Profundis

IST-2001-33100

Proofs of Functionality for Mobile Distributed Systems

Self Evaluation Plan

Report Version: first

Report Preparation Date: June 19, 2002

Self Evaluation Plan

The Approach to Self Evaluation

The purpose of this document is to set out a plan for self evaluation of project Profundis. As well as assessing the results of the project in contractual deliverables, this evaluation is expected to inform the *Steering Committe* (SC) in the scientific guidance of the project and in the day-to-day management of contingencies. It is therefore a process driven by project members and directed towards project members.

Self evaluation for Profundis will consist of assessing each workpackage systematically and thoroughly against its targets, as measured by set quality and success indicators. This document fixes such indicators; in particular, it prescribes evaluation and success criteria specific to each workpackage. The outcome of the assessment exercise will be reported in the final report (where appropriate), and in the yearly self-assessment deliverables.

Self Evaluation Procedure

The evaluation will be administered by the SC during the periodic workshops and project meetings, as well as by email and video/audio conference when the need arises. The SC consists of the coordinator (chair), currently Joachim Parrow, and all site and work package leaders, currently Ugo Montanari, Luis Monteiro, Davide Sangiorgi and Björn Victor. Self Evaluation will largely follow the structure of the Work Packages (WP). Each WP will initiate its own yearly Self Evaluation, well in time for the annual workshop. This is the responsibility of each WP leader and should be conducted in collaboration with all personell related to the WP, and possibly (if the WP leader so chooses) by consulting with an independent expert. A draft statement from the WP leader, commenting on how the WP fulfills the criteria set out in this plan, and possibly also suggestions for revised criteria for the present or following periods, should be available a few weeks before the workshop. At the workshop, ample time will be set aside for a SC meeting, and one part of the agenda will be discussion of the Self Evaluation drafts. At this point the SC may also choose to hear the opinion of independent experts specifically invited to the workshop. After the discussion, the WP leaders shall rewrite their drafts into formal Self Assesment reports and submit them to the coordinaror, who shall compile them into a report for the whole project.

Self Evaluation Criteria

Regarding setting the criteria, we follow a systematic methodology dividing indicators in two kinds: *checkpoints* ([C]) and *quality measures* ([Q]).

Checkpoints are objective measures with an easily verifiable fulfilment. They are mostly expressed in terms of the completion of a certain activity, or the production of a document, the creation of a tool, and similarly. The outcome of assessing such criteria is totally internal to the project, directed expressly to the

SC who will use it to monitor the steady progress of the project according to the set plan. Quality measures, on the other hand, are specifically designed to assess the impact of the project achievements. They are applied to deliverables after completion, and provide a set of criteria that serve the SC as well as external evaluators. Given the speculative and theoretical nature of the project, quality is often determined by acceptance and adoption of ideas and developments in the scientific community. The *Dissemination and Use Plan* for Profundis lists relevant conferences and journals.

Structure of the document. Having described the general infrastructure, we now proceed with the discussion specific to the work packages (WP). For reader's sake, we first describe concisely the general objectives of each WP as derivable from the Annex II to the contract (IST-2001-33100).

We then set the specific criteria that will apply to each of them at the set milestones.

Workpackage Objectives

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.

Evaluation Rounds

Month 12

WP1

We expect to have a publication in good conferences for each of the following topics of Tasks 1.1 and 1.2 [Q]:

a) Full formal specification of the minimization algorithm for HD automata with permutations.
b) Symbolic approach for the analysis of security protocols.
c) Mobile calculi with parallel composition and restriction, with firm coalgebraic foundations allowing for minimization.

We expect to have first prototypes on each of the following topics of Task 1.3 [C]:

d) Minimization tool for HD automata with permutations.
e) Tool for the symbolic analysis of security protocols.
f) Verification environment architecture (local).

We expect to have drafts of initial results for each of the following topics of Tasks 1.1 and 1.2 [C]:

g) Symbolic calculus with substitutions.
h) HD automata with fusions.
i) Spatial logic.

