comlab.ox.ac.uk/archive/procos/procos-wg.html`

This information will be available and maintained for the foreseeable future. An associated Virtual Library repository comprising a directory of on-line information for guidance concerning formal methods, and also safety-critical systems, has been particularly successful, attracting around 300 virtual "visitors" each day. See under:

http://www.comlab.ox.ac.uk/archive/formal-methods.html

Newer and related ProCoS activities will be installed and maintained under the following location:

http://www.cs.reading.ac.uk/procos/

Bibliography

[1] J.-R. Abrial, E. Börger, and H. Langmaack, editors. *Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control*, volume 1165 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[2] R. Berghammer and B. von Karger. Formal derivation of CSP programs from temporal specifications. In B. Möller, editor, *Mathematics of Program Construction*, volume 947 of *Lecture Notes in Computer Science*, pages 180–196. Springer-Verlag, 1995.

[3] R. Berghammer and B. von Karger. Towards a design calculus for CSP. *Science of Computer Programming*, 26:99–115, 1996.

[4] W. Bibel, D. Korn, C. Kreitz, F. Kurucz, J. Otten, S. Schmitt, and G. Stolpmann. A multi-level approach to program synthesis. In *Proc. 7th International Workshop on Logic Program Synthesis and Transformation*, Lecture Notes in Computer Science. Springer-Verlag, 1997. To appear.

[5] W. Bibel, D. Korn, C. Kreitz, and S. Schmitt. Problem-oriented applications of automated theorem proving. In J. Calmet and C. Limongelli, editors, *Design and Implementation of Symbolic Computation Systems*, volume 1128 of *Lecture Notes in Computer Science*, pages 1–21. Springer-Verlag, 1996.

[6] E. Börger and I. Durdanovic. Correctness of compiling Occam to Transputer code. *The Computer Journal*, 39(1):52–92, 1996.

[7] E. Börger and S. Mazzanti. A practical method for rigorously controllable hardware design. In Bowen et al. [18], pages 151–187.

[8] J. P. Bowen. Select Z bibliography. In Bowen et al. [18], pages 391–424.

[9] J. P. Bowen, R. W. Butler, D. L. Dill, R. L. Glass, D. Gries, J. A. Hall, M. G. Hinchey, C. M. Holloway, D. Jackson, C. B. Jones, M. J. Lutz, D. L. Parnas, J. Rushby, H. Saiedian, J. Wing, and P. Zave. An invitation to formal methods. *IEEE Computer*, 29(4):16–30, April 1996.

[10] J. P. Bowen and J. A. Hall, editors. *Z User Workshop, Cambridge 1994*, Workshops in Computing. Springer-Verlag, 1994.

[11] J. P. Bowen and M. G. Hinchey. Formal methods and safety-critical standards. *IEEE Computer*, 27(8):68–71, August 1994.

[12] J. P. Bowen and M. G. Hinchey. Seven more myths of formal methods. *IEEE Software*, 12(4):34–41, July 1995.

[13] J. P. Bowen and M. G. Hinchey. Ten commandments of formal methods. *IEEE Computer*, 28(4):56–63, April 1995.

[14] J. P. Bowen and M. G. Hinchey. Z special issue: Editorial. *Information and Software Technology*, 37(5–6):258–259, May/June 1995.

[15] J. P. Bowen and M. G. Hinchey, editors. *ZUM '95: The Z Formal Specification Notation, 9th International Conference of Z Users, Limerick, Ireland, 7–9 September 1995*, volume 967 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995.

[16] J. P. Bowen and M. G. Hinchey. Formal models and the specification process. In A. B. Tucker, Jr., editor, *The Computer Science and Engineering Handbook*, chapter 107, pages 2302–2322. CRC Press, 1997.

[17] J. P. Bowen and M. G. Hinchey. The use of industrial-strength formal methods. In *Proc. 21st International Computer Software & Application Conference (COMPSAC'97), Washington D.C., USA*, pages 332–337. IEEE Computer Society Press, 13–15 August 1997.

[18] J. P. Bowen, M. G. Hinchey, and D. Till, editors. *ZUM '97: The Z Formal Specification Notation, 10th International Conference of Z Users, Reading, UK, 3–4 April 1997*, volume 1212 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[19] J. P. Bowen, C. A. R. Hoare, M. R. Hansen, A. P. Ravn, H. Rischel, E.-R. Olderog, M. Schenke, M. Fränzle, M. Müller-Olm, He Jifeng, and Zheng Jianping. Provably correct systems – FTRTFT'94 tutorial. ProCoS II document [COORD JB 7/1], Oxford University, UK, September 1994.

