Formal Testing and System Exploration
Research Group Members

Permanent Members (June 30th, 2013)

<table>
<thead>
<tr>
<th>Name</th>
<th>First name</th>
<th>Position</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAUDEL</td>
<td>Marie-Claude</td>
<td>PREM</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>LONGUET</td>
<td>Delphine</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>VOISIN</td>
<td>Frédéric</td>
<td>MCFHC</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>WOLFF</td>
<td>Burkhard</td>
<td>PR2</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>ZAIDI</td>
<td>Fatihha</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
</tbody>
</table>

Group evolution

- Delphine Longuet joined the team on September 2009 as a Maître de Conférences
- Abderrahmane Feliachi joined the team in September 2009 as a Ph. D. student
- Huu Nghia Nguyen joined the team on January 2010 as a Ph. D. student
- Markus Wenzel joined the team on April 2010 as a post-doc
- Rania Khefifi joined the team on November 2010 as a Ph. D. student
- Romain Aissat joined the team on September 2012 as a Ph. D. student
- Yacoub Nemouchi joined the team on September 2012 as a Ph. D. student
- Frédéric Tuong joined the team on December 2012 as a Ph. D. student
- Johan Oudinet left the team on December 2010 after passing his Ph.D.
- Matthias Krieger joined the team on September 2009 and left on March 2012 after passing his Ph.D.
- Lina Bentakouk left the team on December 2011 after passing her Ph.D.
- Pascal Poizat left the team on September 2012 and is now a professor at LIP6
- Abderrahmane Feliachi became post-doc after defending his thesis in December 2012.

Research Description

The research of the ForTesSE group is dedicated to formal methods and their applications to soft- and hardware systems. Particular emphasis is put on combinations of Test and Proof techniques.

There are three strongly related fundamental research activities underlying our approaches to system validation and verification. We categorize as follows:

1. testing using logical representations and proof techniques,
2. random exploration methods, and
3. behavioural models for testing, adaptation and composition.

The fundamental research of the group relies on theoretical activities around the formalisms used for specification and modelling (logics [1, 42, 56], transition systems [26, 30] and process algebras [5, 28]) and their associated verification methods (theorem proving [4], symbolic evaluation [16, 32], model-checking [7, SP-5]) or exploration methods (random-based exploration of large models or programs (SP-1)).

On the other end, the group engages to apply these activities in the development of tools, which is driven by specific application domains in software engineering. This is reflected by a number of international collaborations with industrial partners, be it directly [76] or within national [78, 75] or European projects [77].
Testing using logical representations and proof techniques


Techniques for automated test generation — be it from specifications in form of pre- and postconditions, from transition systems or from annotated programs — suffer from state-space explosion similarly to model-checking techniques. One possible answer to the challenge is to use symbolic representations of models, their normal forms, symbolic states and symbolic test cases (partitions of test data) were generated, processed, and finally input into constraint-solving techniques for test data selection. This way, the state-space explosion can be deferred at a later stage, allowing usually for a “deeper” exploration of the test space.

Theorem-prover based testing. Instead promising “push-button”-solutions to model-based testing, we developed an interactive test development approach based on the theorem proving environment Isabelle/HOL. The resulting HOL-TestGen system (4) is designed to explore and exploit the complementary assets of test and proof (an example is (16), where a proven correct symbolic transformation of problem-specific specifications allows drastically improved test generations).

Built on top of a widely-used interactive theorem prover excelling with a logical language of nearly unlimited expressive power, it provides automatic procedures for test case generation and test data selection as well as interactive means to perform logical massages of the intermediate results by derived rules. The purpose of this line of research is to investigate universal, i.e. not specification language oriented techniques for the representation of test specifications and their decomposition. This covers monadic representations of test sequences and infrastructures for automated test driver generation. We put particular emphasis on extending the Isabelle platform by pervasively parallel symbolic computing (36), which improves the exploitation of current multi-core hardware by an order of magnitude (33). Our developments inside the ANR Project Paral-ITP are meanwhile integrated in Isabelle’s standard distribution, together with an IDE-like user-interface (51).

Testing based on Process Algebra Specifications. Process algebras like CSP (Concurrent Sequential Processes), CCS/Lotos or Circus provide a framework to model abstract and concrete system processes, their reactive behavior and their architecture in form of sub-processes. We produced a logical embedding of the Circus language in Isabelle/HOL, geared towards efficient symbolic computing (42, 28), developed a testing theory (5) together with an efficient symbolic implementation called Cirta (79), which is currently integrated into HOL-TestGen in order to combine process-oriented with generic data-oriented test generation. Cirta generated automatically JUnit test suites for a critical component of a pacemaker monitoring system in collaboration with Biotronik GmbH (79).

Modeling Security Policies. The goal of this research area is to find unified framework to security policies, the “Unified Policy Framework” (UPF) enabling to model, combine, and test security enforcement points in system architectures and to test and prove abstract properties over them (see Brucker,Wolff: Formal firewall testing. Accepted in Aug.’13 in: Softw. Test. Verif. Reliab.). UPF has similar goals to Belnap-Logics for security modeling, but a more constructivist flavor. The main incentive of the approach is to view UPF-models as testable specifications. The UPF framework as well as concrete policies are specified in Higher-order logic. We mention two UPF-instance used in major case studies:

- automatic generation of test-cases for firewalls from policies (16), and Formal firewall testing mentioned above), and
- together with our industrial partner BT, addressed the access-control policies for a large-scale patient data-management system for the NHS in Britain (17).

Operating and Embedded Systems. The goal of this research area is to develop modeling and testing techniques for low-level, machine oriented computer components. This includes memory and processor models (19) and their embedding in a “real OS”-environment (6) and related verification methods (1, 25). The models are typically oriented on bitvector representations: successful verification attempts require combinations of test and proofs in industrial certification processes (as undertaken in (77)).

Random exploration methods

Participants: M.-C. Gaudel, J. Oudinet, F. Volsin, R. Alissat

Laboratoire de Recherche en Informatique / 2008-2013 report
Methods based on randomness seem attractive for testing large programs or checking large models. However, designing efficient random methods is far from obvious since the underlying probability distributions must be carefully designed to get a good coverage of the program or model and to quantify it probabilistically. On the basis of classical results in the area of random generation of combinatorial structures, we have developed algorithms and tools for the randomised exploration of graphs with probabilistic guarantees of coverage. This work has led to applications to random program testing and model-checking. The main aspects have been published in STTT in 2011 (SP-1). It has involved members of several LRI groups: Algo, BioInfo, ForTesSE and of the “Equipe de Logique Mathématique de Paris 7”. Since 2008, our main results are the following.

