Project Number:	IST-2001-33100
Project Acronym:	PROFUNDIS
Title :	Proofs of Functionality for Mobile Distributed Systems

Deliverable 12: Summary of Dissemination Activities Year 2

Preparation date:	8 January 2003
Classification:	Public
Contract start date	1 January 2002
Duration:	3 years
Project co-ordinator:	Joachim Parrow
Partners:	Univ. Uppsala, Sweden Univ. Pisa, Italy INRIA, France Univ. FFCT, Portugal

PROFUNDIS Deliverable 12: Summary of Dissemination Activities Year 2

February 11, 2004

1 Executive Summary

The work in PROFUNDIS has been successful in year 2 (2003), with only minor deviations from the Technical Annex (TA) and from the Dissemination and Use Plan (DUP). An elaboration of what has been accomplished can be found in the Periodic Progress Report (PPR) for year 2. The present document contains a summary of dissemination activities in PROFUNDIS year 2.

The main form of dissemination for PROFUNDIS at this stage is through publications in scientific conferences, workshops and journals. Here we have been successful with 20 peer reviewed publications, 5 invited contributions and 24 other reports, several of which are being submitted.

There has been one general PROFUNDIS workshop and 9 visits between partners, sometimes involving several persons. These indirectly contribute also to dissemination outside the project, since visitors often give presentations attracting an external audience.

There have been 30 visits from project members to sites outside the project in order to present parts of the project. These visits range from lecture series at summer schools and invited talks at conferences to more informal presentations. The number is almost twice that of the previous year and the many invitations confirm our impression that PROFUNDIS is well regarded in the scientific community.

6 websites with links to papers and tools have been created.

2 Overview of the Work Packages

PROFUNDIS consists of three technical Work Packages (WPs) outlined below. A fourth WP is devoted to project management and is given no special consideration in the DUP.

WP1

The objectives of the Work Package consist of the development of a HD-Automata model, suitable for finite-state verification, enhanced with additional capabilities like name fusions and substitutions. Also, versions of mobile calculi should be defined, e.g. for the symbolic analysis of security protocols. A verification environment should be designed and implemented, equipped with a general, open architecture and consisting of new tools realizing the models and the verification methods above. Several case studies should show the flexibility and effectiveness of our approach.

WP2

The objectives of the Work Package are to develop new logics to support the verification of structural (spatial) and behavioural properties of concurrent mobile systems, and to develop proof systems for these logics based on sequent calculi. A tool for the logical framework should be built, integrated in the verification environment developed together with other tasks. The usefulness of the approach should be illustrated by several case studies.

WP3

The objectives are to develop new type systems to control interferences among processes and the resources used by the processes [Task 3.1]; to integrate the type techniques with operational and logic techniques [Task 3.2]; to investigate the robustness of the type techniques and their algorithmic definitions [Task 3.3]; to assess the applicability of the techniques by means of case studies, and to implement some of the type algorithms and proof techniques.

3 Publications

The project has in the second year produced a total of 49 papers, out of which 20 have already passed an international peer review process to be accepted for publication at a conference or journal. This represents a substantial effort and demonstrates our committment to follow established scientific routes for dissemination of results. The complete list of papers is at the end of this report.

4 Web Presence

- `http://www.it.uu.se/profundis` is the project main web page. It includes:
  - A main page with synopsis of overview and pointers to all other resources.
  - A project overview, related projects, and a list of official (yearly) progress reports.
  - A list of meetings, with links to files for each meeting.
  - A list of visits.
  - A list of events, with links to the main web page of each event.
  - A list of publications reporting the work done within the project.
  - Links to all delivered software.
- `http://jordie.di.unipi.it:8080/pweb` is a web site for the distributed PROFUNDIS tools. Here the tools STA, pi-compiler, Reducer, MWB and Trust can be accessed in a general framework.
- `http://www.cmi.univ-mrs.fr/~vvanacke/trust.html` is a web site for the TRUST tool.
- `http://rep1.iei.pi.cnr.it/projects/JACK/hal.html` is the web site for the HAL tool.
- `http://www.it.uu.se/research/docs/fm/mobility/mwb` is the web site for the MWB tool.
- `http://www.dsi.unifi.it/ boreale/tool.html` is the web site of the STA tool.