WP2

The work in this period will be mainly on Task 2.1, where we expect to have two publications in good conferences on the following topics [Q]:

a) First version of the syntax and semantics of the spatial logic.
b) Proof systems for spatial and temporal properties.

On Task 2.2 we expect to have a preliminary report on the expressiveness and decidability of validity and satisfaction of fragments of the logic (propositional version, restricted sets of connectives, restricted higher-order quantification) [C].

On Task 2.3 we expect to have a first version of the prototype theorem-proving tool for the spatial logic [C].

WP3

Most of the work will be on Task 3.1, on the following topics:

a) Classification of process interference.
b) Access control (controlling migration of processes and the resources on the host site that a migrated process can use).
c) Resource allocation.

d) Secure Composition of processes.

The work on Task 3.2 will be on these topics:

e) combination of operational techniques and type systems
f) space-sensitive type systems

We expect to have drafts of initial results on each of the above topics (a-f) [C].

We expect to have at least 2 publications in good conferences [Q].

Month 24

WP1

We expect to have a publication in good conferences for each of the following topics of Tasks 1.1 and 1.2 [Q]:

a) A symbolic calculus with permutations.
b) HD automata with fusions.
c) Spatial logic.

We expect to have prototypes on each of the following topics of Task 1.3 [C]:

d) Optimized version of the minimization tool for HD automata with permutations.
e) First version of the minimization tool for HD automata with fusions.
f) Second version of the verification environment architecture (distributed).
g) First version of a symbolic interpreter with substitutions.
h) First version of a tool for spatial logic.

We expect to have drafts of initial results on the following topic of Tasks 1.3 [C]:

Description of a collection of case studies.

WP2

On Tasks 2.1 and 2.2 we expect to have two publications in good conferences on the following topics [Q]:

a) Extensions to the logic with data domains and diverse notions of space like forests and labeled graphs, and high-level extensions handling resources, locations, and dynamically created objects.
b) Continuation of the investigation on expressiveness and decidability of the spatial logic.

On Task 2.3 we shall write a first report with a description of a collection of case studies, and have a first prototype of the integration of the theorem-proving tool with the project verification environment [C].

WP3

The investigation on the topics (a-f) from month 12 above will continue. In all these topics, the initial results obtained during the first year will become conference publications (when this has not already happened before Month 12) [Q].

The results of the first year will be developed for at least the topics (b),(c),(e). Some of these developments will involve:

— the design of type-inference algorithms, and the study of the robustness of our approach, as by Task 3.3;
— the implementation of some results or algorithms (or the integration of them in existing implementations of programming languages or tools), as by Task 3.4 [C].

For Task 3.2 we will also start the study of types that would allow us to capture existing type systems in a single framework; a first draft of results will be available at the end of the year [C].

Month 36

WP1

We expect to have two publications in good journals about HD-Automata with capabilities for name fusions and substitutions, about symbolic calculi for the analysis of security protocols and about spatial logic [Q].

We should have final versions of the tools, of the verification environment and of the case studies [C]. We expect them to be well accessed and distributed [Q].

WP2

We expect to have two publications in good conferences on a final integrated version of the logic with high-level extensions (Tasks 2.1, 2.2), and on a presentation of the final prototype of the proof tool (Task 2.3) [Q].

We shall have a collection of validated case studies, and a final version of the integrated proof tool for the logic (Task 2.3) [C].

We expect at least two publications in good journals describing the main contributions of the workpackage on the verification framework based on the spatial logic [Q].

WP3

For Task 3.1 and 3.2: we will publish the results obtained in year 2 in good conferences [Q].

For Task 3.3: we will study algorithms for type inference for (some of) the types introduced in previous years; we will study the transfer of results to realistic concurrent programming languages (these languages may be functional, or object-oriented) [C].

For Task 3.4: we will carry out some case studies for the type systems developed in the project; we will integrate techniques based on typed into the tools developped in WP1 [C].

At least three of the papers from the work package should be accepted for publication in good journqals [Q].