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

Periodic Progress Report Year 3

Preparation date:	March 15, 2005
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 3

March 15, 2005

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 3 (2004).

Overall PROFUNDIS has been successful and reached all the major scientific goals. Inevitably there are small discrepancies in comparison to the plan we made three and a half years ago. In some areas we have fewer results than hoped, and in some we have progressed farther than envisaged.

All scientific deliverables have been produced according to plan. Dissemination activities have been well above plan, with 37 refereed publications and 28 visits outside PROFUNDIS. The PROFUNDIS distributed tool architecture is well on its way with a solid web presence. Application oriented case studies are emerging.

Manpower spent on the project during year three is exactly according to plan. Because of recruitment difficulties in the first years, particularly in Lisbon, the cumulative effort of the whole project is only 93% of plan. Total costs for the period is 81% of plan (the manpower to a large extent derives from people not directly funded by this contract) and the cumulative cost is 85% of plan. PROFUNDIS has been granted a four month extension and will terminate 30 April 2005; this will allow us to catch up.

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 3, 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. We end with the modifications to plan for the remaining months. The obligatory deliverable summary tables are contained in appendices.

2.1 Specific objectives for year 3

The specific objectives for year 3 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. The activities on Task 1.1. (Automata with operations and substitutions) were expected to be completed by the end of the second year. However, we modified our initial plans and we continued them also in the third year. Hence, for year 3 the specific objective for Task 1.1 include automata with substitutions, higher order abstract syntax and functorial semantics, and (bialgebraic and functorial) models for distinctions (open π-calculus, fusion) and models for spatial logics. For Task 1.2 we continued the development of proof techniques (typically of security protocols) based on symbolic execution. Task 1.3. was concerned with extending the Profundis toolkit infrastructure (the PWeb). Moreover, to assess our verification infrastructure we focused on some case studies.

2.1.2 WP2

The goal of this work package is to develop a logical framework to support the specification and verification of spatial and behavioural properties of mobile concurrent systems and to develop verification tools for the logical framework. The specific objectives for the third year were a final prototype of the proof tool and a collection of case studies. These objectives have been extended to allow for further refinements of the logics, their expressiveness properties and applications.

2.1.3 WP3

This Work Package deals with formal type systems for our calculi and logics. The work in year 3 was planned to consist in publishing the results from year 2 and, above all, studying issues related to the applicability of type systems, through the analysis of advanced programming constructs, implementations, and 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

Task 1.1: Automata with Operations and Substitutions

Automata with substitutions and Bialgebraic models The formulation of HD-automata as the basic model for name passing process calculi has been further developed. We developed a general framework to describe the symbolic semantics of nominal calculi, where inputs are represented as variables which are instantiated only when needed as it happens in logic programming. We introduce a general approach to lift calculi with structural axioms to bialgebras. In order for the lifting to hold, two conditions are required: the transition rules of the calculus are in tyft format and the axioms bisimulate with respect to the lts. We also provided a compositional coalgebraic semantics of the Fusion calculus.

Functorial Semantics for Nominal Calculi We have here two lines of research, both aiming at the development of abstract models for nominal calculi. The first line of research developed at Uppsala concerns the development of functorial models for names. A key result shows that open bisimulation requires us to move from the usual semantic domain of presheaves over subcategories of Set to presheaves over subcategories of Rel. The second line of research developed in Pisa aims at providing a general framework to relate the different abstract models of nominal calculi. The relationships among these models have been studied and the proposed framework allows one to transfer techniques and constructions from one model to the other.

Fusion and Binding We introduced the U-Calculus, a process calculus with no I/O polarities and a unique form of binding. The U-Calculus, is proven to be more expressive than pi-calculus and Fusion calculus separately.

Models for Spatial Logics Lisbon and Pisa have developed an alternative notion of model of spatial logics which has been proved to coincide with the standard one. Furthermore, logical equivalence is characterized in terms of the bisimilarity of SCCS.