5 Project meetings

There has been one formal PROFUNDIS meeting, at Rovereto, March 8-10 2003, with around 30 participants. All sites were well represented, there were technical presentations from all Work Packages and a PROFUNDIS business meeting.

6 Visits between members of the project

In order to continue collaboration and disseminate progress from different sites the following 9 visits have been made. Note that some of these involve several people visiting simultaneously.

1. January 2003: G. Ferrari, R. Raggi and E. Tuosto (Pisa) visited Uppsala for four days to work on the design and implementation of the PROFUNDIS WEB and on the definition of a finite state automata-like model for the fusion calculus.
2. March 2003: L Caires and L. Monteiro (Lisbon) visited D. Hirschkoff and E. Lozes at the University of Lyon for four days.
3. March 2003: D. Hirschkoff and E. Lozes (Lyon) visited D. Sangiorgi (Bologna) for four days to work on the expressiveness of the spatial logics for concurrency.
4. April 2003: M. Baldamus (Uppsala) visited Pisa for two weeks to work co-algebraic models for the Fusion Calculus.
5. April 2003: V. Vanackère (INRIA) visited Pisa for one week to work on the integration of the TRUST tool into the PROFUNDIS verification environment.
6. June 2003: M. Baldamus (Uppsala) visited Pisa for twelve days to work on the design of the XML types for the data exchanges inside the PROFUNDIS Web.
7. October 2003: M. Johansson (Uppsala) visited Pisa for one month to start the activity on the development of new verification techniques based on the exploitation of type information.
8. October-November 2003: E. Tuosto (Pisa) visited Uppsala for three weeks to work on the definition of HD-automata with name fusions and substitutions.
9. December 2003: R. Raggi (Pisa) visited Uppsala for one week to work on the design and implementation of the directory service for the PWeb.

7 Visits and talks by project members outside PROFUNDIS

On 30 occasions PROFUNDIS researchers have travelled outside their sites to present ongoing PROFUNDIS work. Though most of these trips entailed a single presentation some trips gave rise to several presentations or a series of lectures at research schools. PROFUNDIS now have been truly globally disseminated with visits to both Uruguay and Australia, although the vast majority understandably is within Europe.

1. January 2003: R. Amadio gave a talk at the University of Munich, on the reachability problem for the π-calculus.
2. January 2003: S. Dal Zilio presented his work on the Workshop on Types for Global Computing organised in Paris.
3. January 2003: D. Hirschkoff lectured at the Torino-Chambéry Winter School in Theoretical Computer Science in Aussois (France), also presenting some work done in PROFUNDIS on type systems.
4. February 2003: R. Amadio presented a talk on the Dolev-Yao model at University Paris 7.
5. February 2003: R. Amadio presented a talk on the Reachability problem in the Dolev-Yao model, at a meeting of the French research initiative "AS Sécurité" in Cachan (France).
6. March 2003: L. Caires partipated in the Special Workshop on Spatial Logics at the University of Nottingham during the APPSEM II meeting, and gave a talk on model-checking spatial logics.
7. March 2003: A. Ravara gave a talk at the Department of Computer Science, Aalborg University, Denmark, about "Session Types for Inter-Process Communication".
8. March 2003: D. Hirschkoff organised the second meeting of the french AS CNRS "Méthodes formelles pour la mobilité", in Lyon. Talks related to WP2 and WP3 were given at this occasion, both by people inside and outside PROFUNDIS.
9. May 2003: M. Buscemi has presented a talk on a typed bialgebraic model for open π-calculus at the Workshop of the Italian project Cometa in Como.
10. May 2003: A. Ravara participated in a meeting involving the GC projects that work on type systems in Sussex.
11. June 2003: D. Teller presented his work on types for resource control at the *"Foundations of Global Computation"* workshop, a satellite workshop of ICALP'03, in Eindhoven.
12. June 2003: R. Amadio presented his work on Max-plus quasi-interpretations at the TLCA'03 conference.
13. June 2003: G. Ferrari gave a talk on the PROFUNDIS Web at a meeting of the Italian Research Initiative on Software Architectures called "SAHARA" hels in Pisa. A demonstration of a verification session on the PWeb was also given.
14. June 2003: S. Dal Zilio presented his work on Logic for semi-structured data at the RTA'2003 conference in Valencia (Spain).