The **dichopile** algorithm and the RUKIA library. Implementations of uniform random generation algorithms (namely recursive methods) need tables whose size grows with the length of the paths to be generated. Moreover, using floating numbers is essential for time and memory efficiencies. We have studied two different strategies: The first, most natural one, consisted in inverting the recurrences that are used in the classical recursive method; however, this method exhibits numerical instability when using floating point arithmetic (11). This led us to develop the second one called **dichopile**: based on a divide-and-conquer approach, it avoids numerical instability and offers an excellent compromise in terms of space and time requirements. The algorithm was published in Gascom’2010 (SP-10) and then in TCS (SP-2). Combined with our methods for uniform path exploration in very large composed models, it dramatically improves the scalability or our approach: in his thesis J. Oudinet was able to generate paths of length 4000 in an automaton with more than 12 million states (81). All these algorithms are implemented and available in the RUKIA library. Rukia is a free software under Lesser GNU Public License (LGPL).

Uniformly randomised LTL model-checking. We have generalised uniform drawing of paths to uniform drawing of so-called “lassos” that are interesting for model-checking of LTL formulas. This implies counting and drawing elementary circuits, which is known as a hard problem. However, efficient solutions exist for specific graphs, such as reducible data flow graphs, which correspond to well-structured programs and control-command systems. This work was published at ETAPS-FASE 2011 (SP-11) and integrated in RUKIA. An interesting perspective would be to embed this method in an existing model-checker such as SPIN or CADP, with the aim of developing efficient randomised methods for LTL model-checking with as result a guaranteed probability of satisfaction of the checked formula.

Randomised coverage of states and transitions and Applications to structural testing of programs. This work revisits the thesis of Sandrine Gouraud, who left the team in 2008. Uniform drawing of paths has been adapted to address the coverage of other structural items like vertices (states), edges (transitions) or some structurally defined subset of all paths. The RUKIA library has been enriched accordingly by R. Aissat, a new PhD student. Our aim is showing that coverage-biased drawing of paths can be improved for not drawing too many unfeasible paths and can scale up reasonably well. Among other techniques we investigate the use of program slicing and of annotations on combinatorial aspects of a computation (like relations about the numbers of traversals of different loops or other parts of the program) in addition to the usual annotations about its functional behavior. We plan to implement a prototype within the Frama-C platform (http://frama-c.com) for a realistic subset of C, possibly using a memory model in the lines of (1) integrated in the ACSL annotation language provided by Frama-C.

**Behavioural models for testing, adaptation and composition**


Behavioural models are very relevant for different domains of research. In our case, we need such models for testing, composition and adaptation techniques (7). We have conducted research based on formal models to verify, test, compose, and adapt Web services and communicating protocols. Our aim is to propose models that capture the genuine features of the applications in order to be closer to the real implementation which is very important especially when testing. The composition of Web services can be done from several perspectives, a centralised one, known as orchestration, or a distributed one, known as choreography. Such composition allows to create from existing services new added-value services.

**Service Orchestration Modelling and Testing.** Abstraction used in the requirement, composition, and adaptation processes, together with the important role played by composition execution engines, make
it important to test service compositions. In this direction, we have addressed conformance testing of service orchestrations with several methods that go from enumerative (24, 60) to symbolic approaches. The main contributions of this work are an end-to-end and fully automated online testing technique and a symbolic approach to avoid state space explosion in formal models due to the rich XML-based data used in Web service interfaces. This work has been published to Testcom/fates 2009 and TAP 2010 (31, 32). A tool is available as an eclipse plug-in at http://swst.lri.fr.

Model-checking and testing of Distributed and Concurrent Systems. In distributed environment, services can be developed independently and are composed to achieve common requirements through interactions between them. Several kinds of models like service choreographies, message sequence charts or Petri nets are used to define such requirements, specifying the interactions among a set of participants. As for choreography specifications, we have formalized the problems and developed a framework by which service choreographies can be developed correctly for top-down or bottom-up approaches. It consists in analyzing relation between a choreography specification and a choreography implementation at both model and real implementation level. Particularly, it concerns the composition/decomposition service design (35, 34), the testing of choreography implementation. In our framework, we support value-passing among service by using symbolic technique and SMT solver, which allows to overcome false negatives state space explosion issues due by abstracting or limiting data domain of value-passing in existing approaches. The second strength of our approach relies on the black-box passive testing of choreographies implementation. The framework is fully implemented and can be used online through a Web application (http://Schora.lri.fr). This work has been published in SAC 2012, ICSOC 2012 and in HASE 2012 (47, 46, 30).

We also started to work on testing from Petri net specifications of concurrent systems, proposing a theoretical framework for this purpose. We defined several conformance relations allowing to handle concurrency explicitly. We proposed a test case generation algorithm and we defined a test selection criterion that allows to build a finite test set from an exhaustive infinite one, which covers every basic behaviour the specification describes. This work has been published in TAP 2012 (26).

Testing and model-checking of protocols. Based on the background of conformance and interoperability testing of communicating systems (44), we have addressed some of new issues raised by Wireless Self-Organizing Networks (WSON). We have proposed models that deal with such specific constraints and defined a testing generation approach to test properties of WSON protocols. We have also defined specific testing architecture that mainly relies on monitors to test the properties (9, 45, 39). In the network area, we have also proposed a flexible proactive data dissemination approach for data gathering in self-organized Wireless Sensor Networks (WSN). To address this issue, we gained experience from our background on random strategy and walks. This work has been published in MSWIM 2010 (SP-4).

We have also started an activity of model-checking in collaboration with Sylvain Cochon of the team Toccata. We have worked on an efficient model-checker, Cubicle, for parameterized systems that proved the safety of cache coherence protocols and mutual exclusion algorithms. This work has been published in CAV 2012 (SP-5).

Context-Aware Personal Information Integration Users are faced with an increasing amount of personal information that are available under different formats (e.g., pdf, doc, mails, calendar). This leads to a real need to develop tools that can help them to manage efficiently this big amount of heterogeneous personal information. Personal Information Spaces (PIS) are at the core of Personal Information Management Systems (PIMS). They enable the structuring, storage, and retrieval of data on-demand. In (SP-12), we have proposed a semantic context-aware PIS. The user may define his/her own ontology for personal information ontology directly or by reuse of existing domain ontologies. Furthermore, we have considered the fact that the usability of personal information depends on contexts.