Other Extensions We developed a complete axiomatization for a process calculus which combines both nondeterministic and probabilistic behavior. We also analyzed the computational limits of open constraint satisfaction problems and the relationships with automata over infinite-sequences.

Task 1.2: Proof Techniques

Symbolic Verification Techniques for Security Protocols We have here three lines of research, all aiming at the development of models and reasoning techniques for the analysis of security protocols. The first line, developed at INRIA, concerns the TRUST cryptographic protocol verifier. The second line of work, developed at Pisa, has been concerned with the development of a general framework for the analysis of security protocols based on the notion of *frame*, essentially a rewrite system plus a set of distinguished terms called *messages*. The third line, also developed at Pisa has addressed the development of a verification methodology for security protocols where coordination techniques are exploited to guide the checking of the security properties reducing the dimension of the state space.

Task 1.3: Prototype and Case Studies

The Profundis WEB The distinguished and innovative feature of the Profundis Verification environment, called *Profundis WEB*, or *PWeb*, is the idea of viewing the environment as a distributed infrastructure exploited as a *service distributor*. In the third year of the project Uppsala has enriched the XML facilities of the PWEB. In particular, some data-to-XML parser and an XML-to-data converter allows us integrate within the PWeb different calculi in a clear and economic fashion.

Verification Toolkits PWeb verification toolkits have been extended and reengineered to accommodate new facilities, suggested by the theoretical investigations. The MIHDA front-end has been extended to take advantage of type information. Moreover, the spatial model checker developed in Lisbon has been integrated inside the PWeb. By taking advantage of the availability of the new XML schemata, the spi2pi translator developed in Uppsala has been added as a new service of the PWeb in an economic fashion.

Case Studies We have two main contribution in the third year. The first contribution reported on our experience in exploiting the facilities of the PWeb infrastructure in the verification of properties of distributed systems specified in some dialect of the π-calculus. In particular, the verification of the KSL protocol will allow us to demonstrate how service coordination supports and facilitates modular verification techniques. The second contribution creates a generic library for a variety of process calculi in the automatic theorem prover Isabelle.

2.2.2 WP2

Task 2.1: Logics for systems with spatial and temporal structure We extended our investigation on decision procedures for model checking pi-calculus processes against spatial logic properties. In particular, extensions to

the mechanisms for coping with recursive properties (both inductive and co-inductive) were devised and implemented. Another line of research, which will be pursued before the end of the project, is the proposal of decidable spatial type systems inspired by spatial logics.

A CCS-like calculus has been defined for which the observations have been enriched with spatial observations, giving rise to models of spatial logic.

A simple spatial logic that supports specification of quality of service (QoS) properties of applications has been introduced. The evaluation of a formula in the spatial logic is a value of a suitable algebraic structure, a c-semiring, representing the QoS level of the formula and not just a boolean value expressing whether or not the formula holds. Applications of this spatial logic with quantitative information to web services and wireless systems have been considered.

Task 2.2: Expressiveness We addressed the difficult problem of decidability of validity in dynamic spatial logics. The striking conclusion of this research is that the validity problem for the simplest dynamic spatial logics is undecidable, which entails the undecidability of model-checking of spatial logics with contextual operators (composition adjunct). This research contributed to raise the question of finding expressive and tractable forms of contextual reasoning inspired by the composition adjunct, extending those already provided by the decidable behavioral-spatial logics also investigated in the project.

The comparison between the spatial logics for concurrency and more standard logics has led to the definition of a spatial logic for the π-calculus that is *extensional*, in the sense that the induced logical equivalence coincides with behavioural equivalence on processes. This result shows which subset of spatial logics shares the same separative power as the Hennessy-Milner logic.

Separation logic and a classical fragment of it have been compared and shown to be equally expressive.

A framework for specifying constraint problems with an open number of variables was proposed and the decidability of the satisfiability for various families of these problems has been studied.

