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

Deliverable 15: Self Assessment 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 15: Self Assessment Year 1

January 6, 2003

1 Summary

The work in PROFUNDIS has been successful in year 1 (2002), with only minor deviations from the TA (Technical Annex) and from the criteria established in the Self Evaluation Plan (SEP). An elaboration of what has been accomplished can be found in the Periodic Progress Report (PPR) for year 1. The present document contains a self assessment of our progress in relation to the SEP.

In some subtasks we have not yet met the criteria in the SEP but the shortcomings are not critical and can be recovered in subsequent years. The difficulties have mainly been that recruiting personell was slower than planned, and the slow start in Uppsala due to the fact that the co-ordinator moved from The Royal Institute of Technology (KTH) to Uppsala, leading to a delay in transfer of funds and ability to recruit. This can be compensated by setting a slightly higher pace in following years with the persons recruited in the second half of year 1.

In only one part of a subtask (Task 3.1 "Declassification") have we encountered technical obstacles that have prompted us to choose a different route from that originally planned. The difficulties and our revised approach are detailed in Section 5 below. It is not a critical deviation and will not have any impact on our main goals.

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 SEP, but here it can be remarked that management has proceeded completely as expected and without incidents or conflicts (after the transfer from KTH to Uppsala completed).

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 Self Assessment of Work Package 1

The work on WP1 has progressed according to what has been scheduled in the TA and SEP even if the work in Uppsala and Lisbon has been delayed due to the difficulties of recruiting personnel. The first year has been successful for all the tasks. In particular,

- Theoretical results have been established about HD automata modeled as coalgebras. They have provided the firm foundations needed for the experimental development. Also coalgebraic models (not necessarily finite state) of mobile calculi have been defined, equipped with operations of parallel composition and restriction. The coalgebraic-algebraic approach guarantees automatically fundamental properties like compositionality of abstract semantics.

- Symbolic verification techniques have been developed and applied to verify properties of security protocols. Verification toolkits exploiting symbolic techniques have been also designed, implemented and tested. The control reachability problem in the Dolev-Yao model of cryptographic protocols has been studied when principals are represented by tail recursive processes with generated names.

- A first version of the tool *Mihda*, which performs minimization of HD automata wrt. bisimilarity, has been designed and implemented following a specification-driven method. Some classical case studies have been implemented and tested. The tool is available on the web. Also, the distributed infrastructure of the PROFUNDIS Verification Environment has been designed. A preliminary implementation has been developed and tested. Some individual components of the PROFUNDIS Verification environment have been successfully integrated in the PROFUNDIS Verification environment.

The success of the activities in the first year can be measured in terms of the following facts:

- the work on the PROFUNDIS verification environment is a result of collaborations and visits within PROFUNDIS;
- the objectives indicated in the TA and SEP have been obtained. Some differences with respect to the SEP are discussed below;
- some of the papers have already become publications, in high-quality conferences and journals;
- the prototype implementation of the PROFUNDIS verification environment has been considered as an interesting case study within a national project (supported by the Italian ministry of education), which includes participations from industries, in particular the research center (TILab) of the Italian Telecom.

While initial drafts were expected on the topics "HD automata with fusions" and "Spatial logics" of Task 1.1. and 1.2 respectively, only work in progress can be claimed. The visits to Pisa of Yemane (from Uppsala) and Monteiro (from Lisbon) were instrumental to the ongoing work on the two topics, respectively.

4 Self Assessment of Work Package 2

The work in WP2 has progressed according to the schedule in the TA and the SEP, despite some difficulties encountered by Lisbon in recruiting personnel. According to the TA and the SEP, the work to be performed in the first year was mainly on Task 2.1 on logics for systems with spatial and temporal structure. We expected to achieve the following results:

- First version of the syntax and semantics of the spatial logics.
- Proof systems for spatial and temporal properties.

