

PROFUNDIS

Proofs of Functionality for Mobile Distributed Systems

IST 2001-33100

Co-ordinator: Joachim Parrow, KTH, SE

Objective:

Formal modelling and partly automated analysis of modern distributed systems: Systems that are

Open

Mobile

Extensible

Means:

Operational models

High-level logics

Advanced type systems

Participants

KTH Royal Inst. of Technology, Stockholm
Joachim Parrow, Mads Dam, Björn Victor

FFCT Universidad Nova de Lisboa
Luis Monteiro, Luis Caires, Antonio Ravara

INRIA Sophia Antipolis
Davide Sangiorgi, Roberto Amadio, Gilles Barthe, Ilaria Castellani, Daniel Hirschhoff

PISA Università di Pisa
Ugo Montanari, Michele Boreale, Gianluigi Ferrari, Stefania Gnesi, Marco Pistore

WP1: Models

Leader: Ugo Montanari

Automata with operations and substitutions

Generalisation of HD-automata

Include name fusions, algebraic structure etc

Proof techniques

Symbolic execution

Semantic equivalence and test contexts

Co-inductive techniques

Prototypes and case studies

Mobility Workbench

Integration

WP2: Specifications

Leader: Luis Monteiro

Logics with spatial and temporal structure

Based on temporal logic with fixed points
Include intentional connectives
Sequent-based proof systems

Expressiveness

Decidability issues
High-level extensions

Tools and case studies

Supporting the logical framework
Semi-automatic user assisted verification

WP3: Types

Leader: Davide Sangiorgi

Interference and access control

Designing novel type systems

Interference, resource allocation, declassification, etc

Integrating with operational and logic techniques

Extending WP1 and WP2

Practicality and Scalability

Type inference

High-level constructs

Case studies and tools

Type inference / checking

Integration with tools from WP1 and WP2

Other

Duration

3 years, starting 1/1 2002

Funding

1 268 KE

Workshops

One per year

Invited speakers

Internal review of deliverables

Steering committee meeting

School

At end of project