15. July 2003: U. Montanari gave a talk on modeling quality of (web) services at the International Symposium on Verification, Taormina.

16. July 2003: R. Amadio gave a talk at the Process Algebra Workshop held in Bertinoro (Italy) on Max-plus quasi-interpretations.

17. July 2003: U. Montanari gave a talk on Tile Logic at the Process Algebra Workshop held in Bertinoro (Italy).

18. July 2003: D. Sangiorgi lectured at the International Winter School on Semantics and Applications in Montevideo (Uruguay). Sangiorgi gave eight lectures on the topic of types for mobility, partly presenting work done under the WP "Types" of the PROFUNDIS project.

19. July 2003: D. Sangiorgi lectured at the European Educational Forum Global Computing Summer School 2003 in Edinburgh (United Kingdom). This school was organised as part of the initiatives under the "Global Computing" programme.

20. September 2003: U. Montanari gave an advanced lecture on Coordinating Mobile Processes at the 4th Advanced Course on Petri Nets, Eichstätt.

21. September 2003: E. Lozes presented two talks, at the Express (on the expressiveness of the Static Ambient Logic) workshop and at the FMM workshop (on minimality results for Spatial Logics), two satellites workshops of CONCUR'03, in Marseille.

22. September 2003: A. Ravara gave a talk at Project Mimosa, INRIA Sophia-Antipolis, France about his work on type systems.

23. September 2003: D. Sangiorgi lectured at the Advanced School on Mobile Computing in Pisa (Italy) on the topic of types for mobility, partly presenting work that has been done in WP3.

24. September 2003: At the conference SEFM'03 (Software Engineering and Formal Methods) Sangiorgi gave an invited lecture, whose title was "Timing processes using types". Further, in the tutorial sessions of the same conference Sangiorgi gave a 4-hour tutorial on "mobile processes", where he has also presented work carried out within PROFUNDIS and other GC projects. Sangiorgi gave further lectures on the same topic at the University of Queensland (in Brisbane, where SEFM'03 was held).

25. October 2003: Teller gave a presentation about the π-calculus at the Xerox Research Center in Grenoble (France), where he described some work related to PROFUNDIS WP3.

26. December 2004: E. Tuosto gave a talk on the PROFUNDIS Web at a meeting of the Italian Research initiative called "*Architetture Software ad Alta Qualità di Servizio per Global Computing su Cooperative Wide Area Networks*" held in Milano (Italy). A demonstration of a verification session of Security Protocols on the PWeb was also given.

27. December 2004: G. Baldi and E. Tuosto gave a talk on the toolkit of the PWeb called ASPASYA at a meeting of the Italian Research initiative called "NAPOLI" held in Pisa (Italy). A demonstration of a verification session of Security Protocols was also given.

28. December 2003: M. Buscemi presented a talk on DFusion at the Workshop of the Italian project Cometa in Udine.

29. December 2003: G. Ferrari gave a talk on the exploitation of MetaKlaim to develop and compose WEB Services at a meeting of the Italian Research initiative called "NAPOLI" held in Pisa (Italy).

30. December 2003: K. Yemane (Uppsala) visited Department of Mathematics and Computer Science, University of Leicester for one month, working on higher order abstract syntax and coalgebraic semantics of mobile calculi.

Articles and reports produced by PROFUNDIS year 2

Reviewed Publications

[1] M. Baldamus, J. Bengtson, G. Ferrari, and R. Raggi. Web-Services as a New Approach to Distributing and Coordinating Semantics-Based Verification Toolkits. In *Web Services and Formal Methods*, 2004. WS-FM workshop proceedings, to appear.

[2] G. Barthe, A. Basu, and T. Rezk. Security Types Preserving Compilation. In *Proc. of VMCAI'04*, LNCS. Springer Verlag, 2004. to appear.

[3] M. Boreale and M. Buscemi. Symbolic analysis of crypto-protocols based on modular exponentiation. In *Proc. of MFCS 2003*, Lecture Notes in Computer Science 2747. Springer-Verlag, 2003. An extended version appears in Proc. of FCS'03.