Task 2.3: Tools and case studies Version 1.0 of the Spatial Logic Model Checker (SLMC) was implemented and made available to the community through the web, together with illustrating examples. We also reported on an example of verification of correctness of a distributed protocol using spatial logics with a proof-theoretic approach.

2.2.3 WP3

We have made further steps on the integration of types with algebraic and logical techniques for reasoning on the behaviour of processes. Specifically, we have used a combination of types with techniques from term rewriting to guarantee properties of termination (i.e., absence of divergence), and we have enhanced the techniques for axiomatising finite-state processes by taking into account some type information.

Most of the work however has gone into applying types studied in previous year to advanced programming construct. On this topic we have had four strands of work. One such strand has focused on information flow type systems that enforce non-interference. Here we have designed such type systems for realistic assembly languages (JVM-like), and we have introduced compilers from high-level programming languages to our low-level languages and showed that the compilers preserve information flow types. We have also studied logical formulations of non-interference, which allow a more precise analysis of programs than that allowed by type systems, and amenable to interactive or automated verification techniques.

The second strand of work has focused on session types. A session type, associated with a communication channel, can specify the state transitions of a protocol and also the data types of messages associated with transitions; thus typechecking can verify both correctness of individual messages and correctness of sequences of transitions. We have designed type systems of this kind for a multi-threaded functional language with side-effecting input/output operations. And we have showed how session types allow not only high level specifications of complex interactions, but also the definition of powerful interoperability tests at the protocol level, namely compatibility and substitutability of components.

The third strand of work has focused on type system for resource bounds. Following the typed assembly language (TAL) approach, we have developed a type-based analysis for statically ensuring bounds on the resources needed for the execution of systems of concurrent, interactive threads. Also, we have investigated the robustness of techniques developed in previous years, by using them to control resources such as memory or disk usage, using the pi-calculus as underlying formalism.

The fourth strand of work, that initiated last year, has used static techniques based on control flow analysis, initially inspired by type system works, in the context of access control policies based on stack inspection and dynamic security policies. Here we have proposed a new static analysis that allows for various security aware program optimizations and that is parametric with respect to the security policy in force. We have also proposed a new model for access control that allows for policies that have a possibly nested, local scope. On this topic, a case analysis has also been carried out. It is about a specific optimization technique, namely method inlining.

Concerning implementations, the main work has gone into the design of an abstract machine for the execution of Safe Ambients, that improves the machine designed in Year 1. The new machine is made more efficient by adapting some standard algorithms in distributed programming, such as forwarder chains contraction using Tarjan sets.

There has been also efforts in integrations of types into the Profundis tools, and in the design of types that take space into account, but no papers have yet been written.

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. The Technology Implementation Plan will be provided with the obligatory documents at the closing of the project after its four month extension.

2.3 Comparison to plan

2.3.1 WP1

Task 1.1 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, and name substitutions for nominal calculi has progressed rather well. The development of a general framework for handling the symbolic semantics of nominal calculi based on the notion of reactive system with observed borrowed contexts can be considered as an important contribution of this task. Indeed, the generality of the approach gives some hope that interesting abstractions of the Service Oriented Computing paradigm could also be modeled that way. The development of abstract models for nominal calculi based on functorial semantics is another important contribution of this task. The semantical understanding of models for spatial logics as progressed as expected. The work in this activity has also been made in connection with the activities of Workpackage 2. Bialgebraic models of nominal calculi have been extended to deal with name fusions and distinctions.

Task 1.2 The research activity on this task focused on the definition of effective verification techniques for symbolic analysis of security protocols. We can say that the work has progressed as expected and the results are successful. The work in this task has also been made in connection with the tool development activity.

Task 1.3 The development of the Profundis WEB has to be considered successful. Moreover, the theoretical investigations on the symbolic analysis of security protocols have lead to the development of new toolkits and the reengineering of other toolkits with new verification facilities.
Activities on case studies are also going on. The Profundis group in Pisa has established a collaboration with an industrial partner – Telecom Italia Lab (TILAB) . Together with the TILAB group, the Pisa Profundis Group is exploiting some of the toolkits of the PWeb to verify functional and non-functional properties of the PARLAY-X infrastructure. This work has lead to the definition of process calculus to compose overlay network with different Service Level Agreement (SLA) requirements. The results of this activity will be reported in the description of Workpackage 3.

