**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 14, 2005 |

Short Description: Automata with substitutions, Fusion and Bindings, Models for Open $\pi$-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: | |

# Contents

**1 Overview** **3**

**2 Scientific Contributions** **3**
2.0.1 Task 1.1: Automata with Operations and Substitutions . 3
2.0.2 Task 1.2: Proof Techniques . . . . . 5
2.0.3 Task 1.3: Prototype and Case Studies . . . . . 5
2.1 Update Second Year Report . . . . . 6

**3 Appendix: WP1 Scientific Contributions** **9**

**4 Appendix: WP1 Updated Versions** **10**

# 1 Overview

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 $\pi$-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 infrustructure (the Pweb). Moreover, we to assess our verification infrastructure we focussed on some case studies.

This deliverable includes the scientific contributions of the third year for WP1. The deliverable consists of a short presentation of the contributions and of several appendices with the contributed papers.

# 2 Scientific Contributions

The research activities of all tasks have advanced well, providing some results in terms of both publications and experimentation. Hereafter, we will briefly summarize the results of the research activities of the third year for each of the three tasks.

### 2.0.1 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. During the third year, we developed [13] 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. The approach we follow relies on the notions of reactive system and of observable borrowed contexts introduced by Leifer and Milner and further developed by Sassone, Lack and Sobocinski using G-categories and adhesive categories. The reduction semantics of reactive systems is extended in order to introduce as borrowed contexts both the variable instantiations needed in the transitions and the ordinary $\pi$-calculus actions. The proposed model can naturally describe interactions with binding mechanisms can be conveniently applied to handle web service discovery and invocations. Bialgebraic models of process calculi enjoy the property that bisimilarity is a congruence. Indeed, the unique morphism to the final bialgebra induces a bisimilarity relation which coincides with observational equivalence and which is a congruence with respect to the operations. However, the application of the bialgebraic approach to process calculi with structural axioms (e.g. name passing process calculi) is more

problematic, because of the interaction between axioms and inference rules. In [16], 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. In [17] we provide a compositional coalgebraic semantics of the Fusion calculus. In our model, the unique morphism to the final bialgebra induces a bisimilarity relation which coincides with hyperequivalence and which is a congruence with respect to the operations.

**Functorial Semantics for Nominal Calculi** We have here two lines of research, all aiming at the development of abstract models for nomical calculi. The first line of research developed at Uppsala concerns the development of functorial models for names. In [15] the techniques of higher order abstract syntax and functorial operational semantics have been extended to give a clean presentation of open bisimularity. 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 $Rel$. In [18] a category theoretic model where both "variables" and "names", usually viewed as separate notions, have been investigated. The proposal considers functors over the category of irreflexive, symmetric finite relations. The models previously proposed for the notions of "variables" and "names" embed faithfully in the new one, and initial algebra/final coalgebra constructions can be transferred from the formers to the latter. The second line of research developed in Pisa [14] aims at providing a general framework to relate the different abstract models of nominal calculi, namely *(pre)sheaf categories*, *nominal sets*, *permutation algebras* and *named sets*. The relationships among these models have been studied and the proposed frameworw allows one to transfer techniques and constructions from one model to the other.

**Fusion and Binding** We introduced [7] the U-Calculus, a process calculus with no I/O polarities and a unique form of binding. The latter can be used both to control the scope of fusions and to handle fresh name generation. The U-Calculus, is proven to be more expressive than pi-calculus and Fusion calculus separately. In U-Calculus, the syntactic nesting of name binders has a semantic meaning, which cannot be overcome by the ordering of name extrusions at runtime. Thanks to this mixture of static and dynamic ordering of names, U-Calculus admits a form of labelled bisimulation which is a congruence.

**Models for Spatial Logics** With respect to models for spatial logic, 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 [20].

**Other Extensions** A process calculus which combines both nondeterministic and probabilistic behavior has been developed [9]. We provide complete axiom-

atizations for finite-state processes, restricted to guarded definitions in case of the weak equivalences. This is the first work, to our knowledge, that provides a complete axiomatization for weak equivalences in the presence of recursion and both nondeterministic and probabilistic choice. In [8] we focused on the computational limits of open constraint satisfaction problems and on the relationships with *automata over infinite-sequences*.