[4] L. Caires. Behavioral and spatial properties in a logic for the pi-calculus. In Igor Walukiwicz, editor, *Proc. of Foundations of Software Science and Computation Structures'2004*, Lecture Notes in Computer Science. Springer Verlag, 2003.

[5] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part I). *Information and Computation*, 186(2):194–235, 2003.

[6] L. Caires and L. Cardelli. A Spatial Logic for Concurrency (Part II). *Theoretical Computer Science*, to appear.

[7] Witold Charatonik, Silvano Dal Zilio, Andrew D. Gordon, Supratik Mukhopadhyay, and Jean-Marc Talbot. Model checking mobile ambients. *Theoretical Computer Science*, 308(1):277–331, November 2003.

[8] Silvano Dal Zilio and Denis Lugiez. XML schema, tree logic and sheaves automata. In *RTA 2003 – 14th International Conference on Rewriting Techniques and Applications*, volume 2706 of *Lecture Notes in Computer Science*, pages 246–263. Springer, June 2003.

[9] Silvano Dal Zilio and Denis Lugiez. A logic you can count on. In *POPL 2004 – 31st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 2004.

[10] M. Miculan F. Gadducci and U. Montanari. Some characterization results for permutation algebras. In *Workshop COMETA*, ENTCS. Elsevier, 2003. to appear.

[11] G. Ferrari, S. Gnesi, U. Montanari, and M. Pistore. A model checking verification environment for mobile processes. *ACM Transactions on Software Engineering and Methodologies (TOSEM)*, To appear, 2004.

[12] G. Ferrari, U. Montanari, R. Raggi, and E. Tuosto. From co-algebraic specifications to implementation: The mihda toolkit. In *First International Symposium on Formal Methods for Components and Objects (FMCO)*, Springer Lecture Notes in Computer Science. Springer, 2003.

[13] P. Giambiagi, G. Schneider, and F. Valencia. On the expressiveness of ccs-like calculi. In *In Proceedings of FOSSACS'04*. LNCS, Springer-Verlag, 2004.

[14] D. Hirschkoff, E. Lozes, and D. Sangiorgi. Minimality results for the spatial logics. In *Proc. of FSTTCS'2003*, LNCS. Springer Verlag, 2003.

[15] E. Lozes. Adjunct elimination in the static Ambient Logic. In *Proc. of EXPRESS'2003*, 2003. to appear in ENTCS, Elsevier.

[16] A. Ravara, A. G. Matos, V. T. Vasconcelos, and L. Lopes. Lexically scoped distribution: what you see is what you get. *Electronic Notes in Theoretical Computer Science*, 85(1), 2003. Presented at FGC'03.

[17] David Teller. Formalisms for mobile resource control. *Electronic Notes in Theoretical Computer Science*, 85(1), 2003. Presented at FGC'03.

[18] F. Valencia. Timed concurrent constraint programming: Decidability results and their application to ltl. In *Proceedings of the Nineteenth International Conference on Logic Programming (ICLP 2003)*. LNCS, Springer-Verlag, 2003.

[19] A. Vallecillo, V. T. Vasconcelos, and A. Ravara. Typing the behavior of objects and components using session types. *Electronic Notes in Theoretical Computer Science*, 68(3), 2003. Presented at FOCLASA'02.

[20] V. Vanackere. History-dependent scheduling for cryptographic processes. In *Proc. VMCAI 2004*, Springer Lecture Notes in Computer Science. Springer, 2004. to appear.

Invited Publications

[21] M. Bartoletti, P. Degano, and G. Ferrari. Stack Inspection and Secure Program Transformations. *International Journal of Information Security*, 2003. To appear.

[22] L.Bettini, V.Bono, R.De Nicola, G.Ferrari, D.Gorla, M.Loreti, E.Moggi, R.Pugliese, E.Tuosto, and B.Venneri. The klaim project: Theory and practice. In C.Priami, editor, *Global Computing: Programming Environments, Languages, Security and Analysis of Systems*, number 2874 in LNCS, 2003.

[23] Mogens Nielsen and Frank Valencia. Notes on timed ccp. In *4th Advanced Course on Petri Nets ICPN'03*. LNCS, Springer-Verlag, 2004.

[24] D. Teller, P. Zimmer, and D. Hirschkoff. Using Ambients to Control Resources (long version). *International Journal of Information Security*, 2003. to appear.