1/ ForTesSE

Collaborations

Participation to national and international collaborative research projects

- VERAP, ANR, approximate verification of Probabilistic Systems, Michel de Rougemont (scientific coordinator), LRI, LIAFA, Équipe de Logique Mathématique, Université Paris 7 and CNRS

Laboratoire de Recherche en Informatique / 2008-2013 report
Collaborations with other laboratories

- MBT-SEC, (funded by British Telecom), Deriving test-cases from security policies seen as model-based specifications. (17, 16, 37) (Sept. 2007 - Aug. 2010).
- Aline Carneiro Viana, Equipe Hipercom, Inria-Saclay, Réseaux auto-organisables (SP-4, 9).
- Stéphane Maag, Telecom SudParis, SAMOVAR UMR, Test de protocoles de communications (9, 45, 60).
- R. Lassaigne, Equipe de Logique Mathématique, Université Paris 7 and CNRS - UMR 7056: RAndom System Testing and Analysis, (SP-1, SP-11), (SP-3)
- Ana C. V. de Melo, co-tutelle PhD, Universidade de Sao Paulo, Paulo Salem da Silva, Multi-Agent Systems Verification by Means of Simulation Analysis, November 2011, (85).
- Radu Mateescu, Gwen Salaun, LIG and INRIA-Grenoble, Service adaptation and choreography verification, (7)
- Y Yan, Concordia University (Canada), Service composition and repair (54, 55, 34)
- Stefan Haar, co-directed PhD, LSV ENS Cachan: Hernán Ponce de León: testing concurrent systems with event structures, (26)

Participation to national and international networks

Participation to “investissement d’avenir” program

- IDEX Paris-Saclay
- Labex DigiCosme (B. Wolff is co-director of the programme Scilex)
- IRT SystemX (B. Wolff and D. Longuet are part of the programme FSF (Projet Fiabilité et Sureté de Fonctionnement), which funds the thesis of F. Tuong.)

Volunteer Professional Service

Management Positions in Scientific Organisations

- Digiteo: M.-C. Gaudel, présidente du Comité des Programmes (2006-2013)
- GDR/GPL, Conseil Scientifique, M.-C. Gaudel (2008-)
- GDR/GPL, co-direction of the group MTIV2, F. Zaïdi, 2008-2011
- GDR GPL, co-direction of the COSMAL WG, P. Poizat (since 2011)
- Research council of the faculty of Science d’Orsay, member, F. Zaïdi (since 2012)
Organisation of Conferences and Scientific Events

- Service Cup at the Services joint conferences, 2012: P. Poizat, co-chair

Steering Committee memberships:

- FME, International Symposium on Formal Methods, M.-C. Gaudel (2006-)
- TAP, International Conference on Tests and Proofs, B. Wolff, (2011-)

Participation to editorial and programme committees

Journal editorial Committees

- 1024, Bulletin de la société informatique de France, SIF: M.-C. Gaudel (2013-)

Other Responsibilities

- F. Zaidi, elected member of the CCSU-27ième section (Commission Consultative des Spécialistes de l’Université)
- B. Wolff, elected member of the CCSU-27ième section (Commission Consultative des Spécialistes de l’Université)
- D. Longuet, nominated member of the board (“conseil de laboratoire”) of LRI, since 2011
- B. Wolff, elected member of the board (“conseil de laboratoire”) of LRI, since 2011

1/ ForTesSE

Honors

Prizes and Awards

- M.-C. Gaudel, Doctor Honoris Causa, University of York, 2013

Keynote Addresses

International

F. Zaidi, TAROT Summer School, Bath, 2008: The WebMov Project

B. Wolff, Brainstorming Workshop For Creation of Center of Excellence in Information and Communication Technology, Indian Institute of Technology (IIT), Jodpur, Rajasthan, 2010: Formal Methods and Its Relevance for Industry and Emmergent Markets


F. Zaidi, TAROT Summer School, University of St Petersbourg, 2011: Formal Testing of Web Services


France


B. Wolff, Digicosme Spring School, Orsay, 2013, Program Analysis and Verification

Other Honors

M.-C. Gaudel, Chevalier dans l’ordre de la Légion d’Honneur, 2012

1/ ForTesSE

Evaluation of Research

Editorial Boards

International

Science of Computer Programming, Elsevier: M.-C. Gaudel, member of the editorial board, 1981-

Formal Aspects of Computing, Springer: M.-C. Gaudel, member of the editorial board, 1989-

National

1024, Bulletin de la société informatique de France, SIF: M.-C. Gaudel (2013- )

Program Committees

Chair


ICST, IEEE International Conference on Software Testing,Verification and Validation, M.-C. Gaudel, general chair, 2010

ICTAC, International Colloquium on Theoretical Aspects of Computing, M.-C. Gaudel, chair of the special track on software testing, 2010


OCL 2011, International Workshop on OCL, B. Wolff, 2011,


Conferences and Symposia

- **TPHOLs08, International Conference on Theorem-Proving in Higher-order Logics, B. Wolff, 2008**
- **ICFEM, International Conference on Formal Engineering Methods, F. Zaidi, 2009**
- **FM 2009, 16th International Symposium on Formal Methods, M.-C. Gaudel, 2009**
- **FoVeOOS, International Conference on Formal Verification of Object-Oriented Software, B. Wolff, 2010 and 2011**
- **ICST, IEEE International Conference on Software Testing, Verification and Validation (Industry Track), B. Wolff, 2010 and 2011**
- **ICTAC, International Colloquium on Theoretical Aspects of Computing, B. Wolff, 2010 and 2013**
- **ICST Mentoring Program, International Conference on Software Testing, F. Zaidi, 2013**
- **ICSOFC, International Conference on Service Oriented Computing, P. Poizat, 2012**
- **ISSTA, ACM International Symposium in Software Testing and Analysis, M.-C. Gaudel, 2013**
- **Tools@, International Conference on Software Testing (Tools Track), B. Wolff, 2013**
- **FM 2014, 19th International Symposium on Formal Methods, M.-C. Gaudel, 2014**

