Electronic Notes in Theoretical Computer Science 21 (1999)
URL: http://www.elsevier.nl/locate/entcs/volume21.html 8 pages

Preface of ENTCS Volume 21

S.F.M. van Vlijmen

Faculty of Philosophy, Utrecht University
Heidelberglaan 8, 3584 CS, Utrecht, The Netherlands

Abstract

This document is one of the parts of the electronic version of the PhD thesis by S.F.M. van Vlijmen [26]. This document presents the motivation behind the research project, gives an outline of the thesis and the sources of the chapters. The goal of the PhD project was to get a better understanding of the problems with the integration of formal specification technique in the day to day software practice. The approach followed was to execute a number of projects in cooperation with industry on realistic cases.

Mathematically endorsed languages, techniques, methods and tools for the design, construction and maintenance of software increasingly attract attention. They are often referred to as the 'formal methods'. However, in this thesis, the term 'formal specification technique' is used to address these matters because I consider this term a more precise designation.

There is a mismatch between the promises and claims made about the usefulness and power imputed by some concerning formal specification technique and the level of acceptance it has received in the software industry. I also had the conviction that formal specification technique could solve, or at least seriously mitigate, problems encountered in practice. This is the motivation behind beginning a project i aimed at testing this hypothesis. The project was launched early in 1992 at the University of Amsterdam (UvA). From Fall 1993, the work continued at Utrecht University (UU). The motivation was boosted by societal responsibility mixed with euphoria and ignorance: this beautiful piece of theory has to be promulgated, and why isn't it used already? In retrospect, the timing of the project is not surprising. In the early nineties, the tooling matured for languages as PSF, μCRL and ASF+SDF, albeit modestly, this enabled one to handle cases far larger than the typical academic research examples.

Because the research groups at the UvA and UU were most familiar with the techniques for algebraic specification of data types and process algebra for dynamic behaviour, and because these techniques seemed to be widely applicable, they were the natural choice. Given the main target of the project, i.e., to prove the potential of the techniques, various other insights and spin-offs were expected: to better understand the application of algebraic specification in the development and maintenance of computer-based systems, to shed some light on the aforementioned mismatch, to gain feedback from practice and to find ways to bridge the gap between theory and practice.

A project strategy was formulated: create openings in certain areas in the industry (including the software industry), explore and analyze what happens when the technology is applied there, then establish lines of 'formal' work in these areas. Such an area or domain, together with the selected themes and industrial parties involved, were called bridgeheads. The idea was that others would join the effort and continue or add to the work, giving the bridgeheads a sound base, which is problem-oriented and in close contact with the realities of daily practice.

In this style, a number of case studies of realistic examples has been carried out in various areas and on various subjects in order to found bridgeheads. An important part of the work in carrying out this applied research was searching for companies with appropriate applications and setting up the projects. The experiences gained in this respect form part of the conclusion.

The thesis reports on nine cases completed between Fall 1992 and Spring 1996. Six other cases from this period have been left out because they were not completed or because the findings, which did not differ, were less outspoken. The selected cases are mostly about technical applications, and the formalisms used are mainly algebraic. This thesis will, however, discuss how the results may be carried over to formal specification technique in a more general setting.

Outline of the Thesis and Origin of the Chapters

Chapter 1 [1] starts with an introduction to software engineering issues and formal specification technique. The hypotheses to be tested follow at the end of the chapter.

The case studies are presented in Chapter 2 to Chapter 7. The first five chapters (2 to 6) give elaborate presentations. In Sections 1 to 4 four additional cases are discussed in the form of epitomes. The reason for presenting some cases elaborately and others more concisely is that the first five cases cover a range of techniques and issues: PSF in a data-oriented style, process algebra for semantics, PSF in a process-oriented style, μCRL, the modal logic for μCRL, ASF+SDF, verification and the ToolBus. The other four cases add not much new in that respect, but help to strengthen the observations.

In Chapter 8, the basic engineering notions and hypotheses as presented in the introduction, and the observations on the cases, come together in a final

[1] Note that references are made to chapters and sometimes to sections that may be stored as separate files at the ENTCS site [27]. The original text has been partitioned into: preface and the Chapters 1 to 8, each part is stored in a separate file, and each part has its own bibliography and appendices. To circumvent confusion, a reference to a part of the thesis outside the part at hand is followed by a bibliography style reference.

conclusion.