2.3.2 WP2

On the whole Work Package 2 has progressed according to what was planned, with two main deviations. One concerns the work on high-level extensions to the basic spatial logic, which required further foundational work and experience with the case studies, and was given lower priority. The other concerns the prototype of the theorem-proving tool, which as an outcome of theoretical results on expressiveness of the logic was delayed in favour of the development of the Spatial Logic Model Checker.

2.3.3 WP3

Globally, the work in WP 3 has proceeded according to plans. As expected, most of the work has gone into Tasks 3.3 and 3.4, and aimed at understanding the applicability of the type-based, or type-inspired, techniques developed during the project. There has been also some works on the other tasks: part of this in the form of polished/extended versions of shorter/draft papers that appeared in last year's deliverables; other work, in Task 3.2, as the continuation of research efforts that have been active throughout the whole project.

The main discrepancies w.r.t. what was announced in the TA are the following. The effort on the subtask "advanced programming constructs" (Task 3.3) has been bigger than expected. The reason for this is that we have found a number of challenging cases and programming constructs that we thought worth investigating. We have fewer results than expected on the subtasks "Case studies" (Task 3.4), "expressiveness" and "space in types" (Task 3.2), "type inference" (Task 3.3). We did put effort on these topics. We have however encountered unexpected technical difficulties. For instance, on "space in types", Ferrari (Pisa) visited Lisbon, and Hugo Viera (Lisbon) is currently visiting Pisa; both visits have had this topic as their main goal; the progress has however been slow, and the work remains in its early stage. We were planning to carry our main case studies using the Profundis tools, after having enhanced them with type information. Magnus Johansson (UU) has visited Bologna and Pisa, with the objective to work on this topic. Here as well progress has been slow. People in Pisa did some experiments but we have not written any paper on it (basically we have a front-end for MIHDA which exploits a form of type annotation in the generation of the HD automaton). Concerning type inference, some papers considers it but without it as the main objective; we are currently working on problems of type inference for session types.

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 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	35	24	44	21	82	54	95	51
FFCT	45	33	40	28	135	99	90	51
INRIA	23	23	19	19	69	69	63	63
PISA	30	24	30	24	95	54	107	85
Total	133	104	133	92	381	276	355	250

The total effort for year 3 is very close to plan, although personnel actually paid by PROFUNDIS are only on 91% of plan. The cumulative effort of the first three years is 94% of plan (92% paid), reflecting the initial difficulties in recruiting researchers. The planned four month extension will allow us to finally catch up in this respect, especially so for FFCT.

2.4.2 WP1

WP1	Year 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	15	10	32	18	46	32	74	46
FFCT	14	11	4	2	42	33	10	2
INRIA	6	6	3	3	18	18	13	13
PISA	18	15	18	15	59	34	68	52
Total	53	42	57	38	165	117	165	113

With respect to Year 3 efforts, even if some of the partners (FFCT and INRIA) have used less than planned, given the numbers produced by Uppsala, the total effort for WP1 is right as planned.

The activity in Uppsala is significantly larger than planned but the overall effort is acceptable with respect to the planned activities.

2.4.3 WP2

WP2	Year 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	9	7	3	3	15	11	5	5
FFCT	24	18	29	23	72	54	63	42
INRIA	6	6	5	5	18	18	16	16
PISA	5	4	5	4	15	9	15	19
Total	44	35	42	35	120	92	99	82

There is less work than expected in Uppsala due to reordering of priorities. The initial difficulty felt by Lisbon in hiring people was partly compensated in the third year and will be further compensated in the project extension.

