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

Deliverable 11: Summary of Dissemination Activities Year 1

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 11: Summary of Dissemination Activities Year 1

January 8, 2003

1 Summary

The work in PROFUNDIS has been successful in year 1 (2002), 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 1. The present document contains a summary of dissemination activities in PROFUNDIS.

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 18 peer reviewed publications and several other reports.

There has been one general PROFUNDIS workshop, two minor project meetings on particalar topics, and seven visits between partners. These indirectly contribute also to dissemination outside the project, since visitors often give presentations attracting an audience from outside the project.

There have been 16 visits from project members to sites outside the project in order to present parts of the project. These visits range from invited talks at conferences to more informal presentations.

A website with links to papers and tools has 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 produced a total of 32 papers, out of which 18 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

A project web page, `http://www.it.uu.se/profundis`, has been set up by the coordinator. 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.

5 Project meetings

There has been one formal PROFUNDIS meeting, at INRIA 25–27 April 2002, with around 30 participants. All sites were well represented, there were technical presentations from all work packages and a PROFUNDIS business meeting.

The TA calls for only one PROFUNDIS meeting per year. Nervertheless the following impromptu meetings have been organized on a less formal basis, mainly to ensure the collaboration for the tool development in WP1:

1. (Pisa June 10 - 11) The main results of this meeting have been the identification and the preliminary design of the PROFUNDIS Verification Environment.

   The participants are listed in the following table.

UU	B. Victor, M. Baldamus, M. Johansson
FFCT	L. Caires, L. Monteiro
INRIA	D. Hirschkoff
PISA	U. Montanari, S. Gnesi, G. Ferrari, E. Tuosto,
	M. Boreale, R. Raggi, G. Buscemi

2. (Pisa September 16) The main result of the meeting has been the design of the format for data exchanging among the components of the PROFUNDIS Verification Environment.

   The participants are listed in the following table.

UU	B. Victor, M. Baldamus, M. Johansson
FFCT	L. Monteiro
PISA	U. Montanari, S. Gnesi, G. Ferrari, E. Tuosto,
	M. Boreale, R. Raggi, G. Buscemi

6 Visits between members of the project

In order to continue collaboration and disseminate progress from different sites the following intraproject visits have been made:

1. January 2002: Levi (Pisa) has visited Inria Sophia Antipolis for 2 weeks to work with Sangiorgi on the formalisation of interferences.
2. January – June 2002: Ravara (Lisbon) has visited Inria Sophia Antipolis for 6 months. Although this visit has not been directly funded by PROFUNDIS (the funding came from a grant from Portuguese government;

PROFUNDIS has only supported the travels of Ravara while at Inria), types for mobile processes was the scientific topic for the visit, and indeed most of the contributions of Ravara in WP3 have been carried out during the period at Inria.

3. January – July 2002: Lozes spent 6 months in Lisbon for his PhD, co-directed between Lisbon and Lyon.
4. September 2002: Yemane (UU) has visited Pisa for one month. During this visit work on HD automata with fusions and substitutions has started.
5. September 2002: Monteiro (FFCT) has visited Pisa for three weeks. During this visit work on models for spatial logics based on variations of HD-automata has started.
6. November 2002: Baldamus (UU) has visited Pisa for two weeks. During this visit the data format for the interoperation among the components of the PROFUNDIS Verification Environment has been completed and experimented about.
7. December 2002: Hirschkoff and Lozes visited Lisbon for 3 days to discuss Lozes' PhD.

7 Visits and talks by project members outside PROFUNDIS

1. February 2002: Montanari has given an invited talk titled *History Dependent Automata* at the Logic and Interaction Programme, January 28th - March 1st 2002,Luminy.
2. February 2002: Caires, Lozes and Monteiro presented their work in Lisbon (in the context of a joint workshop of FET projects with portuguese participation).
3. March 2002: Caires has given an invited talk on spatial logics for concurrency, at a special session on spatial logics of the MFPS'02 (Tulane, New Orleans, USA) organized by Philippa Gardner and Peter O'Hearn.
4. August 2002: Sangiorgi has given an invited talk on the topic of Task 3.2 at CONCUR 02 (Brno)
5. August 2002– Amadio visits Munich for 6 months to discuss with the people involved in the MSR GC projects and has given a talk on his work in Task 3.1.
6. September 2002: Hirschkoff visited the University of Turin for 1 week where he discussed, among other topics, the work on expressiveness of spatial logic, and gave a talk on his work in Task 3.1 (control of resources).

