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

Periodic Progress Report Year 2

Preparation date:	February 11, 2004
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

Contents

PROFUNDIS:
Periodic Progress Report Year 2

February 11, 2004

1 Executive Summary

PROFUNDIS is a FET GC project with the main goal to advance the state of the art of formal modelling and verification techniques to the point where key issues in mobile distributed systems can be treated rigorously and with considerable automatic support. The partners are Uppsala (co-ordinator), Lisbon, INRIA and Pisa. In this Periodic Progress Report we present the developments in Year 2 (2003).

Overall PROFUNDIS has been successful and reached all the major scientific goals. Inevitably there are now some minor discrepancies in comparison to the plan we made two and a half years ago. In some areas we have fewer results than hoped, and in some we have progressed farther than envisaged. We shall continue to work in a few subtasks which have proved more fruitful or necessary than planned. We do not expect any reductions in the goals of the other subtasks.

All devliverables have been produced according to plan. Dissemination activities have been well above plan, with 20 refereed publications and 30 visits outside PROFUNDIS. The PROFINDIS distributed tool architecture is well on its way with a solid web presence.

Manpower spent on the project is exactly according to plan for year 2, and 90% of the plan for the sum of years 1 and 2. The recruitment difficulties in Uppsala have been solved and that site is now up to speed, but the difficulties in Lisbon remain. The many visits mean that travel cost has exceeded expectation.

As the reviewers suggested one uear ago, we have spent effort on case studies and have started collaborations with two companies for this purpose. We have also strengthened ties between the different Work Packages through concrete collaborations.

Project management has been without friction of any kind.

Other related documents are the Self Assessment, where we compare our achievements against the goals in the Self Evaluation Plan, and the Summary of Dissemination Activities.

2 Work progress overview

We here elaborate on the objectives of year 2, on the progress made and on how it compares to plan. We report on activities in man months per Work Package. We give a brief update of the state of the art in our field and how this affects PROFUNDIS, and pay special attention to how we have reacted to the reviewers' comments. We end with the modifications to plan for the remaining year. Te obligatory deliverable summary tables and project achievements fiche are contained in appendices.

2.1 Specific objectives for year 2

The specific objectives for year 2 can be broken down onto the three scientific Work Packages as follows.

2.1.1 WP1

The overall goal of this Work Package is to develop a comprehensive automata-like model that supports effective techniques to specify and verify properties of network applications. For year 2 the specific objective for Task 1.1 was the definition of an extended version of History Dependent (HD) automata for handling names and substitutions in their full generality, while for Task 1.2 we intended to develop proof techniques (typically of security protocols) based on symbolic execution. Task 1.3. was concerned with extending the existing tools to handle the enriched versions of HD-automata.

2.1.2 WP2

The objectives of WP2 for the second year were expressiveness and decidability results for several logics for mobile processes and semi-structured data. An important goal of PROFUNDIS is the development of an integrated verification framework and associated verification tools for the logics. In this context, refined proposals of a base logic, first prototypes of verification tools, and worked out case studies were also envisaged.

2.1.3 WP3

This Work Package deals with formal type systems for our calculi and logics. The work in year 2 was planned to consist in publishing the results from year 1, in developing the type systems introduced during year 1 further (making them more powerful, adapting them to more advanced constructs), and in starting the study of issues related to the applicability of type systems (eg through case studies).

2.2 Overview of progress

We here first briefly say what concrete scientific progress has been made and what results have been achieved, and then summarize the deliverables.

2.2.1 WP1

The structure of HD-automata and the state-space minimization algorithm have been formally specified using a polymorphic λ-calculus with dependent types. This specification closely corresponds to the ML implementation of the Mihda toolkit. It has been shown that the different categorical formulation of HD-automata, namely the category of named sets and named functions, the category of permutation algebras and certain categories of presheaves, are essentially equivalent. Finally, the HD-automata approach has been extended to Fusion Calculus, and the bialgebra approach to Fusion Calculus with explicit fusions. Fusion Calculus has also been also mapped to logic programming clauses. A new calculus with two binders, called DFusion, which is an extension of both open π-calculus and Fusion Calculus, has been defined.