2.4.4 WP3

WP3	Year 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	9	7	7	0	15	11	10	0
FFCT	6	4	6	3	18	12	14	7
INRIA	10	10	10	10	30	30	31	31
PISA	6	5	6	5	18	11	21	14
Total	31	26	29	18	81	64	76	52

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

2.4.5 WP4: Management

WP4	Year 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	2	0	2	0	6	0	6	0
FFCT	1	0	1	0	3	0	3	0
INRIA	1	1	1	1	3	3	3	3
PISA	1	0	1	0	3	0	3	0
Total	5	1	5	1	15	3	15	3

Activities are according to plan.

2.5 State of the art update

The syntax-free models of name-passing calculi aim at providing uniform theories that can be used to handle a variety of calculi and semantics regardless of their syntactic details. A well studied approach is based on the so-called permutation model, whose ingredients are a set of names and an action of its group of permutations (renaming substitutions) on an abstract set. In this setting, transition systems for nominal calculi are constructed via suitable functors over the underlying category of names and permutations: the internal theory of names. Quite relevant to the foundations of HD automata are the the work of Gabbay-Pitts, and Cattani-Sewell. The main advantage of History-Dependent automata with respect to similar approaches reside of the fact they that they provide a notion of minimal realization. Minimal automata have a very important practical fall-out for the development of proof-techniques and verification toolkits.

Research in the field of type systems has been active during year 2004, 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 basically as expected, and have not caused major deviations from our original plans.

2.6 Reviewer comments

In their report on the first year of PROFUNDIS the reviewers commented that more case studies and stronger interactions between workpackages were called for. This caused us to revise our actions in this respect and at the end of the second year we had implemented such changes.

In their report on the second year of PROFUNDIS the reviewers had no particular comments or requests for a change of plan. We have continued the case studies and workpackage interactions started in Year 2 (as described in the PPR for year 2).

2.7 Planned work

The final four months of the project will be used to complete the activities as follows.

2.7.1 WP1

We plan to experiment with the facilities of the PWeb service infrastructure by considering illustrative case studies. Moreover, we plan to continue to enrich HD-automata with new features.

2.7.2 WP2

Work on WP2 will proceed on the Spatial Logic Model Checker (SLMC) and case studies, spatial logics with quantitative information and types for spatial properties.

2.7.3 WP3

During 2005 we expect that the main work will be about polishing, sometimes possibly improving, the results produced during this year. At least two journal papers will be prepared; further, a first draft of Deng's PhD thesis (funded by Profundis to work on WP3) will be ready.

A few new results and conference papers might also be produced, especially in the topic of access control policies based on stack inspection. We are also currently working on problems of type inference and type checking for session types.

The work on "space in types" and the work on the integration of types into the Profundis tool will continue. We do not expect to have papers ready by the end of the project. Certainly this work will continue after the project (for instance as part of Magnus Johansson's thesis) and we expect that some results will be obtained by the end of the year.

2.8 Assessment of results and achievements

A related document is our Self Assessment (Deliverable 16). A brief summary is that the project as expected is rich in technical innovation, with considerable 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 second year review meeting in Rovereto 2004, 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.

There have been six further visits between partners in order to work together on technical problems as described in Deliverable 13 (Summary of dissemination activities).

There have been no contractual issues.

4 Cost breakdown

See appendix.

5 Information dissemination and exploitation of results

The obligatory report here on information dissemination and exploitation of results seems excessive since we have an entire deliverable (Deliverable 13) summarising information dissemination, and as per plan nothing has happened on exploitation. We mention here only that information dissemination has been extremely high:

37 articles in reviewed journals or conferences
12 other articles (many currently being refereed)
9 websites
28 trips by project members to give talks about the project

The details of these can be found in Deliverable 13. 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
3	Verification with extended...	R/S	Pub	Month 36	March 2005
6	High level extensions...	R/S	Pub	Month 36	March 2005
9	Advanced programming ...	R	Pub	Month 36	March 2005
13	Summary of dissemination year 3	R	Pub	Month 36	March 2005
14	Technology Implementation Plan	R	Pub	Month 36	Pending
17	Self-assessment year 3	R	Pub	Month 36	March 2005

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	3
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Automata with substitutions, Fusion and Bindings, Models for Open π-calculus and distinctions, Models of Spatial Logics.