### 2.0.2 Task 1.2: Proof Techniques

**Symbolic Verification Techniques for Security Protocols** As pointed out in the previous the previous PPR - symbolic verification techniques and security protocols - are now fully interdependent. We have here three lines of research, all aiming at the development of models and reasoning techniques for the analysis of security protocols. In the first line, developed at INRIA, concerns the TRUST cryptographic protocol verifier. The PhD Thesis of Vincent Vanackere [21] describes in full detail the theoretical basis, the design, the implementation and the application of the TRUST cryptographic protocol verifier. The second line of work, developed at Pisa, was also active in the first and second year had concerned with the development of a general framework for the analysis of security protocols [5] . We developed a general method for automatic analysis of security protocols based on the notion of *frame*, essentially a rewrite system plus a set of distinguished terms called *messages*. Frames are intended to model generic crypto-systems. Based on frames, we introduce a process language akin to Abadi and Fournet's applied pi. For this language, we define a symbolic operational semantics that relies on unification and provides finite and effective protocol models. Next, we give a method to carry out trace analysis directly on the symbolic model. We spell out a *regularity* condition on the underlying frame, which guarantees completeness of our method for the considered class of properties, including secrecy and various forms of authentication. We show how to instantiate our method to some of the most common crypto-systems, including shared- and public-key encryption, hashing and Diffie-Hellmann key exchange. The third line, also developed at Pisa [3] has addressed the development of a verification methodology for security protocols. In this approach, coordination techniques are exploited to guide the checking of the security properties reducing the dimension of the state space.

### 2.0.3 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 Profundis WEB each verification toolkit has an interface which is network accessible through standard network protocols and which describes the interaction capabilities of the verification toolkit. The PWeb is developed at Pisa and Uppsala. 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** The verification toolkits implemented in the first year of the project have been extended and/or re-engineered to accommodate new facilities, suggested by the theoretical investigations. In particular, the MIHDA front-end has been extended to take adavntage of type information. Moreover, the spatial model checker developed in Lisbon has been integrated inside the PWeb. By taking advantage of the avaiability of the new XML schemata, the spi2pi translator developed in Uppsala has been added as a new service of the PWeb in a economic fashion.

**Case Studies** We have two main contribution in the third year. The first contribution [11] 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 $\pi$-calculus. To illustrate the effectiveness and usability of our approach, we consider some case studies. In particular, the verification of the KSL protocol will allow us to demonstrate how service coordination supports and facilitates modular verification techniques. The secondi contribution [4] creates a generic library for a variety of process calculi in the automatic theorem prover Isabelle.

## 2.1 Update Second Year Report

Several unpublished notes described in the second year report have been revised and published during the third year of the project [12, 2, 19, 6, 1, 10].

# References


[1] 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.

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

[3] 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.

[4] 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.

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

[6] Michele Boreale, Marzia Buscemi, and Ugo Montanari. D-fusion: A distinctive fusion calculus. In *Programming Languages and Systems: Second Asian Symposium, APLAS 2004, Taipei, Taiwan, November 4-6, 2004. Proceedings*, volume 3302 of *LNCS*. Springer, 2004.

[7] Michele Boreale, Marzia Buscemi, and Ugo Montanari. A general name binding mechanism. In *Symposium on Trustworthy Global Computing*, 2005. To appear.

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

[9] 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.

[10] Gianluigi Ferrari, Stefania Gnesi, Ugo Montanari, Roberto Raggi, Gianluca Trentanni, and Emilio Tuosto. Verification on the WEB. In Juan Carlos Augusto and Ulrich Ultes-Nitsche, editors, *VVEIS 2004*, pages 72–74, Porto, Portugal, 2004. INSTICC Press.

[11] Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Modular verification of systems via service coordination. In *Workshop on Software Engineering Tools: Compatibility and Integration, Monterey Workshop Series*, LNCS, 2004. To appear.

[12] Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Co-algebraic minimization of HD-automata for the $\pi$-calculus using polymorphic types. *Theoretical Computer Science*, 2005. To appear.