Symbolic verification techniques for security protocols have been further developed. The symbolic technique of *history-dependent scheduling* has been formally defined and implemented in the TRUST verifier. A "low level" protocol description language has been introduced, together with a notion of symbolic execution. A verification methodology based on the notion of symbolic state-space exploration has been developed and implemented in the verification environment called ASPASYA.

The development of PROFUNDIS WEB has progressed and several toolkits have been made available on the the PROFUNDIS WEB service directory. Some of the services available on the PWeb have been exploited in the verification of properties of mobile systems.

Additional results have been obtained for relevant verification models: a translation of the spi calculus into a basic dialect of π has been defined and implemented which is sound with respect to may-testing; automatic techniques for reachability analysis of infinite-state systems have been studied; the verification problem for a substantial fragment of the ntcc calculus with infinite processes and the negation-free fragment of LTL have been shown to be decidable (joint work with WP2); and several CCS variants differing for infinite behavior and for name scoping have been compared.

2.2.2 WP2

Expressiveness results for a spatial logic for systems specified in the synchronous Pi-calculus with recursion were studied. It was shown that model-checking in this logic is decidable for a useful class of processes. Expressiveness and minimality results have also been obtained for spatial logics. Minimality has been addressed for the static Ambient Logic with operator of name revelation and fresh name quantification. It was proved that the spatial adjunct operator can be eliminated without losing expressive power.

Tree automata were applied to obtain several complexity results related to XML schema, in a tree logic that is a form of spatial logic. This approach was also applied to derive the decidability of a fragment of ambient logic that corresponds to a kind of regular expression language for semistructured data.

A prototype version of a tool for model-checking distributed systems modelled in the pi-calculus against a version of a spatial logic was implemented, and some case studies have been tested and implemented using this tool. A sound and complete sequent calculus-based proof system for a core spatial logic was developed, and the corresponding decision procedure for validity of formulas has led to a prototype implementation. Some case studies of concurrent systems related to global computing were developed.

2.2.3 WP3

We have been working on the type systems introduced in year 1, generalising and further enhancing these. New static methods have also been proposed, notably: for program transformation in presence of stack inspection; for static control of migrating processes; for specifying the state transitions of a protocol (session types). We have also worked on the applicability of type systems; we have specified and formally proved a method to guarantee noninterference in a proof assistant; we have designed type systems for rich programming languages such as Klaim and the Java Virtual Machine. Finally, we have worked on the integration of type systems to the verification tools developed in Work Package 1.

2.2.4 Summary of Deliverables

According to plan we have produced three deliverables, one for each Work Package described above, in addition to two managerial deliverables containing our self assessment and summary of dissemination activities. A table with deliverable summaries is contained in Appendix A.

2.3 Comparison to plan

Work Package 1 has basically progressed as planned in the TA and SEP. The main difference concerns the semantical understanding of models for spatial logics in terms of HD-automata with operations. These models are not fully developed, even if this year two notes have been produced on a closely related subject and a collaboration between Lisbon and Pisa has started. Also the study of logic programming in this context (relevant for the theme of automata with substitutions) was limited to the case of *synchronized* logic programming, which is the natural counterpart of process calculi.

Work Package 2 has basically progressed according to what was planned. The main difference is that some work on high-level extensions to the base logic was expected at this point, but experience has shown that the subject was better dealt with in connection with the ongoing work on case studies.

Work Package 3 is also on the whole according to plan. Some subtasks that were planned to be addressed in year 2 have not led to results yet: this is the case for *'space in types'* (Task 3.2) and *'type inference algorithms'* (Task 3.3). This is compensated by an active research effort on other subjects.

We comment on two directions for which work has not been as fruitful as expected. The study of advanced programming constructs (Task 3.3) has been developed, but the postdoc that had been hired to work on this subject quit after a year, which resulted in an effort smaller than expected on this subject. The PhD student who has been hired in year 2 to work on using types to establish liveness properties such as termination of mobile processes (Task 3.2) has been facing some difficulties. While we were hoping to improve on last year results (that is, to be able to prove termination for a much larger class of processes), we have not really succeeded in that: we have only some – rather incremental — new results. As a consequence, we have started examining other techniques for proving termination. Some promising initial results have been obtained; a paper is in preparation.

2.4 Activities per Work Package

We here give the tables indicating the effort spent in man months on the different Work Packages.