These objectives have been attained by the following contributions:

- A spatial logic to describe and verify properties of concurrent systems specified in the pi-calculus. The logic allows the specification of spatial and behavioural properties by induction and co-induction (for instance, properties related to resource usage), and includes freshness and hidden name quantifiers (important to define secrecy and non-interference properties).
- A sequent calculus based proof-system for the spatial logic that combines good proof-theoretic properties (*e.g.*, cut-elimination) and direct applicability to concurrency.
- New logics TL and SL to describe and query semi-structured data represented by multitrees, which can embed XML Schema as a plain subset. Decision procedures for satisfaction and model-checking the query languages logics TL and SL againts formal representations of semi-structured documents were provided.
- A logical formalization of the secure composition of web services.

On Task 2.2 we expected to have preliminary results on the expressiveness of versions of spatial logic. Several expressiveness and separation results were established in the case where we also consider in the underlying calculus the presence of the replication operator, that leads to possibly infinite behaviours and spatial decompositions.

The success of the activities in WP2 in the first year is justified as follows:

- The objectives indicated in the TA and SEP have been obtained, except for one minor delay discussed below.
- Some papers have been published or accepted for publication in high-quality conferences and journals.

The one point where our expectancy was not entirely fulfilled concerns a first version of the prototype theorem-proving tool for the spatial logic. Preliminary work on the tool has already started, but it did not yet give rise to a prototype. This delay is not serious and can be recovered in the second year.

The delay can be explained by the difficulty experienced by Lisbon in hiring a Ph.D. student or a postdoc to work on WP2. A Ph.D. student has started in September in Lisbon, but has not been able so far to contribute to the project. Lisbon expects to fill the postdoc position soon.

5 Self Assessment of Work Package 3

The work on WP3 has progressed according to the schedule in TA and SEP (in some cases, going beyond what originally expected). Taking into account the effort in manmonths put into WP3, we think that Year 1 for WP3 has been successful for the following reasons:

- the quantity and the quality (the originality) of the papers that have come out of the effort;
- some of the papers have already become publications, in high-quality conferences and journals
- some of the works are results of collaborations and visits, both within PROFUNDIS and between PROFUNDIS and other FET GC projects
- the objectives indicated in TA and SEP have been obtained (in the number of publications we are well above the 2 conference papers promised in the SEP); some (minor) differences with the TA are discussed below.

As anticipated in TA and SEP, most of the work for Year 1 has gone into Task 3.2 and, even more, into Task 3.1. We have already began the work in Tasks 3.3 and 3.4; these are tasks that we had originally planned to open only at Year 2.

In the TA, the description of Task 3.1 had several headers. They have all been tackled, with the excection of "Declassification" (see below). Some of the work done also cover aspects not announced in the TA; see the headers "access control" and "behavioural types" in the PPR (part B). This extra work is however strongly related, and is a natural addition, to the themes of Task 3.1.

We comment the lack of a contribution on the header "declassification." The problem of designing type systems for declassification appears to be much harder than expected. We have invited at the first PROFUNDIS meeting in Sophia an external speaker (F. Pottier) who has worked on this problem for sequential languages. We have learnt from Pottier's talk and subsequent questions that in concurrency we have probably not reached yet a point in which the problem can be successfully tackled. Although we remain very interested, we do not expect to be able to produce direct contributions on this point in the near future. We plan however to explore an indirect (but hopefully practical) approach to declassification in the case of the Java Virtual Machine (JavaCard and related languages are used for case studies in WP3); the goal is to establish a correspondence between a reference defensive virtual machine that performs verifications at run-time and may allow for declassification, and an implementation offensive virtual machine that relies on the bytecode verifier to perform verifications statically (building on previous work by Barthe, Courtieu, Dufay, and Melo de Sousa).

In Task 3.2, all the work has gone into the direction named "Operational and logical techniques for typed calculi" in the TA. This focus of interest in Task 3.2 can be justified both with its mathematical interest (it brings up challenging technical problems), and its practical significance (the study carried out was motivated by specific problems in systems and system development that we encountered while doing research elsewhere).

Inria was expecting to hire a PhD student and a Postdoc to work on WP3. These have arrived only in September, hence they have not been able to contribute yet. They have begun to work on tasks 3.2, 3.3, and 3.4. We expect useful output from them during next year.