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

[14] 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.

[15] 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.

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

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

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

[19] L. Monteiro. A noninterleaving model of concurrency based on transition systems with spatial structure. In *Proceedings of CMCS 2004 (7th International Workshop on Coalgebraic Methods in Computer Science)*, volume 106 of *ENTCS*. Elsevier, 2004.

[20] 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, 2004. Elsevier. To appear.

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

# 3 Appendix: WP1 Scientific Contributions

This section lists the papers contributing to Work Package 1.

1. Appendix 1.3.1
   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.

2. Appendix 1.3.2
   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.

3. Appendix 1.3.3
   Michele Boreale and Marzia Buscemi. A method for the analysis of security protocols. *Theoretical Computer Science*, 2005. To appear.

4. Appendix 1.3.4
   Michele Boreale, Marzia Buscemi, and Ugo Montanari. D-fusion: A distinctive fusion calculus. In *Programming Languages and Systems: Second Asian Symposium, APLAS 2004, Taipei, Taiwan, November 4-6, 2004. Proceedings*, volume 3302 of *LNCS*. Springer, 2004.

5. Appendix 1.3.5
   Michele Boreale, Marzia Buscemi, and Ugo Montanari. A general name binding mechanism. In *Symposium on Trustworthy Global Computing*, 2005. To appear.

6. Appendix 1.3.6
   Stefan Dantchev and Frank D. Valencia. On infinite CSP's. In *In proceedings of the Third International Workshop on Modelling and Reformulating CSPs*, 2004.

7. Appendix 1.3.7
   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.

8. Appendix 1.3.8
   Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Modular Verification of Systems via Service Coordination. In *Workshop on Software Engineering Tools: Compatibility and Integration, Monterey Workshop Series*, LNCS, 2004. To appear.

9. Appendix 1.3.9
Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Model Checking for Nominal Calculi. In *FOSSACS*, LNCS, Edinburgh, UK, 2005. Springer. To appear.

10. Appendix 1.3.10
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.

11. Appendix 1.3.11
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.

12. Appendix 1.3.12
Buscemi Marzia and Montanari Ugo. A compositional coalgebraic model of monadic fusion calculus. Submitted for publication, 2005.

13. Appendix 1.3.13
Buscemi Marzia and Montanari Ugo. A congruence result for process calculi with structural axioms. Submitted for publication, 2005.

14. Appendix 1.3.14
Marino Miculan and Kidane Yemane. A unifying model of variables and names. In *Proceedings of FOSSACS'05*, LNCS. Springer, 2005. To appear.

15. Appendix 1.3.15
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, 2004. Elsevier. To appear.

16. Appendix 1.3.16
Vincent Vanackere. *TRUST: un systeme de verification automatique de protocole cryptographique.* PhD thesis, Universit de Provence, 2005.

# 4 Appendix: WP1 Updated Versions

1. Appendix 1.3.1.1
Gianluigi Ferrari, Ugo Montanari, and Emilio Tuosto. Co-algebraic minimization of hd-automata for the $\pi$-calculus using polymorphic types. *Theoretical Computer Science*, 2005.

2. Appendix 1.3.1.2
Gianluigi Ferrari, Stefania Gnesi, Ugo Montanari, Roberto Raggi, Gianluca Trentanni, and Emilio Tuosto. Verification on the WEB. In Juan

Carlos Augusto and Ulrich Ultes-Nitsche, editors, *VVEIS 2004*, pages 72–74, Porto, Portugal, 2004. INSTICC Press.

3. Appendix 1.3.1.3
   Michael Baldamus, Joachim Parrow, and Björn Victor. Spi calculus translated to pi-calculus preserving may-tests. In *Proceedings of LICS'04, IEEE Press*, 2004.

4. Appendix 1.3.1.4
   L. Monteiro. A noninterleaving model of concurrency based on transition systems with spatial structure. In *Proceedings of CMCS 2004 (7th International Workshop on Coalgebraic Methods in Computer Science)*, volume 106 of *ENTCS*. Elsevier, 2004.

5. Appendix 1.3.1.5
   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.