2.4.1 Project total

TOTAL	Year 2 Planned		Year 2 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	35	24	37	24	47	30	51	30
FFCT	45	33	28	16	90	66	50	23
INRIA	23	23	26	26	46	46	44	44
PISA	35	18	47	33	65	30	77	51
Total	138	98	138	99	248	172	222	148

The total effort for year 2 is precisely according to the revised plan. The difficulties in recruiting at FFCT are continuing but have been compensated by a higher activity at Pisa. The cumulative effort of the two first years is 90% of the plan (86% of paid effort). All sites but FFCT have overcome their initial problems.

2.4.2 WP1

WP1	Year 2 Planned		Year 2 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	21	16	30	22	31	22	42	28
FFCT	14	11	3	0	28	22	6	0
INRIA	6	6	6	6	12	12	10	10
PISA	23	12	32	24	41	19	50	37
Total	64	45	71	52	112	75	108	75

The work in Uppsala was delayed in the first year but has recovered in the second year. In Lisbon, the difficulty in recruiting personnel has continued in the second year, so no paid man-months are listed. Instead in Pisa, following the trend of the first year, the paid activity is significantly larger than planned, but still within an acceptable cost.

For the last year of the project, no significant changes are expected to the manmonths planned in the TA.

2.4.3 WP2

WP2	Year 2 Planned		Year 2 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	6	4	2	2	6	4	2	2
FFCT	24	18	22	16	48	36	34	19
INRIA	6	6	6	6	12	12	11	11
PISA	5	3	5	3	10	5	10	5
Total	41	31	35	27	76	57	57	37

The total effort in persons-months in the second year was a little less than expected, but with no significant consequences to the planned work. For the last year of the project no significant changes are expected to the persons-months planned in the TA.

2.4.4 WP3

WP3	Year 2 Planned		Year 2 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	6	4	3	0	6	4	3	0
FFCT	6	4	2	0	12	8	8	4
INRIA	10	10	13	13	20	20	21	21
PISA	6	3	9	6	12	6	15	9
Total	28	21	27	19	50	38	47	34

Figures are globally as expected, less work as expected in Uppsala and Lisbon being compensated by additional effort at Pisa and INRIA.

2.4.5 WP4: Management

WP4	Year 2 Planned		Year 2 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	2	0	2	0	4	0	4	0
FFCT	1	0	1	0	2	0	2	0
INRIA	1	1	1	1	2	2	2	2
PISA	1	0	1	0	2	0	2	0
Total	5	1	5	1	10	2	10	2

Activities are according to plan.

2.5 State of the art update

The work of Murdoch (Jamie) Gabbay is worth mentioning. After his 2001 PhD thesis on inductive definitions with α-equivalence at Cambridge UK supervised by Andrew Pitts, he has developed versions of Fraenkel-Mostowski set theory suitable for mobile calculi (e.g. π-calculus). Several references can be found on his web site, but no comprehensive paper is available to our knowledge. Relations of Gabbay's work with HD-automata are not fully understood, but a possible advantage could be avoiding a fixed ordering of names, probably at the expense of a more complex theory.

Quite relevant to the foundations of HD-automata is the recent work of Marino Miculan and Ivan Scagnetto on typed higher-order abstract syntax for named systems. An active collaboration with the first author has been started, and has already given rather valuable results [10]. A possible outcome of a full understanding of the connection of this work with HD-automata is the development of a logic framework for proving complex properties of mobile systems. However we see this activity as out of scope for PROFUNDIS.

A very interesting development is the *Highwire* programming language within the *BigTop* initiative led by Greg Meredith at Microsoft. If successful, the influence of this activity on Microsoft policy for web service programming could be decisive. Connections with PROFUNDIS activities could concern both verification (a front-end of Highwire with HD-automata is quite feasible) and language design (DFusion concepts could find interesting applications here).

In the theme of specification logics for mobility, the work of the Klaim group lead by Rocco de Nicola on modal logics for mobile agents seems related, at least in intent, with some of the work being developed in PROFUNDIS; however, intersections with the work developed in PROFUNDIS, which is based on spatial logics, are not likely to occur. Some results about expressiveness of logics related to the ones studied in PROFUNDIS have been obtained. Concerning the validity problem for spatial logics with the revelation operator (a logical operator that talks about restricted channels in processes), Ghelli and Conforti have shown its undecidability. This result is related to work performed in PROFUNDIS by Lozes on (non-constructive) elimination of adjunct operators for the spatial logics in the sense that it complements it. These developments have contributed to better delineate the scope of model-checking for spatial logics for concurrent systems being pursued in PROFUNDIS.