Workshops

- **MBT, ETAPS Workshop on Model-Based Testing, M.-C. Gaudel, 2008, 2009**
- **MOCA, International Workshop on Modelling of Objects, Components, and Agents, P. Poizat, 2009**
- **ORGMOD, International Workshop on Organization Modelling, P. Poizat, 2009**
- **TAV-Web, 4th International Workshop on Testing, Analysis and Verification, F. Zaidi, 2010**
- **WCSI, International Workshop on Component and Service Interoperability, P. Poizat, 2010**
- **CAMPUS, Workshop on Context-Aware Adaptation Mechanisms for Pervasive and Ubiquitous Services, P. Poizat, 2010, and 2011**
- **Service Cup at the Services joint conferences, P. Poizat, 2010, 2011, and 2012**
- **ICSOFC PhD Symposium, P. Poizat, 2011**
- **UITP, International Workshop on User-interfaces for Theorem Provers, B. Wolff, 2011**
- **SCENARIOS, 1st International Workshop on Scenario-based Testing, F. Zaidi, 2011**
- **FormSERA, Workshop on Formal Methods in Software Engineering: Rigorous and Agile Approaches, F. Zaidi, 2012**

Member (national events)

• MSR, Colloque Francophone sur la Modélisation des Systèmes Réactifs, M.-C. Gaudel, 2009, 2011
• CIEL, Conférence en Ingénierie du Logiciel (CIEL is LMO+IDM), P. Poizat, 2012
• GPL2013, Journées du GDR GPL, M.-C. Gaudel, 2013

Evaluation Committees and Invited Expertise

International

• European Research Council (ERC Starting Grants), E. U.: M.-C. Gaudel member of Panel 6 (2008-2013)

National

• ANR, committee of programmes SIMI2, blanc et Jeunes Chercheurs et Chercheuses : M.-C. Gaudel (Mai 2011)
• CNRS, PEPS 2011, B. Wolff

Other evaluation activities

• Expertise for the ANR french agency - program INS and VERSO, F. Zaidi, 2012, 2011
• Expertise for the ANR french agency - B. Wolff
• Expertise for NWO (NL), P. Poizat, 2008, 2011
• Expertise for several ERC Advanced Grants, and for various projects submissions to EPSRC (UK), NSERC (Canada), FQRNT (Quebec), Christian Doppler Forschungsgesellschaft (Austria), NWO (NL), Research Grant Council Hong Kong, NICTA (Australia), DFG (Germany), M.-C. Gaudel, (2008-2013)

Hiring Committees

• B. Wolff, hiring committees of professor positions at University Paris-Sud in 2013, 2012
• F. Zaidi, hiring committees of assistant professor positions at University Paris-Sud in 2013 and 2010, at Grenoble and Lyon 1 in 2011, at Nancy in 2009
• D. Longuet, hiring committees of assistant professor positions at University of Poitiers and Ecole Centrale Paris in 2010

PhD and Habilitation Juries

• F. Zaidi: reviewer (5 PhD), examiner (8 PhD)
• B. Wolff: president (2 PhD), reviewer (9 PhD), examiner (2 PhD)
• F. Voisin: examiner (1 PhD)
• M.-C. Gaudel: president, reviewer, and examiner, several times.
Reviews of journal submissions

- Journal Software: Practice and Experience (Wiley), F. Zaidi, 2010
- JISA, Journal of Internet Services and Application, F. Zaidi, 2010
- ETRI, Korean Journal, F. Zaidi, 2010
- STVR, Software Testing, Verification and Reliability, F. Zaidi, 2009
- TSI, Technique et Science Informatique, 2009
- TOSEM, ACM Transactions On Software Engineering And Methodology (ACM), 2010
- STTT, Software Tools for Technology Transfer (Springer), B. Wolff, 2011
- Several journals, M.-C. Gaudel, (2008-2013)

1/ ForTesSE

Interactions with the social, economic and cultural environment

Popularisation of Research Results

- Contributions to “Fête de la Science”, 2012, general public, F. Voisin, secondary schools, B. Wolff
- Scientific board of Centre d’Alembert d’Orsay, M.-C. Gaudel, for many years ... http://www.centre-dalembert.u-psud.fr/
- Scientific board of the Club Science et Citoyens de Bobigny-Drancy: http://www.scienceouverte.fr/ with organisation of a guided tour of LRI for pupils of secondary schools in November 2012, M.-C. Gaudel,
- Board of the association “Femmes et Sciences”: http://www.femmesetsciences.fr/; presentations in secondary schools and in professional orientation forums, M.-C. Gaudel, since 2011
- Rayonnement du CNRS, article titled “Le test de logiciel : pourquoi et comment” in March 2012, M.-C. Gaudel, (66)

1/ ForTesSE

Strategy and five-year project

The ForTesSE group fused — as part of a general restructuring of the LRI — in July 2013 with the Toccata-team to a new group VALS. The strategy and five-year project of the new group can be found in Section 3.1 over the VALS team.
2/ Implication dans la formation par la recherche

Implication dans la formation par la recherche
2/ Implication dans la formation par la recherche

ForTesSE

**Graduate Courses**

- Master Informatique, Université Paris Sud,
- Test des Systèmes Informatique Burkhart Wolff
- Sûreté et Sécurité de Fonctionnement, Fatiha Zaidi,
3/ Strategy and five-year project

Strategy and five-year project
3/ Strategy and five-year project

Strategy and five-year project

Following the general policy of the LRI that suggests to group similar activities in larger teams, we decided to join the former teams ForTesSE and Toccata. The name of this new team is VALS, standing for “Verification/Validation of Algorithms, Languages and Systems”. We detail below why this fusion makes sense in a scientific point of view.

VALS team members

The new team is directed by Burkhart Wolff, aside with Claude Marché as co-director.