7. September 2002: Sangiorgi has lectured at the "TYPES Summer School'02" on "Types for Mobile Process" (the topic of WP3), also presenting some of the results obtained by PROFUNDIS and briefly presenting the FET GC initiative.

8. September 2002: Sangiorgi has visited UPenn for 1 week to discuss with the local people working on Active Networks, and has given a talk on his work in Task 3.2

9. September 2002: Ferrari and Montanari presented the features and the prototype implementation of the Profundis Verification Environment within the context of a national technology transfer project. The industrial partners of the project (Telecom Italia Lab and Think3) will test and exploit the prototype implementation of the environment to specify and verify properties of two case studies.

10. October 2002: Montanari has given an invited opening talk titled *Bialgebras for HD-Automata* at the Fifth Brazilian Workshop on Formal Methods, Gramado, October 2002.

11. November 2002: Montanari has given an invited talk titled *HD-Automata: Foundations and Implemerntation* at the First International Symposium on Formal Methods for Objects and Components (FMCO 2002), Leiden, November 2002.

12. November 2002: Caires visited Paris and Orsay for 1 week, and gave a talk about spatial logics at PPS Jussieu.

13. December 2002: Dal Zilio presented the work on XML Schema and Sheaves Automata at a meeting of the Action Spécifique “Mobilité” (project “Outils mathematiques pour l'informatique” - CNRS) in Paris.

14. December 2002: Lozes presented his work on Spatial Logics at a meeting of the Action Spécifique “Mobilité” (project “Outils mathematiques pour l'informatique” - CNRS) in Paris.

15. December 2002: Caires visited Cambridge for 1 week, and gave a talk about spatial logics and model-checking.

16. December 2002: Sangiorgi has visited Paris 6 for 1 week to discuss with the local people working on Types and Logics, and has given a talk on his work in Task 3.2

References

[1] R. Amadio and W. Charatonik. On name generation and set-based analysis in Dolev-Yao model (extended abstract). In *Proc. CONCUR'02*, volume 2421 of *LNCS*. Springer Verlag, 2002.

[2] R. Amadio, D. Lugiez, and V. Vanackere. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, To appear.

[3] R. Amadio and C. Meyssonnier. On decidability of the control reachability problem in the asynchronous pi-calculus. *Nordic Journal of Computing*, 9(2):70–101, 2002.

[4] R. M. Amadio, G. Boudol, and C. Lhoussaine. On message deliverability and non-uniform receptivity. Research report 05-2002, LIF, Marseille, France, May 2002. Accepted for pubblication in Fundamenta Informaticae.

[5] M. Boreale and M. Buscemi. A framework for the analysis of security protocols. In *Proc. CONCUR'02*, volume 2421 of *LNCS*. Springer Verlag, 2002.

[6] M. Boreale and M. Buscemi. *STA, a Tool for the Analysis of Cryptographic Protocols (Online version)*. Dipartimento di Sistemi ed Informatica, Università di Firenze, and Dipartimento di Informatica, Università di Pisa,, http://www.dsi.unifi.it/ boreale/tool.html, 2002.

[7] A. Bracciali, A. Brogi, G. Ferrari, and E. Tuosto. Security and dynamic composition of web services. In *Proc. Int. Conference on Parallel and Distributed Techniques and applications*. CSREA Press, USA, 2002.

[8] M. Buscemi and U. Montanari. A first order coalgebraic model of pi-calculus early observational equivalence. In *Proc. CONCUR'02*, volume 2421 of *LNCS*. Springer Verlag, 2002. Full version in Technical Report TR-02-14, Dipartimento di Informatica, Universitá di Pisa, August 2002.

[9] L. Caires. Model-checking of spatial properties in the pi-calculus. Research report 3, DI/FCT/UNL, December 2002.

[10] L. Caires and L. Cardelli. A spatial logic for concurrency (part i). *Information and Computation*, 2002. Accepted for publication.

[11] L. Caires and L. Cardelli. A spatial logic for concurrency (part ii). In *CONCUR 2002: Concurrency Theory (13th International Conference)*, Berlin, 2002. Lecture Notes in Computer Science. Springer-Verlag. Also as Technical Report 3/2002/DI/PLM/FCTUNL.

[12] G. Ferrari, S. Gnesi, U. Montanari, and M. Pistore. A model checking verification environment for mobile processes. *Submitted to ACM TOSEM (under revision)*, 2002.