Research in the field of type systems has been active during year 2003, and a substantial part of it has been carried out within the Global Computing initiative. Due to our connections with other projects, we are in close contact with the researchers who are active in the area. Recent evolutions have gone essentially as expected, and developments in 2003 should not affect our goals as expressed in the Technical Annex of the original proposal.

2.6 Reviewer comments

In their report on the first year of PROFUNDIS the reviewers recommended us to identify convincing case studies and to strengthen the interactions across Work Package boundaries.

2.6.1 Case studies

We have conducted new case studies for the HAL Model Checker reported in [11].

The PROFUNDIS group in Pisa has established a collaboration with an industrial partner – Telecom Italia Lab (TILAB) – within the context of a national research project (*Architetture Software ad Alta Qualità di Servizio per Global Computing su Cooperative Wide Area Networks*). Together with the TILAB group, we have exploited some of the toolkits of the PWeb to verify security properties of the PARLAY-X infrastructure. This analysis has lead to the discovery of a security flaw inside the specification of the PARLAY-X authentication facilities. The collaboration between PROFUNDIS and TILAB will address several issues of a case study on *Network Intelligence* in the field of telecommunications. We are involved in the analysis of the security issues and the handling of *Service Level Agreement* (SLA). We expect to report on the results of this activity in the continuation of PROFUNDIS next year.

A case study on the verification of correctness properties of a peer-to-peer algorithm (the Arrow Distributed Directory Protocol of Demmer and Herlihy) was developed, using spatial logic and proof-theoretic techniques ([44]).

2.6.2 Interaction across Work Packages

A collaboration has started to work on the addition of types (WP3) to the verification environment (WP1) to reduce the growth of state spaces during cerification, leading to improved efficiency in some cases. This work is in progress, and should lead to an extension of (some of) the tools in year 3, as well as to published material. In relation with this interaction, preliminary investigations have been made regarding connections between types and operational/algebraic techniques, which could result in enrichments of existing verification algorithms. Work in this area is at a too early stage to be reported here.

A collaboration on the definition of types (WP3) for spatial properties (WP2) has started. For the moment there has been no results. We plan to work on this during year 3, having now a better understanding of spatial logics and of possibile static analyses that can be made using them. It should be pointed out that exchanges and interactions among the researchers involved in WP2 and WP3 are fairly strong (PhD student jointly supervised between the Inria and Lisbon sites, mutual visits, etc.).

The semantical understanding of models for spatial logics (WP2) in terms of HD-automata with operations (WP1) has not been fully developed, and a collaboration on this research topic has started. Moreover, a dialect of the μ-calculus (WP2) directly defined on HD automata (WP1)has been recently defined by the PROFUNDIS group in Pisa. Results about this activity should be ready in a few months. A long stay of a PhD student from Lisbon in Pisa is expected to occur soon, with the intention of strengthening the collaboration between WP1 and WP2 on model-checking spatial logics. Another collaboration is that the verification problem was shown to be decidable for a substantial fragment of the ntcc calculus, allowing infinite-state processes, and the negation-free fragment of LTL. A collaboration between WP1 and WP2 on the expressiveness of models and LTL logics for name passing calculi has started. This is work in progress and should lead to some tool prototype (model checker) and published papers in the third year of the project.

2.7 Planned work

The PROFUNDIS consortium is planning to ask for a four month extension of the project. This will allow participants to disseminate the results of the project at the planned EU-FET event that will be held at ETAPS 2005. The project budget (hiring of people, travel) will be modified accordingly.

In other respects the work will continue as originally planned in the TA. We comment here mainly on the few cases where we have adjusted our plans.