The presentations have been based on technical reports about the cases. Chapters 2, 3 and 4 were based respectively on [31], [29] and [28]; Chapter 5 was based on [11], derived texts have been published in [12] and [13]. Chapter 6 was based on a report in Dutch [18]. This was rewritten and the presentation enhanced for use in this thesis. The epitomized cases in Section 1, 2, 3 and 4 have been based respectively on [30], [19], [5] and [9]. Publication of the latter work is forthcoming (see [10]).

The work on the cases has resulted in only a few publications. Major reasons for this include the fact that the reports have been written for a different audience than usual (industrial parties instead of academics), and that the initial target within a domain was to get a project going. Publication would follow at a later stage, as it often did (which will be shown in the conclusion). Furthermore, it was considered wise to have a number of cases first and then to write about them. That is what this thesis achieves. Last but not least, publication of case studies is somewhat troublesome.

The core presentations of the cases were not updated because that would blur the historic perspective and that which was considered important or state-of-the-art at the time the case was executed. For instance, I could have pretty printed the PSF specifications with modern ASF+SDF means, but decided not to do so. Post-hoc comments have been added in separate sections, after the presentations of the original cases.

The Specification Languages Used

The various specification techniques used in this thesis are not accompanied by preliminaries, as these are easily accessible in the literature. The languages used, together with some general references, are: ACP, [4,1]; PSF, [20–22,24,25]; Synchronous Interworkings, [23]; μCRL , [14,15]; the modal logic for μCRL, [16]; ASF+SDF & ToolBus, [17,8,2,3]; and propositional logic [7].

Bas van Vlijmen
Utrecht, 23rd July 1999.

Acknowledgements

Many people contributed to this thesis. In the first place I would like to thank the companies and their people with which and with whom I cooperated. The treatment below is on alphabetical order, on company name, and includes the projects that did not make it into a chapter in this thesis. The latter are the following: Interworkings, Philips, [32]; Documentation systems, Vialle Autogas Systems; Organization models, M.M.C. Management Consultants; Real-time video and sound editing, Les Entreprises Le Gué & MM7; Traffic regulation systems, Nederland Haarlem, [6]; Implementation from algebraic specification, Holland Railconsult.

The Model Factory project took place at the premises of Digital Equipment Corporation. Ronald van Riessen, manager of the CIM group, gave us the opportunity to work on the project. Carlo Koopmans took time to show and explain the Model Factory to us. Gert Veltink (UvA) helped to get Arjan and me going with the PSF-language and the PSF Toolkit.

The two projects that were executed in cooperation with Holland Railconsult and Rail Infrabeheer are discussed in Chapter 5 and Section 3. Gea Kolk of Holland Railconsult was the central figure because she coordinated our cooperation, brought us in contact with the right people, and was last but not least able to answer many of our questions. Detailed information on the VPI, EURIS and IDEAL we received from Peter Musters, Robert Straatman, André Klap and Frits Makkinga. Peter Middelraad of Rail Infrabeheer was always available for discussions on EURIS, both on the details and on the philosophical concepts behind it, and on railway safety in general.

MM7 formed the context for a short exercise in the specification of real-time video and sound editing, this was done in cooperation with Raymond Le Gué. Jos Baeten and Alex Sellink are thanked for their contribution to conversations with MM7 on a projected requirements engineering effort for MM7.

M.M.C. Management Consultants' Erik van Hoorn put me in contact with Robert Wijnberg of Informatiebeheersing & Management. They are thanked for their time spent on the question whether organization models would lend themselves for formal specification, and if so, whether it would make sense to do so.

Three projects in this thesis were executed in cooperation with Nederland Haarlem. Jan Kroone coordinated all three projects, and in most cases he contributed also technically. Henk Spronk helped on the more technical details of traffic regulation systems and Lamp Remplace. For the Compact Dynamic Bus Station, Hans van Ruijven joined the team, and for Lamp Remplace Thom Nelissen did some work. Jan, Henk and Hans frequently took time to answer our questions, and they supplied us with clear and concise documentation. Paul Klint and Adri Steenbeek of the CWI are thanked for their assistance with ToolBus and Cplex programming respectively. Finally, without Willem van Wilsem, I, as a severe RSI sufferer at that time, would have not survived the production of the bulky Lamp Remplace reports.