Symbolic Verification of Security Protocols.

Verification Services and Case Studies.

Partners owning:	Dipartimento di Informatica Univ. Pisa, Italy
Partners contributed:	Uppsala, FFCT Lisbon, INRIA, Pisa
Made available to:	

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	6
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Short Description: Extension of model checking for coping with recursive properties. Spatial observations. Spatial logic for quality-of-service properties. Applications to web services and wireless systems. Undecidability of dynamic spatial logics and of model checking with contextual operators. Separation logic and a classical fragment. Extensional spatial logics. Implementation of version 1.0 of the Spatial Logic Model Checker (SLMC). Case study.

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

DELIVERABLE SUMMARY SHEET

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

Deliverable Number:	9
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Algebraic techniques for typed processes; combination of types with techniques from term rewriting to ensure properties of termination; information flow type systems that enforce non-interference for realistic assembly languages and preserved through compilation from high level languages; logical formulations of non-interference.
Application to advances programming constructs of types for: specifying the state transitions of a protocol (session types); statically ensuring bounds on the resources needed for the execution of concurrent systems.
Techniques based on control flow analysis for problems of access control policies based on stack inspection.
An abstract machine for the execution of Safe Ambients that improves the efficiency of the machine designed in Year 1.
Some experiments with integration of type systems to the verification tools developed in WP1.

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:	13
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Summary of Dissemination of the project year 3

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:	17
Due date:	Project month 36
Delivery date:	March 15, 2005

Short Description: Self-assessment of the project year 3

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

Appendix : Publications and reports

Reviewed Publications

[1] Roberto M. Amadio and Silvano Dal Zilio. Resource Control for Synchronous Cooperative Threads. In *CONCUR 2004 – 15th International Conference on Concurrency Theory*, volume 3170 of *Lecture Notes in Computer Science*, pages 68–82. Springer-Verlag, August 2004.

[2] Michael Baldamus, Jesper Bengtson, Gianluigi Ferrari, and Roberto Raggi. Web services as a new approach to distributing and coordinating semantics-based verification toolkits. In *Proceedings of the First International Workshop on Web Services and Formal Methods (WSFM 2004)*, volume 105 of *ENTCS*, pages 11–20. Elsevier, February 2004.

[3] Michael Baldamus, Joachim Parrow, and Björn Victor. Spi calculus translated to pi-calculus preserving may-tests. In *Proceedings of LICS'04*, Turku, Finland, July 2004. IEEE, Computer Society Press.

[4] Giacomo Baldi, Andrea Bracciali, Gianluigi Ferrari, and Emilio Tuosto. A Coordination-based Methodology for Security Protocol Verification. In *WISP'04*, volume 121 of *ENCTS*. Elsevier, 2005.

[5] G. Barthe, A. Basu, and T. Rezk. Security types preserving compilation. *Journal of Computer Languages, Systems and Structures*, 2005. To appear.

[6] G. Barthe, P. D'Argenio, and T. Rezk. Secure Information Flow by Self-Composition. In R. Foccardi, editor, *Proceedings of CSFW'04*, pages 100–114. IEEE Press, 2004.

[7] G. Barthe and L. Prensa-Nieto. Formally verifying information flow type systems for concurrent and thread systems. In M. Backes, D. Basin, and M. Waidner, editors, *Proceedings of FMSE'04*, pages 13–22. ACM Press, 2004.

[8] G. Barthe and T. Rezk. Non-interference for a JVM-like language. In G. Morrisett and M. Fähndrich, editors, *Proceedings of TLDI'05*. ACM Press, 2005.

[9] Massimo Bartoletti, Pierpaolo Degano, and Gianluigi Ferrari. Method inlining in presence of stack inspection. In *Workshop on Issues in the Theory of Security (WITS'04)*, 2004.