2.7.1 WP1

The general goal of developing the theory of HD-automata and of modeling in terms of HD-automata the basic phenomena related to the handling of names in process calculi and other formalisms has progressed rather well. However there are good reasons for not considering this task completed within the second year - as planned - but to extend it until the end of the project. The reasons for extending the task are of two kinds: some issues which were considered in the technical annex have not been fully addressed yet, and some new issues have naturally arisen from the ongoing work which are worth pursuing. About the first kind, the semantical understanding of models for spatial logics in terms of HD-automata with operations is not fully developed, even if this year two notes have been produced on a closely related subject and a collaboration between Lisbon and Pisa has started. Also the study of logic programming in this context (relevant for the theme of automata with substitutions) was limited to the case of *synchronized* logic programming, which is the natural counterpart of process calculi. About the second kind of reasons, we think that the work on comparisons of HD-automata with existing domain theory is worth continuing. Also we think that the expressiveness analysis about the need of two name binders which has led to the definition of DFusion should be brought in the context of HD-automata and bialgebras. The extension of Task 1.1 will not cause reductions of the efforts in other tasks.

Therefore we plan to extend Task 1.1 until the end of the project. The research should include models for spatial logics, automata with substitutions, comparisons of HD-automata with existing domain theory and bialgebraic models for distinctions (open π-calculus and DFusion). The remaining tasks of WP1 should progress as planned in the TA.

2.7.2 WP2

In WP2 we plan to develop the verification framework and integrate it with the verification environment of the project, continue the work on the case studies and investigate extensions to the logic, as described in the Technical Annex and Self Evaluation Plan.

2.7.3 WP3

In WP3, work on Tasks 3.1 and 3.2, that was planned to stop at the end of year 2, turned out to be quite fruitful and should proceed in year 3. This shall not prevent us from reaching the objectives in the two other Tasks during year 3.

The publication effort should follow the lines announced in the TA, as has been the case until now (exceeding expectations in some cases). In particular, we plan to have at least three papers from Work Package 3 accepted for publication in good journals by the end of year 3.

We also plan to strengthen the work on applicability of the type systems we have developed, by giving more weight to the corresponding Tasks in the TA (3.3 and 3.4). The subtasks *'space in types'* and *'type inference algorithms'*, that have not been adressed as expected in year 2, will be studied in year 3.

2.8 Assessment of results and achievements

The obligatory "Project Achievement Fiche" is contianed in Appendix B to this PPR. A related document is our Self Assessment (Deliverable 16). A brief summary is that the project as expected is rich in technical innovation, with considerble impact on the scientific community in terms of publications, visits, and PhD students engaged, but still weak in the technology implementation aspect (though contact with companies are starting to form).

3 Project management and coordination

Project management and coordination has been conducted without any friction.

The yearly PROFUNDIS workshop was held in connection with the first year review meeting in Rovereto 2003, and included strong participation from all sites. This meeting was also instrumental in strengthening contacts with other relevant GC projects.

There have been no conflicts within the consortium and several new concrete collaborations started as reported in section 2.6.2.

There have been nine visits between partners in order to work together on techincal problems as further detailed in Deliverable 12 (Summary of dissemination activities).

There have been no contractual issues.

4 Cost breakdown

See enclosed sheet.

5 Information dissemination and exploitation of results

The obligatory report here on information dissemination and exploitition of results seems excessive since we have an entire deliverable (Deliverable 12) summarising information dissemination, and as per plan nothing has happened on exploitation. We mention here only that information dissemination has been extremely high:

20	articles in reviewed journals or conferences
5	invited articles
24	other articles (many currently being refereed)
6	websites
30	trips by project members to give talks about the project
12	PhD students hired with thesis projects related to PROFUNDIS

The details of these can be found in Deliverable 12. In all we regard this as a satisfying output.

Appendix A: Deliverable Summaries

DELIVERABLES TABLE

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

Del no	Title	Type	Class	Due	Issued
2	Automata with substitutions...	R/S	Pub	Month 24	Feb. 2004
5	Verification framework...	R/S	Pub	Month 24	Feb. 2004
8	Integration and algorithms	R	Pub	Month 24	Feb. 2004
12	Summary of dissemination year 2	R	Pub	Month 24	Feb. 2004
16	Self-assessment year 2	R	Pub	Month 24	Feb. 2004

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	2
Due date:	Project month 24
Delivery date:	February 11, 2004

Short Description: Automata, Domains and Coalgebras for name passing calculi. Automata models and calculi with explicit fusions. Finite state verification techniques for mobility. Symbolic verification techniques for security protocols. Prototype tool development, Web services, directory services and case studies.