<table>
<thead>
<tr>
<th>Name</th>
<th>First name</th>
<th>Position</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>BENZAKEN</td>
<td>Véronique</td>
<td>PREX</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>BOLDO*</td>
<td>Sylvie</td>
<td>CR1</td>
<td>Inria</td>
</tr>
<tr>
<td>CHARGUÉRAUD*</td>
<td>Arthur</td>
<td>CR2</td>
<td>Inria</td>
</tr>
<tr>
<td>CONCHON*</td>
<td>Sylvain</td>
<td>PR2</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>CONTEJEAN*</td>
<td>Évelyne</td>
<td>CR1</td>
<td>CNRS</td>
</tr>
<tr>
<td>FILLIATRE*</td>
<td>Jean-Christophe</td>
<td>CR1</td>
<td>CNRS</td>
</tr>
<tr>
<td>GAUDEL</td>
<td>Marie-Claude</td>
<td>PR émérite</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>LONGUET</td>
<td>Delphine</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>MANDEL**</td>
<td>Louis</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>MARCHE*</td>
<td>Claude</td>
<td>DR2</td>
<td>Inria</td>
</tr>
<tr>
<td>MELQUIOND*</td>
<td>Guillaume</td>
<td>CR1</td>
<td>Inria</td>
</tr>
<tr>
<td>NGUYEN</td>
<td>Kim</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>PASKEVICH*</td>
<td>Andrei</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>PAULIN-MOHRING*</td>
<td>Christine</td>
<td>PREX</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>VOISIN</td>
<td>Frédéric</td>
<td>MCFHC</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>WOLFF</td>
<td>Burkhart</td>
<td>PR1</td>
<td>PARIS SUD</td>
</tr>
<tr>
<td>ZAÏDI</td>
<td>Fatihna</td>
<td>MCF</td>
<td>PARIS SUD</td>
</tr>
</tbody>
</table>

* member of the LRI-Inria joint team Toccata, directed by C. Marché.
** currently on leave ("détachement") at the Collège de France.
### Temporary Personnel (October 1st, 2013)

<table>
<thead>
<tr>
<th>Name</th>
<th>First name</th>
<th>Position</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>AÏSSAT</td>
<td>Romain</td>
<td>Doc.</td>
<td>PARIS SUD (AM)</td>
</tr>
<tr>
<td>CLOCHARD</td>
<td>Martin</td>
<td>Doc.</td>
<td>ENS Paris</td>
</tr>
<tr>
<td>DROSS</td>
<td>Claire</td>
<td>Doc.</td>
<td>AdaCore (CIFRE)</td>
</tr>
<tr>
<td>DUMBRAVA</td>
<td>Stefania</td>
<td>Doc.</td>
<td>PARIS SUD (AM)</td>
</tr>
<tr>
<td>FELIACHI</td>
<td>Abderrahmane</td>
<td>Post-doc</td>
<td>EURO-MILS</td>
</tr>
<tr>
<td>GONDELMAN</td>
<td>Léon</td>
<td>Doc.</td>
<td>PARIS SUD (ANR BWare grant)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM</td>
<td>Hyeonseung</td>
<td>Post-doc</td>
<td>PARIS SUD (ANR TypeX grant)</td>
</tr>
<tr>
<td>KHEFFI</td>
<td>Rania</td>
<td>Doc.</td>
<td>PARIS SUD (CDD)</td>
</tr>
<tr>
<td>LELAY</td>
<td>Catherine</td>
<td>Doc.</td>
<td>Inria (Digitéo PhD grant)</td>
</tr>
<tr>
<td>MARTIN-DOREL</td>
<td>Erik</td>
<td>Post-doc</td>
<td>Inria (ANR Verasco grant)</td>
</tr>
<tr>
<td>MEBSOUT</td>
<td>Alain</td>
<td>Doc.</td>
<td>PARIS SUD (AM)</td>
</tr>
<tr>
<td>NEMOUCHI</td>
<td>Yakoub</td>
<td>Doc.</td>
<td>PARIS SUD (CDD)</td>
</tr>
<tr>
<td>NGUYEN</td>
<td>Huu Nghia</td>
<td>Doc.</td>
<td>PARIS SUD (AM)</td>
</tr>
<tr>
<td>TAFAT-BOUZID</td>
<td>Asma</td>
<td>Post-doc</td>
<td>PARIS SUD (ATER)</td>
</tr>
<tr>
<td>TUONG</td>
<td>Frédéric</td>
<td>Doc.</td>
<td>IRT SystemX (CDD)</td>
</tr>
<tr>
<td>WENZEL</td>
<td>Markus</td>
<td>Post-doc</td>
<td>ANR Paral-ITP</td>
</tr>
</tbody>
</table>

## Self Assessment

**Strengths:** One of the particular strengths of both former teams ForTesSE and Toccata are their tradition of combining theory and practice, fundamental and applied research. Their research ranges from semantic models for specification- and programming languages, over concrete know-how in automated and interactive theorem-prover technology, down to the design and implementation of recognized tools and tool-chains for a variety of verification techniques. Successful applications, partly in collaboration with industrial partners, demonstrate that VALS will belong to the global players in the field of applied formal methods.

Both former parts of the VALS team have a strong national and international network with academic and industrial partners. We engage in various ANR and European projects. We also have intense local cooperation with major scientific players on the plateau de Saclay such as the CEA; here lies the key for its success in the development of recognized formal methods tools in an academic environment, together with the fact that it attracted a high number of permanent researchers.

Both former parts of VALS have a strong publication record and a high academic recognition in their respective fields, which is reflected in the participation of numerous program committees and conference organizations.

We'd like to add that we enjoy our collaborative style of research and the vividness of our group.

**Weaknesses:** While VALS has a clear focus on the foundational research axes, it can be asserted that its efforts in the various application domains is quite scattered driven by a perhaps too large variety of partnerships and collaborations. It would be desirable if the number of collaborations could be reduced to a smaller number of larger/more intensive partnerships.

With respect to the former Toccata part of the VALS team, it was criticized in the past that its collaborations are too French-centric. It was also recommended to address fundamental computing trends like concurrency more actively.

With respect to the former ForTesSE part of the VALS team, it can be criticized that its permanent staff is slightly over-aged, and needs a more active recruiting strategy to attract strong personal and to achieve a size which is more sane. It is particularly desirable that full-time researchers join the team on testing issues.

In order to maintain the quality of tools and documentation, the team should be reinforced by engineers.
Opportunities: The world of computing is changing: becoming ubiquitous, there are larger, more complex and more safety- and security-critical software systems whose quality must be assured by appropriate verification technologies. This is reflected by the growing demand for formal certification processes, e.g. Common Criteria ISO/IEC 15408 require the use of formal methods, both in Test and Proof, as developed in VALS.

Finally, it can be observed that there is for all tools (Frama-C, SparkAda, Isabelle, HOL-TestGen) an increasing number of users — reflected both by downloads and mailing list traffic.

New computing architectures — parallel / grid / cloud — represent new ways to master the inherent complexity of symbolic computing as is fundamental for the technologies developed in VALS. Such changes of basic technologies will have a profound effect both on verification methods, their demand by industrial partners, as well as their implementation.