[13] G. Ferrari, S. Gnesi, U. Montanari, R. Raggi, G. Trentanni, and E. Tuosto. Verification on the web. Technical Report TR-02-18, Dipartimento di Informatica, Università di Pisa, 2002.

[14] G. Ferrari, E. Moggi, and R. Pugliese. Guardians for ambient based monitoring. In *Proc. Foundations of Wide Area Network Programming*, ENTCS. Elseviers, 2002.

[15] G. Ferrari, E. Moggi, and R. Pugliese. Metaklaim: A type safe multi-stage language for global computing. Technical Report Under revision for Mathematical Structures in Computer Science, 2002.

[16] G. Ferrari, U. Montanari, and M. Pistore. Minimizing transition systems for name-passing calculi: A co-algbraic formulation. In *Proc. FOSSACS'02*, volume 2303 of *LNCS*. Springer Verlag, 2002.

[17] G. Ferrari, U. Montanari, R. Raggi, and E. Tuosto. From coalgebraic specification to toolkit development. Technical Report TR-02-19, Technical Report, Dipartimento di Informatica Universita' di Pisa, 2002.

[18] S. Gay, V. T. Vasconcelos, and A. Ravara. Session types for inter-process communication. Preprint, Department of Computer Science, University of Lisbon, Campo Grande, Edifcio C5, 1749-016 Lisboa, Portugal, 2002. Submitted for publication.

[19] P. Giannini, D. Sangiorgi, and A. Valente. A distributed abstract machine for Safe Ambients. Extended and refined version of a paper appeared in *Icalp.01*, 2002.

[20] D. Hirschkoff, E. Lozes, and D. Sangiorgi. Separability, Expressiveness and Decidability in the Ambient Logic. In *Proc. of LICS'02*, 2002.

[21] F. Levi and D. Sangiorgi. Mobile safe ambients. To appear in the TOPLAS journal. Extended and refined version of a paper appeared in *Proc. 27th POPL*, ACM Press, 2002.

[22] D. Lugiez and S. D. Zilio. Multitrees Automata, Presburger's Constraints and Tree Logics. Research report 08-2002, LIF, Marseille, France, June 2002. http://www.lim.univ-mrs.fr/Rapports/08-2002-Lugiez-DalZilio.html.

[23] D. Lugiez and S. D. Zilio. XML Schema, Tree Logic and Sheaves Automata. Research report 4631, INRIA, November 2002. http://www.inria.fr/rrrt/rr-4631.html.

[24] F. Martins and A. Ravara. Controling migration in lsdpi. Preprint, Section of Computer Science, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2002. In preparation.

[25] L. Monteiro. Transition systems with spatial structures: A coalgebraic framework. Manuscript, 2002.

[26] R. Raggi and E. Tuosto. *HD-Reducer (Online version)*. Dipartimento di Informatica, Universita' di Pisa, http://jordie.di.unipi.it:8080/mihda, 2002.

[27] A. Ravara, P. Resende, and V. Vasconcelos. An algebra of behavioural types. Preprint, Section of Computer Science, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2002. Submitted for publication.

[28] D. Sangiorgi. Types, or: Where's the difference between CCS and π? In *Proc. CONCUR '02*, volume 2421 of *LNCS*. Springer Verlag, 2002. accompanying paper for an invited talk.

[29] D. Teller, P. Zimmer, and D. Hirschkoff. Using Ambients to Control Resources. In *Proceedings of the 13th Int. Conf. in Concurrency Theory (CONCUR'02)*, volume 2421 of *LNCS*, pages 288–303. Springer Verlag, 2002.

[30] A. Vallecillo, V. T. Vasconcelos, and A. Ravara. Typing the behavior of objects and components using session types. In A. Brogi and J.-M. Jacquet, editors, *Electronic Notes in Theoretical Computer Science*, volume 68. Elsevier Science Publishers, 2002. presented at FOCLASA'02 - 1st International Workshop on Foundations of Coordination Languages and Software Architectures.

[31] V. Vanackère. *The TRUST protocol analyser.* Lab. Informatique de Marseille, http://www.cmi.univ-mrs.fr/~vvanacke/trust.html, 2002.

[32] V. Vanackère. The TRUST protocol analyser, automatic and efficient verification of cryptographic protocols. In *Verification Workshop - Verify02*, 2002.