[25] F. Valencia. Concurrency, time and constraints. In *Proceedings of the Nineteenth International Conference on Logic Programming (ICLP 2003)*. LNCS, Springer-Verlag, 2003. WP2, Invited publication.

Other: Papers Submitted for Publication, Reports, Drafts)

[26] M. Baldamus. A Fully-Abstract Model for the Fusion Calculus. Preliminary Draft, 2003.

[27] M. Baldamus, R. Mayr, and G. Schneider. A Backward/Forward Strategy for Verifying Safety Properties of Infinite-State Systems. Technical Report 2003-065, Department of Information Technology, Uppsala University, Sweden, 2003.

[28] M. Baldamus, J. Parrow, and B. Victor. Spi Calculus Translated to π-Calculus Preserving May Testing. Technical Report 2003-063, Department of Information Technology, Uppsala University, Sweden, 2003.

[29] G. Baldi, A. Bracciali, G. Ferrari, and E. Tuosto. ASPASyA: an automated tool for security protocol analysis based on a symbolic approach. Submitted for publication, 2003.

[30] G. Barthe and L. Prensa Nieto. Formally Verifying Information Flow Type Systems for Concurrent and Thread Systems. manuscript.

[31] G. Barthe and T. Rezk. Secure Information Flow for the JVM. manuscript.

[32] M. Boreale, M. Buscemi, and U. Montanari. The distinctive fusion calculus. Unpublished draft, 2003.

[33] M. Buscemi. *Models and Security Verification of Mobile Systems*. PhD thesis, Dipartimento di Matematica, University of Neaples “Federico II”, 2003.

[34] M. Buscemi and U. Montanari. A compositional coalgebraic model of explicit fusions. Unpublished draft, 2003.

[35] G. Ferrari, S. Gnesi, U. Montanari, R. Raggi, G. Trentanni, and E. Tuosto. Verification on the web of mobile processes. Submitted for publication, 2003.

[36] G. Ferrari, U. Montanari, and E. Tuosto. Co-algebraic minimization of hd-automa in a polymorphic λ-calculus. Under Revision for Theoretical Computer Science, 2003.

[37] G. Ferrari, U. Montanari, E. Tuosto, B. Victor, and K. Yemane. Modelling and minimising the fusion calculus using hd-automata. Technical report, University of Pisa, 2003.

[38] Simon Gay, Vasco T. Vasconcelos, and António Ravara. Session types for inter-process communication. TR 2003–133, Department of Computing, University of Glasgow, March 2003.

[39] I. Lanese and U. Montanari. Mapping fusion and synchronized hyperedge replacement into logic programming. Under Revision for Theory and Practice of Logic Programming, 2003.

[40] F. Martins and A. Ravara. Typing migration control in lsdpi. Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2003. Submitted for publication.

[41] L. Monteiro. A note on a noninterleaving model of concurrency based on transition systems with spatial structure. Technical Note, DI-FCT/UNL, 2003.

[42] L. Monteiro. A note on models for spatial logic based on transition systems with spatial structure. Technical Note, DI-FCT/UNL, 2003.

[43] A. Ravara, P. Resende, and V. Vasconcelos. An algebra of behavioural types. Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2003. Submitted for publication.

[44] A. Ribeiro, L. Caires, and L. Monteiro. Verifying the Arrow Protocol in a Spatial Logic. Technical report, Departamento de Informatica, FCT/UNL, 2003.

[45] C. Rueda and F. Valencia. Non-viability deductions in arc-consistency computation. Technical report, 2003. WP1, Submitted for conference publication.

[46] E. Tuosto. *Non Functional Aspects of Wide area Network Programming.* PhD thesis, Dipartimento di Informatica, Univ. Pisa, 2003.

[47] E. Tuosto, B. Victor, and K. Yemane. Polyadic history-dependent automata for the fusion calculus. Technical Report 2003-062, Department of Information Technology, Uppsala University, December 2003.

[48] F. Valencia. On the decidability of timed ccp. Technical report, Dec 2003. WP2, Submitted to the Journal of Theoretical Computer Science.

[49] H. Vieira and L. Caires. Spatial Model Checker User's Manual. Technical report, Departamento de Informatica, FCT/UNL, 2003.