[20] J. P. Bowen, C. A. R. Hoare, H. Langmaack, E.-R. Olderog, and A. P. Ravn. A ProCoS II project final report: ESPRIT Basic Research project 7071. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 59:76–99, June 1996.

[21] J. P. Bowen, S. Stepney, and R. Barden. Annotated Z bibliography. *Information and Software Technology*, 37(5–6):317–332, May/June 1995.

[22] A. Cau, H. Zedan, N. Coleman, and B. Moszkowski. Using ITL and Tempura for large scale specification and simulation. In *Proc. 4th Euromicro Workshop on Parallel and Distributed Processing*, pages 493–500. IEEE Computer Society Press, 1996.

[23] M. Fränzle. *Controller Design from Temporal Logic: Undecidability need not matter.* Dissertation, Technische Fakultät der Universität Kiel, Germany, 1996. Available as Bericht 9710, Institut für Informatik und Prakt. Mathematik der Univ. Kiel, 1997.

[24] M Fränzle. Hardware synthesis from temporal logic: Undecidability need not matter. Position paper, Hardware Synthesis and Verification Workshop, Cornell University, Ithaca, USA, August 1996.

[25] M. Fränzle. Synthesizing controllers from duration calculus. In Jonsson and Parrow [37], pages 168–187.

[26] M. Fränzle and M. Müller-Olm. Towards provably correct code generation for a hard real-time programming language. In P. A. Fritzson, editor, *Compiler Construction*, volume 786 of *Lecture Notes in Computer Science*, pages 294–308. Springer-Verlag, 1994.

[27] M.-C. Gaudel and J. C. P. Woodcock, editors. *FME'96: Industrial Benefit and Advances in Formal Methods*, volume 1051 of *Lecture Notes in Computer Science*. Formal Methods Europe, Springer-Verlag, 1996.

[28] W. Goerigk, A. Dold, T. Gaul, G. Goos, A. Heberle, F. W. von Henke, U. Hoffmann, H. Langmaack, H. Pfeifer, H. Ruess, and W. Zimmermann. Compiler correctness and implementation verification: The *Verifix* approach. In *CC '96 International Conference on Compiler Construction (poster session)*, Linkøping, Sweden, 1996.

[29] He Jifeng and C. A. R. Hoare. Linking theories of probabilistic programming. In *Proc. SBLP'97*, 1997.

[30] He Jifeng, C. A. R. Hoare, M. Fränzle, M. Müller-Olm, E.-R. Olderog, M. Schenke, M. R. Hansen, A. P. Ravn, and H. Rischel. Provably correct systems. In Langmaack et al. [44], pages 288–335.

[31] He Jifeng, C. A. R. Hoare, M. Müller-Olm, E.-R. Olderog, M. Schenke, M. R. Hansen, A. P. Ravn, and H. Rischel. The ProCoS approach to the design of real-time systems: Linking different formalisms. FME'96 Symposium, University of Oxford, UK, March 1996. Tutorial Papers, Formal Methods Europe 96.

[32] M. G. Hinchey and J. P. Bowen, editors. *Applications of Formal Methods.* Prentice Hall International Series in Computer Science, 1995.

[33] M. G. Hinchey and J. P. Bowen. *High-Integrity System Specification and Development.* Springer-Verlag, London, 1998. In preparation.

[34] M. G. Hinchey and J. P. Bowen, editors. *Industrial-Strength Formal Methods.* International Series in Formal Methods. Academic Press, 1998. In preparation.

[35] C. A. R. Hoare and He Jifeng. Unifying theories of concurrency. In *Proc. Euro Parallel'97*, 1997.

[36] C. A. R. Hoare and He Jifeng. *Unifying Theories of Programming.* Prentice Hall International Series in Computer Science, 1998. To appear.

[37] B. Jonsson and J. Parrow, editors. *Formal Techniques in Real-Time and Fault-Tolerant Systems, 4th International Symposium, FTRTFT'96*, volume 1135 of *Lecture Notes in Computer Science.* Springer-Verlag, 1996.

[38] C. Kreitz. Formal mathematics for verifiably correct program synthesis. *Journal of the Interest Group in Pure and Applied Logics (IGPL)*, 4(1):75–94, 1996.

[39] C. Kreitz, K. Lau, and M. Ornaghi. Formal reasoning about modules, reuse, objects, and their correctness. In *International Conference on Formal and Applied Practical Reasoning*, volume 1085 of *Lecture Notes in Artificial Intelligence*, pages 384–398. Springer-Verlag, 1996.