Last but not least, we view the changes of the academic environment (catchword: Université Paris-Saclay) as a means to integrate verification engineering into traditional software engineering, which can be anchored more intensively into the bachelor and master programme of this institution — a way, to instruct and attract new scientific staff.

Threats: Advancing both fundamental research and tool development in an academic environment puts a team inevitably under a certain stress: Development of research tools is time-consuming and not always rewarding in terms of publications. While both former parts of VALS managed this balancing act quite well in the past, it can be safely stated that the complexity of underlying technology (e.g. multi-core architectures) and the demands of wider user groups (user interfaces, documentation) is growing. There is a perceivable threat that in the competition with industrial research institutions such as Microsoft Research, VALS might be outperformed simply by their investments both in terms of time and money. Just an example for the kind of concurrency we face: the white-box fuzz-test-generation tool SAGE uses a ca. 100 man year effort involving a massive parallel server farm to solve billions of constraints by Z3; the approach is used to systematically detect errors in Win7, Windows and Office.

As mentioned earlier, it is particularly difficult to attract PhD students and scientific staff that fits into our profile: the necessary combination of mathematics, logic and software engineering is difficult to find on the national and international market of applicants.

In principle, the underlying technologies of our research are remarkably computing intensive, which is a problem when scaling-up to industrial size systems. An obvious answer to this threat are new computing paradigms (massive parallel computing, multi-core and grid computing); in order to cope with these trends, additional training and personnel will be necessary.

Strategy

Why does the fusion make sense? Test and proof, originally perceived as adversaries, have a lot in common in leading edge approaches: as “formal methods” (FM), they have both their roots in logic and discrete mathematics, and they share an interest in formal semantics for programming and specification languages, in modeling-approaches for programs and systems, as well as constraint-solving technologies and theorem provers. This mutual interest is reflected by recent collaborations between Toccata and ForTesSE (the Cubicle project). Last but not least, we identified a set of challenges that both former parts of the team would like to address together, listed below.

General objectives. We identified the following general trends in the scientific community that corresponds to our potential in the new VALS team:

1. making verification an easier to use, more wide-spread technology;
2. gaining experience in non-standard application domains, for example hybrid and concurrent systems;
3. advancing the prover technology; e.g. by non-linear arithmetic and parallel prover design;
4. combining test and proof, e.g. by invariant-generation, verified optimized test-generations, etc.;
5. combining proofs and probability.

We believe that the fused VALS team is an adequate structure, joining complementary skills and expertise of its members, to address these objectives. The detailed scientific programme below corresponds to
the way we plan to implement solutions to these objectives.

Scientific Programme

The scientific programme of VALS is structured into six activities. We detail each of these activities below, together with the list of participants. We then provide a list of a few challenges that we want to address in the future. The interest in those challenges is shared between the former parts of the team. We then discuss the application domains we target, and finally give a few elements of positioning.

Activities


Automated Theorem Proving and its applications will remain an important activity of the team. This includes research around satisfiability modulo theories (Alt-Ergo prover), numerical constraint solving (Gappa solver), and applications like SMT-based model-checking (Cubicle).


The research around numerical programs took a lot of importance in the past 5 five years in particular in Toccata. We want to pursue these efforts, towards several directions such as the verification of numerical analysis systems, hybrid systems.

Formalisation of Languages. Participants: B. Wolff (contact), E. Contejean (contact), A. Charguéraud, D. Longuet, V. Benzaken, Ch. Paulin, C. Marché, S. Boldo.

Formalizing in a broad sense is indeed an activity of all members of former teams, in particular using assistants like Coq and Isabelle. It will continue in the future, for formalizing semantics of languages, concurrency, mathematical/numerical theories, etc.

Data-Centric Languages and Systems. Participants: V. Benzaken (contact), K. Nguyen, E. Contejean. This activity aims at designing and developing programming languages as well as systems that seriously take into account massive data. This includes improving existing languages and systems. Ultimately it aims at providing formally verified implementations of data intensive management systems.

Formal Model-based Testing. Participants: F. Zaïdi (contact), B. Wolff, D. Longuet, F. Voisin, M.-C. Gaudel. Testing will remain a strong research activity of the team. Important directions will be to scale up testing techniques by handling efficiently the concurrency aspects of distributed systems (for instance Web services, wireless self-organised networks, etc.) as well as by advancing symbolic and probabilistic approaches. Moreover, we will investigate how to overcome the infeasible paths issues for the test of C programs by finding suitable combinations with static analysis methods.


Our approach of deductive program verification is in need for improved techniques for modular reasoning, support for genericity, for higher-order programs, for refinement-based approaches. This is a key towards scaling-up, in particular via the development of reusable verified libraries.

Transverse challenges we want to address, shared by both former teams

Non-linear arithmetic. Critical software often involves numerical computations on physical quantities. Hybrid systems are those which mix continuous quantities and discrete ones. Such a system can be modeled typically by transitions systems guarded by numerical constraints. In all cases, the constraints involved are usually non-linear ones, hence both in the contexts of testing and proving, it is desirable to rely on automated decision procedures able to check the satisfiability of such kind of constraints.
Parallelism and verification. The challenge raised by parallelism in the context of verification is two-fold: a challenge as a target as well as an implementation means of verification tools. Testing of concurrent programs requires the definition of efficient architectures for distributed testing. Besides the challenge of modeling concurrency, already addressed in the activity Formalisation of Languages, there is the necessity to profit from advances in recent hardware: since 2005, there are no further increases of CPU clock-rates; increasing computing power can only be gained by addressing multi-core and grid computing platforms. This represents a sensible paradigm shift both in algorithmic design as well as system architecture.

Combination of dynamic and static analysis. Combining the respective power of dynamic methods (test, run-time checking) ans static analysis is an interesting research direction per se, and is certainly a way to leverage adoption of formal methods in industry. It is indeed required in certification processes in industry. We already have short-term plans to go in such a direction, in the context of platforms like Spark2014 for Ada, Frama-C for C code (and its executable-ACSL specification language), but also in our own platform Why3 for which we plan to provide an environment for directly executing annotated programs.