Partners owning:	Pisa
Partners contributed:	FFCT, INRIA, Pisa, UU
Made available to:	

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	5
Due date:	Project month 24
Delivery date:	February 11, 2004

Short Description: Expressiveness results for various spatial logics and the pi-calculus. Decidability of model checking. Minimality in a version of static Ambient logic. Prototype tool development and case studies.

Partners owning:	FFCT
Partners contributed:	FFCT, INRIA
Made available to:	

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	8
Due date:	Project month 24
Delivery date:	February 11, 2004

Short Description: Static methods for program transformation in presence of stack inspection; for static control of migrating processes; for specifying the state transitions of a protocol (session types); a generalized and integrated type system for resource bounds; formalization in a proof assistant of a method to guarantee noninterference; type systems for Klaim and for a large fragment of the Java Virtual Machine. Integration of type systems to the verification tools developed in Work Package 1.

Partners owning:	INRIA
Partners contributed:	FFCT, INRIA, Pisa, UU
Made available to:	

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	12
Due date:	Project month 24
Delivery date:	February 11, 2004

Short Description: Summary of Dissemination of the project year 2

Partners owning:	UU
Partners contributed:	FFCT, INRIA, Pisa, UU
Made available to:	

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	16
Due date:	Project month 24
Delivery date:	February 11, 2004

Short Description: Self-assessment of the project year 2

Partners owning:	UU
Partners contributed:	FFCT, INRIA, Pisa, UU
Made available to:	

Appendix B: Project Achievements fiche

1. Scientific and technological achievements of the project (and why are they so ?)

Question 1.1. Which is the 'Breakthrough' or 'real' innovation achieved in the considered period

The structure of HD-automata and the minimization algorithm have been formally specified using a polymorphic λ-calculus with dependent types.
The category of named sets and named functions, the category of permutation algebras and certain categories of presheaves have been shown essentially equivalent.
The HD-automata approach has been extended to Parrow and Victor's Fusion Calculus, and the bialgebra approach to Fusion Calculus with explicit fusions. Fusion Calculus has also been mapped to logic programming clauses.
A new calculus with two binders, called DFusion, which is an extension of both open π-calculus and Fusion Calculus, has been defined.
The symbolic technique of *history-dependent scheduling* has been implemented in the TRUST verifier.
A "low level" protocol description language has been introduced, together with a notion of symbolic execution.
A verification methodology based on the notion of symbolic state-space exploration has been developed and implemented in the verification environment called ASPASYA.
The PROFUNDIS WEB has been designed and several toolkits have been made available on the web. Some services have been described which can be exploited in the verification of mobile systems.
Static methods based on graphs for program transformation in presence of stack inspection have been developed.
The type systems for resource bounds have been generalized.
A theorem prover formalisation of a soundness proof for a type system for noninterference has been finished
Type systems for the Klaim language and for a large fragment of the Java Virtual Machine have been defined.
Minimality results for the static Ambient Logic with operators of name revelation and fresh name quantification havwe been established, showing that the adjunct operators do not increase the expressive power of the logic.
Expressiveness and minimality results for spatial logics for concurrency have been obtained. In particular, it has been established that these spatial logics can express potentiality of interaction, as in the Hennessy-Milner logics.
A spatial logic for the pi-calculus with recursion and behavioral modalities has been defined, and its expressiveness studied.
Model-checking for a pi-calculus spatial logic has been studied, relying on permutation based techniques. A tool for model-checking distributed systems against a spatial logic has been implemented building on these techniques, to be made available on the web.
Complexity results related to XML schema using tree automata, in a tree logic that can be seen as a form of spatial logic, have been obtained.
Decidability results for the quantifier-free, static fragment of ambient logic, with composition adjunct and iteration, have been obtained.
The verification problem for a substantial fragment of the ntcc calculus, with infinite processes, and the negation-free fragment of LTL was shown to be decidable.

2. Impact on Science and Technology: Scientific Publications in scientific magazines

Question 2.1. Scientific or technical publications on reviewed journals and conferences

20	See appendix C

Question 2.2. Scientific or technical publications on non-reviewed journals and conferences

24	See Appendix C

Question 2.3. Invited papers published in scientific or technical journal or conference.