[10] Massimo Bartoletti, Pierpaolo Degano, and Gianluigi Ferrari. Program transformations under dynamic security policies. In *MEPHISTO Final Workshop*, volume 99 of *Electronic Notes in Computer Science*. Elsevier, 2004.

[11] Massimo Bartoletti, Pierpaolo Degano, and Gianluigi Ferrari. Policy framings for access control. In *Workshop on Issues in the Theory of Security (WITS'05)*, 2005.

[12] Michele Boreale and Marzia Buscemi. A framework for the analysis of security protocols. *Theoretical Computer Science*, 2005. To appear.

[13] 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, 2004.

[14] L. Caires and L. Cardelli. A spatial logic for concurrency–II. *Theor. Comput. Sci.*, 322(3):517–565, 2004.

[15] L. Caires and E. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. In *Proc. of CONCUR'04*, number 3170 in Lecture Notes in Computer Science, pages 240–257. Springer Verlag, 2004.

[16] Luis Caires and Etienne Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. *Theoretical Computer Science*. To appear.

[17] S. Dantchev and F. Valencia. On infinite CSP's. In *In proceedings of the Third International Workshop on Modelling and Reformulating CSPs*, 2004.

[18] Yuxin Deng and Catuscia Palamidessi. Axiomatizations for probabilistic finite-state behaviors. In *Proceedings of the 8th International Conference on Foundations of Software Science and Computation Structures*, Lecture Notes in Computer Science. Springer, 2005. To appear.

[19] Yuxin Deng and Catuscia Palamidessi. Axiomatizations for probabilistic finite-state behaviors. In *Proceedings of the 8th International Conference on Foundations of Software Science and Computation Structures*, Lecture Notes in Computer Science. Springer, 2005. To appear.

[20] Yuxin Deng and Davide Sangiorgi. Ensuring termination by typability. In *Proceedings of the 3rd IFIP International Conference on Theoretical Computer Science*, pages 619–632. Kluwer, 2004.

[21] Yuxin Deng and Davide Sangiorgi. Towards an algebraic theory of typed mobile processes. In *Proceedings of the 31th International Colloquium on Automata, Languages and Programming*, volume 3142 of *Lecture Notes in Computer Science*, pages 445–456. Springer, 2004.

[22] Yuxin Deng and Davide Sangiorgi. Towards an algebraic theory of typed mobile processes. *Theoretical Computer Science*, 2005. To appear.

[23] Gianluigi Ferrari and Alberto Lluch-Lafuente. A Logic for Graphs with QoS. In *First International Workshop on Views On Designing Complex Architectures*, Electronic Notes in Computer Science, Bertinoro, Italy, September 2004. Elsevier. To appear.

[24] Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Verification on the web of name-passing process calculi. In *Workshop on Software Engineering Tools: Compatibility and Integration, Monterey Workshop Series*, LNCS, 2004. To appear.

[25] Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Model Checking for Nominal Calculi. In *FOSSACS*, LNCS, Edinburgh, UK, 2005. Springer. To appear.

[26] Neil Ghani, Kidane Yemane, and Björn Victor. Relationally staged computations in calculi of mobile processes. In *Proceedings of CMCS 2004 (7th International Workshop on Coalgebraic Methods in Computer Science)*, volume 106 of *ENTCS*, pages 105–120, Barcelona, Spain, 2004. Elsevier.

[27] D. Hirschkoff. An extensional spatial logic for mobile processes. In *Proc. of CONCUR'04*, volume 3170, pages 325–339. Springer Verlag, 2004.

[28] D. Hirschkoff, D. Pous, and D. Sangiorgi. An Efficient Abstract Machine for Safe Ambients. In *Proc. of COORDINATION '05*, number 2004–63, 2005. To appear.

[29] E. Lozes. Separation logic preserves the expressive power of classical logic. In *Proc. Workshop Space'04*, 2004. Electronic publication.