Verified languages, systems and tools. An emerging trend is the verification of the analysis tools themselves, as exemplified by the CompCert verified compiler. The assurance level provided by a system is directly related the size of its Trusted Code Base, i.e. the core of the system that is not verified, the remaining being verified on top of that core. Libraries (e.g. Flocq, ALEA) and tools (e.g. HOL-TestGen) built on top of assistants (e.g. Coq, Isabelle/HOL) have a small TCB, whereas standalone tools (e.g. automated theorem provers) have a large one. This challenge aims at reducing the TCB of such tools to small cores, thus producing “verified” tools. We target the development of verified theorem provers, verification condition generators, interpreters, compilers including compilers for data-centric languages, etc.

Probabilities and Verification. Scaling-up to large size systems is always a challenge for formal methods. The use of randomized methods is a very promising approach to solve scaling-up issues, ensuring a probabilistic guarantee of the results. Randomized methods have a great potential to apply on many domains including formal testing and proving. Besides, studying verification of randomized programs and systems, which have important application in security, must be continued.

Application areas

VALS will continue to seek for academic and industrial partners to advance and apply its technologies; this covers in particular projects concerning code-verification (in particular numeric algorithms involving floats), security infrastructures, web services, embedded and operating systems, etc. We will try to find more strategic partnerships with companies and larger shares in research projects.

Positioning in the local, national and international context

The domain of formal methods for software engineering is historically a major axis of research in the LRI. This domain of research is important in the context of the institutional evolutions of the “Plateau de Saclay”, in the recent past, the present and for the future. In the past years, the RTRA Digiteo played an important role for the development of collaborative research on the Plateau, and Software Engineering was one of its seven themes of its research programme. In the present, software was also important in the “investissements d’avenir”: SciLex is one of the three action lines of the Labex DigiCosme, centered on the reliability of software; the IRT SystemX, which is more focused on industrial applications, has one theme around embedded systems, where the same problematic appears. We are strongly involved in all these actions.

The near future is the creation of the Université Paris-Saclay, and the creation of a large computer science department. The interest in formal software engineering methods will be shared by several institutions: Inria Saclay, CEA, LSV, ENSTA ParisTech, etc. The new VALS team aims at playing a central role in this future join of forces on the Plateau. Also, we are strongly involved in the new Master programme of the future STIC department. This would be a new mean to attract students, e.g. from engineering schools, to do a PhD thesis.

Our strategy also fits in the national context. We are members of both GDR of CNRS “Génie de la Programmation et du Logiciel” and “Informatique Mathématique”. We will continue collaborations with
many teams in France. At the international level, we want to develop our contacts with major institutions and sites of our domain, such as Microsoft Research, ETH Zürich, Imperial College London, etc. Our involvement in the IFIP WG 1.9/2.5 is also representative of our involvement in world-wide trends.

We plan to continue and improve our collaborations with industrial partners, in particular the companies that promote formal methods. These collaborations are not only a precious source of concrete challenges and real case studies: they are a key for the spreading and the transfer of our methods and tools in the industry.
Annexe 1: présentation synthétique
Nom du responsable de l’équipe : Burkhart WOLFF

Effectifs de l’équipe
The group has now 5 university faculty members (1 PR, 3 MC, 1 PR émérite), 2 post-doctoral students, and 5 Ph.D. students. (compared to January, 2008 : 1 PR, 4 MC, 1 PR émérite, 2 Ph.D. students, and 1 post-doctoral student).

Personnels ayant quitté l’équipe pendant le contrat en cours
Johan Oudinet and Lina Bentakouk left the team on December 2011 after passing their Ph.D.; Matthias Krieger left on March 2012 after passing his Ph.D.; Pascal Poizat left the team on September 2012 and is now a professor at LIP6.

Nombre de recrutements réalisés au cours de la période considérée et origine des personnels
Delphine Longuet joined the team on September 2009 as a Maitre de Conferences after a Ph.D in Evry; Matthias Krieger and Abderrahmane Feliachi joined the team in September 2009 as Ph.D. students; Huu Nghia joined the team on January 2010 as a Ph.D. student; Markus Wenzel joined the team on April 2010 as a post-doc, coming from TUM, Munich; Rania Kheffifi joined the team on November 2010 as a Ph.D. student; Romain Aiissat and Yacoub Nemouchi joined the team on September 2012 as Ph.D. students; Frédéric Tuong joined the team on December 2012 as a Ph.D. student.

Production scientifique au cours de la période écoulée
We present four major results that are couples of high-level publications and available tool.

HOL-TestGen is free software; you can redistribute it and/or modify it under the terms of a BSD-style licence.
HOL-TestGen 1.5 has been deposited in APP: IDDN.FR.001.220032.000.S.A.2011.000.10000


Bilan quantitatif des publications de l’équipe
• Articles dans des revues internationales majeures: 11
• Articles dans les autres revues : 2
• Articles dans des conférences majeures: 23
• Articles dans les autres conférences et workshops : 31
• Livres et chapitres de livres : 6

5 publications majeures

5 (max) documents majeurs (autres que publications) 

The four publicly available tools mentioned as major results, plus several major contributions to Isabelle/HOL as a modeling platform as well as implementation framework for Formal Methods Tools, including the novel Prover IDE (PIDE). Five official Isabelle releases were managed at LRI by M. Wenzel since June 2010.

5 (max) faits illustrant le rayonnement ou l’attractivité académique

1. Chairing and/or organisation of seven important international scientific events, with edition of the proceedings:
2. Foreign visitors (long stays): Ana Cavalcanti, Jim Woodcock, university of York, UK; Petra Malik, Victoria University of Wellington, NZ; Manuel Munez, Universidad Complutense de Madrid, SP; Eliane Martins, Universidade de Campinas, BR.
3. Co-directed PhD theses (co-tutelle): ETH Zürich, Lukas Brügger; Universidade São Paulo, Paulo Salem da Silva.
4. Numerous International Programme Committees and Steering Committees memberships, editorial boards of international scientific journals: Marie-Claude Gaudel, 5PC, 2SC, 2EB; Markus Wenzel, 6PC, 2SC; Burkhart Wolff, 20 PC, 2SC; Fatihya Zaidi, 28 PC, 1SC.
5. Marie-Claude Gaudel was awarded Doctor Honoris Causa of the University of York, UK, and got several grants of the Royal Society and of the Royal Academy of Engineering.