Two projects were executed in cooperation with Philips Research Laboratories in Eindhoven. In the first one, the relation of PSF traces and Interworkings was studied. Thijs Winter of Philips introduced us to the Interworking formalism and gave many helpful comments on the texts we produced. Protocold was the second project, see Chapter 3. Loe Feijs from Philips was the contact in this project, he supplied us with valuable knowledge on

Protocold.

The idea to specify the interaction between the editor components (the GSE case) in PSF originates with Paul Klint, Wilco Koorn and Jan Bergstra. Wilco Koorn and Huub Bakker were a big help for understanding the intricacies of the editor. Mark van Wijk made the Interworking Toolset available to us. He also did some programming on these tools that made it possible to generate interworkings in the EPS-format.

Wiet Bouma, Kees Middelburg and Han Zuidweg of the Dutch PTT Research Centre in Leidschendam are thanked for providing us with the literature on Intelligent Networks, the ITU-T Recommendations and the SIBs. Furthermore, for having fruitful discussions on earlier versions of our texts.

Finally, Arjan and I produced a specification of a documentation system used by Vialle Autogas Systems. This in an effort to convince Erik van Hoorn of the capabilities of process algebra. He is thanked for lending his ear and for discussions about possible applications.

I thank Lieuwe Zigterman, John-Jules Meyer, Cees Middelburg, Roel Wieringa, Paul Klint, Loe Feijs and Marc Bezem for their willingness to be members of the reading and promotion commission. They also supplied me with valuable comments on the text.

Finally, many thanks go to Jan Bergstra. He arranged for me and Arjan a one year position in Amsterdam in order to make a start in the field of application of formal specification technique, and for making the first contacts, e.g. with DEC. Later, he conjured up a position in Utrecht to continue the work. His ability to open new perspectives in seemingly fixed situations is remarkable, and it has always been a joy to work and talk with him. In other words, he has been an inspiring mentor.

References

[1] J.C.M. Baeten and W.P. Weijland. *Process algebra*, volume 18 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1990.

[2] J.A. Bergstra and P. Klint. The discrete time ToolBus. In M. Wirsing and M. Nivat, editors, *Algebraic methodology and software technology AMAST'96*, volume 1101 of *LNCS*, pages 286–305. Springer-Verlag, 1996.

[3] J.A. Bergstra and P. Klint. The ToolBus coordination architecture. In P. Ciancarini and C. Hankin, editors, *Coordination Languages and Models COORDINATION '96*, volume 1061 of *LNCS*, pages 75–88. Springer-Verlag, 1996.

[4] J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Computation*, 60(1/3):109–137, 1984.

[5] R.N. Bol, J.W.C. Koorn, L.H. Oei, and S.F.M. van Vlijmen. Syntax and static semantics of the interlocking design and application language. Technical Report P9422, University of Amsterdam, Programming Research Group, 1994.

[6] T.H.P.F. Bullens. Algebraic specification of a distributed traffic regulation system. Work placement report, 1994.

[7] D. van Dalen. *Logic and structure*. Springer-Verlag, 1989.

[8] A. van Deursen, J. Heering, and P. Klint, editors. *Language prototyping, an algebraic approach*, volume 5 of *AMAST Series in Computing*. World Scientific, 1996.

[9] F.A. van der Duyn Schouten, A.S. Klusener, S.F.M. van Vlijmen, and S.L.E. Vos de Wael. Een beslissingsondersteunend systeem voor lampremplace. Technical report, Utrecht University, Logic Group Preprint Series of the Department of Philosophy, 1996. In Dutch, confidential.

[10] Frank van der Duyn Schouten, Bas van Vlijmen, and Stefan Vos de Wael. Replacement policies for traffic control systems. *IMA Journal of Mathematics Applied in Business and Industry*, 9(4), 1998.

[11] J.F. Groote, J.W.C. Koorn, and S.F.M. van Vlijmen. The safety guaranteeing system at station Hoorn–Kersenboogerd. Technical Report 121, Utrecht University, Logic Group Preprint Series of the Department of Philosophy, 1994.

[12] J.F. Groote, J.W.C. Koorn, and S.F.M. van Vlijmen. Formele analyse van het veiligheidssysteem op het station van Hoorn–Kersenboogerd. *Informatie*, pages 397–404, June 1995. In Dutch.