5	See Appendix C

3. Impact on Innovation and Micro-economy

A - Patents

Question 3.1. Patents filed and pending

0	

Question 3.2. Patents awarded

0	

Question 3.3. Patents sold

0	

B - Start-ups

Question 3.4. Creation of start-up

0	

Question 3.5. Creation of new department of research (ie: organisational change)

0	

C - Technology transfer of project's results

Question 3.6. Collaboration/ partnership with a company

2	Partner Pisa has established a collaboration with Telecom Italia Lab (TILAB). We have exploited some of the toolkits of the PWeb to verify security properties of the PARLAY-X infrastructure. Uppsala has established a research collaboration with IBM Research, TJ Watson Lab, on expressiveness in mobile calculi.

4. Other effects

A - Participation to Conferences/Symposium/Workshops or other dissemination events

Question 4.1. Active participation to Conferences in EU Member states, Candidate countries / NAS. (specify if one partner or "collaborative" between partners)

6	Andrea Corradini, Marina Lenisa and Ugo Montanari, Eds., Special issue dedicated to Coalgebraic Methods in Computer Science, 2001, MSCS, Vol.13, 2, April 2003. Fabio Gadducci, Ugo Montanari, Eds., Proc. of The Fourth International Workshop on Rewriting logic and Its Applications (WRLA2002), ENTCS, to appear. R. Amadio (INRIA site) was program chair of the conference CONCUR'03, held in September 2003 in Marseille, of which S. Dal Zilio was workshop chair. R. Amadio, C. Meyssonnier, S. Dal Zilio, D. Hirschkoff, E. Lozes, D. Teller (INRIA site) were involved in the french initiative AS CNRS *"Méthodes formelles pour la mobilité"* (R. Amadio was head of this project). Two meetings were organised in march (Lyon) and september 2003 (Marseille). This project was concerned with issues related to PROFUNDIS Work Packages 2 and 3. J. Parrow was programme chair for ICALP track B, Eindhoven July 2003

Question 4.2. Active participation to Conferences outside the above countries (specify if one partner or "collaborative" between partners)

1	F. Valencia (Uppsala) was workshop chair and organizer of COLOPS (Constraint and Logic Programming in Security), a satellite event of ICLP'03, Mumbai, India, and B. Victor (Uppsala) was member of the programme committee of the same workshop.

B - Training effect

Question 4.3. Number of PhD students hired for project's completion

12	In all areas of the project.

C - Public Visibility

Question 4.4. Media appearances and general publications (articles, press releases, etc.)

0	

Question 4.5. Web-pages created or other web-site links related to the project

6	Project home page at
	`http://www.it.uu.se/profundis/`
	PROFUNDIS WEB site at
	`http://jordie.di.unipi.it:8080/pweb`
	TRUST tool at
	`http://www.cmi.univ-mrs.fr/~vvanacke/trust.html`
	The web page of HAL at
	`http://rep1.iei.pi.cnr.it/projects/JACK/hal.html`
	The web page of MWB at
	`http://www.it.uu.se/research/docs/fm/mobility/mwb`
	The web page of the STA tool at
	`http://www.dsi.unifi.it/ boreale/tool.html`

Question 4.6. Video produced or other dissemination material

0	

Question 4.7. Key pictures of results

0	

D - Spill-over effects

Question 4.8. Any spill-over to national programs

YES	Italian Ministry of Research Project *Architetture Software ad Alta Qualità di Servizio per Global Computing su Cooperative Wide Area Networks* The French initiative ACI Nouvelles Interfaces des Mathémathiques Geocal The French initiative AS CNRS *"Méthodes formelles pour la mobilité"*, *"Sécurité informatique"*, ACI Cryptologie VERNAM, ACI Cryptologie AZURCRYPT, ACI Sécurité informatique CRISS (head), and ACI Securité informatique Rossignol. The portuguese project MIMO, financed by Fundação para a Ciência e a Tecnologia. The Swedish projects *Semantics of Programming Languages* and *Analysis of security properties* funded by the Swedish Research Council. The Portuguese project POLY, funded by the Fundao para a Cincia e Tecnologia.

Question 4.9. Any spill-over to another part of EU IST Programme

YES	FET-GC

Question 4.10. Are other team(s) involved in the same type of research as the one in your project?

YES	Several of the other projects involved in FET-GC University of Stony Brook, NY University of Dortmund, Germany Microsoft Research (UK) The Big Top Initiative, Microsoft (USA)

Appendix C: Publications and reports

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 hyper-edge 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.