[40] C. Kreitz, J. Otten, and S. Schmitt. Guiding program development systems by a connection based proof strategy. In M. Proietti, editor, *Logic Program Synthesis and Transformation*, volume 1048 of *Lecture Notes in Computer Science*, pages 137–151. Springer-Verlag, 1996.

[41] H. Langmaack. Contribution to Goodenough's and Gerhart's theory of software testing and verification: Relation between strong compiler test and compiler implementation verification. In C. Freksa, M. Jantzen, and R. Valk, editors, *Foundations of Computer Science: Potential, Theory, Cognition*, volume 1337 of *Lecture Notes in Computer Science*, pages 313–335. Springer-Verlag, 1997.

[42] H. Langmaack. The ProCoS approach to correct systems. *Real-Time Systems*, 13:253–275, 1997.

[43] H. Langmaack. Softwareengineering zur Zertifizierung von Systemen. *it+ti – Informationstechnik und Technische Informatik*, 39(3):41–47, 1997.

[44] H. Langmaack, W.-P. de Roever, and J. Vytopil, editors. *Formal Techniques in Real-Time and Fault-Tolerant Systems: Third International Symposium Organized Jointly with the Working Group Provably Correct Systems – ProCoS, Lübeck, Germany, 19–23 September 1994*, volume 863 of *Lecture Notes in Computer Science.* Springer-Verlag, 1994.

[45] B. Moszkowski. Some very compositional temporal properties. In E.-R. Olderog, editor, *Proc. PROCOMET'94.* Consiglio Nazionale delle Ricerche, North-Holland, 6–10 June 1994.

[46] B. Moszkowski. Compositional reasoning about projected and infinite time. In *Proc. 1st International Conference on Engineering of Complex Computer Systems (ICECCS'95)*, pages 238–245. IEEE Computer Society Press, 1995. Received award for the best paper at the conference in the formal methods track.

[47] B. Moszkowski. Using temporal fixpoints to compositionally reason about liveness. In He Jifeng, editor, *Proc. 7th BCS FACS Refinement Workshop*, Electronic Workshops in Computing. Springer-Verlag, July 1996. Invited talk.

[48] M. Müller-Olm. *Modular Compiler Verification.* Dissertation, Technische Fakultät der Universität Kiel, Germany, 1996.

[49] M. Müller-Olm. Three views on preservation of partial correctness. Verifix Technical Report [Verifix/CAU/5.1], Christian-Albrechts-Universität Kiel, Germany, 1996.

[50] M. Müller-Olm. *Modular Compiler Verification: A Refinement-Algebraic Approach Advocating Stepwise Abstraction*, volume 1283 of *Lecture Notes in Computer Science.* Springer-Verlag, 1997.

[51] E.-R. Olderog, A. P. Ravn, and J. U. Skakkebæk. Refining system requirements to program specifications. In C. Heitmeyer and D. Mandroli, editors, *Formal Methods for Real-Time Computing*, volume 5 of *Trends in Software*, pages 107–134. Wiley, 1996.

[52] H. Rischel, J. Cuellar, S. Mørk, A. P. Ravn, and I. Wildgruber. Development of safety-critical real-time systems. In M. Bartošek, J. Staudek, and J. Wiedermann, editors, *SOFSEM'95: Theory and Practice of Informatics*, volume 1012 of *Lecture Notes in Computer Science*, pages 206–235. Springer-Verlag, 1995.

[53] M. Rönkkö and A. P. Ravn. Differential equations as actions. In *Hybrid Systems V, Notre Dame, Indiana, USA*, October 1997. To appear.

[54] M. Schenke and M. Dossis. Provably correct hardware compilation using timing diagrams. Oxford University Computing Laboratory, UK, 1997. Submitted.

[55] M. Schenke and A. P. Ravn. Refinement from a control problem to programs. In Abrial et al. [1], pages 403–427.

[56] B. von Karger. An algebraic approach to temporal logic. In P. D. Mosses, M. Nielsen, and M. I. Schwartzbach, editors, *TAPSOFT'95: Theory and Practice of Software Development*, volume 915 of *Lecture Notes in Computer Science*, pages 232–246. Springer-Verlag, 1995.

[57] B. von Karger. Temporal algebra. In *Mathematical Structures in Computer Science*, 1997. To appear.

[58] B. von Karger. *Temporal Algebra.* Habilitationsschrift, Technische Fakultät der Universität Kiel, Germany, 1997. Submitted.

[59] B. von Karger and C. A. R. Hoare. Sequential calculus. *Information Processing Letters*, 53(3):123–130, 1995.