[13] J.F. Groote, J.W.C. Koorn, and S.F.M. van Vlijmen. The safety guaranteeing system at station Hoorn–Kersenboogerd. In *Proceedings of the Tenth Annual Conference on Computer Assurance, Compass'95*, pages 57–68. IEEE, 1995. IEEE catalog number: 95CH35802.

[14] J.F. Groote and A. Ponse. Proof theory for μCRL: a language for processes with data. In D.J. Andrews, J.F. Groote, and C.A. Middelburg, editors, *Proceedings of the International Workshop on Semantics of Specification Languages*, pages 232–251. Springer-Verlag, 1994. WICS.

[15] J.F. Groote and A. Ponse. Syntax and semantics of μCRL. In A. Ponse, C. Verhoef, and S.F.M. van Vlijmen, editors, *Algebra of communicating processes, Utrecht 1994*, pages 26–62. Springer-Verlag, 1995. WICS.

[16] J.F. Groote and S.F.M. van Vlijmen. A modal logic for μCRL. In A. Ponse, M. de Rijke, and Y. Venema, editors, *Modal logic and process algebra, a bisimulation perspective*, volume 53 of *CSLI lecture notes*, pages 131–150, Stanford, California, 1995. CSLI.

[17] P. Klint. A meta-environment for generating programming environments. *ACM Transactions on Software Engineering and Methodology*, 2(2):176–201, 1993.

[18] A.S. Klusener, S.F.M. van Vlijmen, and A. Schrijver. Compact dynamisch busstation. Technical Report CS–N9601, National Research Institute for Mathematics and Computer Science (CWI), 1996. In Dutch.

[19] A.S. Klusener, S.F.M. van Vlijmen, and A. van Waveren. Service independent building blocks-I; concepts, examples and formal specifications. Technical Report P9310, University of Amsterdam, Programming Research Group, 1993. Also available as CWI report CS-R9326.

[20] S. Mauw and G.J. Veltink. An introduction to PSFd. In J. Diaz and F. Orejas, editors, *Proc. International Joint Conference on Theory and Practice of Software Development TAPSOFT '89*, volume 352 of *LNCS*, pages 272–285. Springer-Verlag, 1989.

[21] S. Mauw and G.J. Veltink. A process specification formalism. *Fundamenta Informaticae*, XIII:85–139, 1990.

[22] S. Mauw and G.J. Veltink, editors. *Algebraic specification of communication protocols*, volume 36 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1993.

[23] S. Mauw, M. van Wijk, and T. Winter. A formal semantics of synchronous Interworkings. In O. Færgemand and A. Sarma, editors, *SDL'93: Using Objects*, Proceedings of the Sixth SDL Forum, pages 167–178, Darmstadt, 1993. Amsterdam, North-Holland.

[24] G.J. Veltink. The PSF toolkit. *Computer Networks and ISDN Systems*, 25:875–898, 1993. Elsevier Science Publishers.

[25] G.J. Veltink. *Tools for PSF*. PhD thesis, University of Amsterdam, 1995.

[26] S.F.M. van Vlijmen. *Algebraic Specification in Action*. PhD thesis, Universiteit Utrecht, dept. of Philosophy, 1998. In Quaestiones infinitae, vol. 26.

[27] S.F.M. van Vlijmen. *Algebraic Specification in Action*, volume 21 of *Electronic Notes in Theoretical Computer Science (ENTCS)*. Elsevier Science, 1999. `http://www.elsevier.nl/locate/entcs/volume21.html`.

[28] S.F.M. van Vlijmen, P.N. Vriend, and A. van Waveren. Control and data transfer in the distributed editor of the ASF+SDF Meta–environment. Technical Report P9415, University of Amsterdam, Programming Research Group, 1994.

[29] S.F.M. van Vlijmen and J.J. van Wamel. A semantic approach to Protocold using process algebra. Technical Report P9317, University of Amsterdam, Programming Research Group, 1993.

[30] S.F.M. van Vlijmen and A. van Waveren. An algebraic specification of a model factory. Technical Report P9209, University of Amsterdam, Programming Research Group, 1992.

[31] S.F.M. van Vlijmen and A. van Waveren. Algebraic specification of a system for traffic regulation at signalized intersections. Technical Report P9313, University of Amsterdam, Programming Research Group, 1993.

[32] S.F.M. van Vlijmen and A. van Waveren. On generating synchronous interworkings from PSF process traces. Technical Report P9304, University of Amsterdam, Programming Research Group, 1993.