[30] F. Martins and A. Ravara. Typing migration control in lsdpi. In *Proceedings of FCS'04*, volume 31, pages 1–12. Turku Centre for Computer Science, 2004.

[31] Marino Miculan and Kidane Yemane. A unifying model of variables and names. In *Proceedings of FOSSACS'05*, LNCS. Springer, 2005. To appear.

[32] Ugo Montanari. Web services and models of computation. In *First International Workshop on Web Services and Formal Methods*, volume 105 of *Electronic Notes in Computer Science*. Elsevier, 2004.

[33] D. Teller. Recovering resources in the pi-calculus. In *Proceedings of IFIP TCS 2004*. Kluwer, 2004.

[34] Emilio Tuosto. Tarzan: Communicating and Moving in Wireless Jungles. In A. Cerone and Alessandra Di Pierro, editors, *2nd Workshop on Quantitative Aspects of Programming Languages*, volume 112 of *Electronic Notes in Computer Science*, pages 77–94. Elsevier, 2004.

[35] Emilio Tuosto and Hugo T. Vieira. An Observational Model for Spatial Logics. In *First International Workshop on Views On Designing Complex Architectures*, ENTCS, Bertinoro, Italy, September 2004. Elsevier. To appear.

[36] Vasco T. Vasconcelos, António Ravara, and Simon Gay. Session types for functional multithreading. In *CONCUR'04*, volume 3170 of *Lecture Notes in Computer Science*, pages 497–511. Springer Verlag, 2004.

[37] S. Dal Zilio, D. Lugiez, and C. Meyssonnier. A logic you can count on. In *POPL 2004 – 31st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. ACM Press, 2004.

Papers Submitted for Publication, Reports, Drafts

[38] Jesper Bengtsson. Generic implementations of process calculi in Isabelle. In Paul Pettersson and Wang Yi, editors, *Proceedings of the 16th Nordic Workshop on Programming Theory*, number 2004-041 in IT Technical Reports, pages 74–78. Department of Information Technology, Uppsala University, October 2004.

[39] Michele Boreale, Marzia Buscemi, and Ugo Montanari. A general name binding mechanism. Submitted for publication, 2005.

[40] Marzia Buscemi and Ugo Montanari. A compositional coalgebraic model of monadic fusion calculus. Submitted for publication, 2005.

[41] Marzia Buscemi and Ugo Montanari. A congruence result for process calculi with structural axioms. Submitted for publication, 2005.

[42] Palamidessi C., Saraswat V., F. Valencia, and B. Victor. Linearity vs persistency in the pi-calculus. Ongoing Work.

[43] Fabio Gadducci, Marino Miculan, and Ugo Montari. About permutation algebras, (pre)sheaves and named sets. Submitted for publication, International Journal on Higher-Order and Symbolic Computation, 2004.

[44] E. Lozes. *Expressivité des logiques d'espaces*. PhD thesis, École Doctorale MathInf, ENS Lyon, 2004.

[45] D. Pous. GCPAN implementation. `http://perso.ens-lyon.fr/damien.pous/gcpan`, 2004.

[46] A. Ribeiro, L. Caires, and L. Monteiro. Verifying the Arrow Protocol in a Spatial Logic. Technical Report TR-DI/FCT/UNL-04/2004, Departamento de Informatica, FCT/UNL, 2004.

[47] D. Teller. *Ressources limitées pour la mobilité: utilisation, réutilisation, garanties*. PhD thesis, École doctorale MathIF, ENS Lyon, 2004.

[48] Antonio Vallecillo, Vasco T. Vasconcelos, and António Ravara. Typing the behavior of software components using session types. Technical report, December 2004. Revised and extended version of Typing the Behavior of Objects and Components using Session Types. In Foclasa 2002, 1st International Workshop on Foundations of Coordination Languages and Software Architectures. Electronic Notes in Theoretical Computer Science, 68(3), 2002.

[49] Vincent Vanackere. *TRUST: un systeme de verification automatique de protocole cryptographique.* PhD thesis, Université de Provence, 2005.