5 (max) faits illustrant les interactions de l’équipe avec son environnement socio-économique ou culturel

1. Participation to the IRT System X: PhD thesis of Frédéric Tuong;
2. Participation to the European project Euro-Mils;
3. Participation to several ANR projects: Paral-ITP, PIMI, WebMov (ForTesSE leader), VERAP
4. Popular science: contributions to “Fête de la Science”; Scientific Board of Centre d’Alembert d’Orsay; Scientific Board of the Club Science et Citoyens de Bobigny-Drancy; Scientific Board of (Scube), “Scientipole Savoirs et Société”; administrative board of the association “Femmes et Sciences”; contribution to the journal “Rayonnement du CNRS”

Principal contributions de l’équipe à des actions de formation

Outside University Paris-Sud

- Summer, winter, and other seasons, schools: Summer SCHOOL TAROT (Training and Research on Testing), twice (Bath 2008, St Petersbourg 2011); Digicosme Spring School (Orsay 2013)
- Tutorials on Isabelle(Cambridge, Orsay, Paris, Orsay, Orléans, Edinburgh) and on HOL/TestGen (NII Tokyo, Euro-Mils Paris)

Inside University Paris Sud

- Responsabilité de la Licence Informatique
- Co-responsabilité du Master pro IICI
- Coordination de l’Informatique pour le Cycle Préparatoire de Polytech Paris-Sud
- Coordination de la spécialité informatique en troisième année (bac+3) de filière ingénieur (formation initiale) à Polytech Paris-Sud
- Responsabilité de la formation continue, spécialité informatique, Polytech Paris Sud
- Responsabilité pour l’informatique des Missions Enseignements pour Paris-Sud et membre du Comité de Pilotage des Missions Enseignement
- Correspondance pour Paris Sud du Master Comasic
Annexe 6: Realisations
### Contracts and grants

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Managing Institution</th>
<th>Start / Duration</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subvention CNRS</td>
<td>MoBasT</td>
<td>CNRS/Royal Society</td>
<td>01.2012 / 12 mo.</td>
<td>4.00 k€</td>
</tr>
<tr>
<td>Subvention DIGITEO</td>
<td>UTP’2012</td>
<td>Université Paris XI</td>
<td>01.2012 / 12 mo.</td>
<td>1.50 k€</td>
</tr>
<tr>
<td>Contrat ANR</td>
<td>PiMI</td>
<td>Université Paris XI</td>
<td>11.2010 / 36 mo.</td>
<td>180.57 k€</td>
</tr>
<tr>
<td>Contrat européen</td>
<td>EURO-MILS</td>
<td>Université Paris XI</td>
<td>10.2012 / 36 mo.</td>
<td>260.73 k€</td>
</tr>
<tr>
<td>Chaire U-PSud</td>
<td>HOL-TestGen XT</td>
<td>Université Paris XI</td>
<td>02.2009 / 36 mo.</td>
<td>170.00 k€</td>
</tr>
<tr>
<td>Chaire DIGITEO</td>
<td>HOL-TestGen XT (supp)</td>
<td>FCS Digiteo</td>
<td>02.2009 / 36 mo.</td>
<td>86.00 k€</td>
</tr>
<tr>
<td>Subvention DIGITEO</td>
<td>ICTSSv3</td>
<td>CNRS</td>
<td>07.2011 / 12 mo.</td>
<td>3.50 k€</td>
</tr>
<tr>
<td>Contrat ANR</td>
<td>Paral-ITP</td>
<td>Université Paris XI</td>
<td>11.2011 / 40 mo.</td>
<td>215.92 k€</td>
</tr>
<tr>
<td>Contrat ANR</td>
<td>WebMov</td>
<td>Université Paris XI</td>
<td>12.2007 / 30 mo.</td>
<td>163.46 k€</td>
</tr>
<tr>
<td>Contrat IRT SystemX</td>
<td>SysMLTests</td>
<td>Université Paris XI</td>
<td>1.1.2013 / 30 mo.</td>
<td>155.37 k€</td>
</tr>
</tbody>
</table>

---

**MoBasT**

*Partners: Université York, LRI*


This project aims at strengthening and consolidating an existing and fruitful collaboration in the area of software testing based on formal specifications. The considered specifications are in CIRCUS, a language developed in York, which integrates the notions of states and complex data types (in a Z-like style) and communicating parallel processes inspired from CSP. Moreover, the language comes with a formal notion of refinement and allows to take into account abstract specifications and their transitions to models of programs. On the bases of the theory of formal software testing and the proof and test generation tools developed in LRI the project will address the following questions: What are the integrated testing strategies applicable to such languages, which combine aspects that have been studied separately, so far, with respect to testing? What are the integrated testing strategies applicable to such languages, which combine aspects that have been studied separately, so far, with respect to testing? How to justify these strategies and their coherence with the underlying test hypothesis? How to implement them in a well-founded way, starting from the existing proof and generation tools that exist in York and Orsay? We also want to address the problem of the selection of finite test sets. Since, in the exhaustive test sets, we have a symbolic version of the tests, with labels constraining communicated values, it is natural to consider strategies based on constraints decomposition and solving. We propose as well to go further and address the challenging problem of providing coverage of complex internal data operations, and justify the soundness of the techniques.
**UTP’2012**

*Partners:* LRI


Subvention of the organization of the conference ICTSS, collocated with FM.

**PIMI**

*Partners:* GENIGRAPH, Genigraph, INRIA, IT Institut Telecom - Sud Paris, Montimage Montimage, LRI Université de Paris-Sid, IRIT Université Toulouse III


The future Internet will bring a growing number of networked applications (services), devices and individual data (including private ones) to end-users (citizens, consumers, employees). The important challenges are the organization of their access, and the guarantee of trust and privacy. The objectives of the PIMI project (Personal Information Management through Internet) are the definition of a model-based design environment and a deployment platform for Personal Information Management System (PIMS). The future PIMS must provide the end-user personal data access with services that are relevant to his needs. In order to take mobility into account, the PIMS will be accessed both by mobile devices (smartphone) and Internet-connected Personal Computers. With the increasing number of e-services and associated data being accessible through Internet, the number and complexity of PIMS will augment dramatically in the near future. This will require strong research investment in a number of topics, all contributing to the expected usability and accessibility of Individual Information Spaces for the end-user: Electronic trust and reputation of the services, Secured private data transfer between PIMS and between services, Ergonomic Human Computer Interface including mobile ones, Service composition and re-composition based on end-users requirements (life events), on e-service trust and runtime feedback, Quality of Service / Quality of Experience self adaptation, and Advanced algorithms to monitor the PIMS, the private data and service accesses.

**EURO-MILS**

*Partners:* Sysgo (France & Germany, coord.), Technikon(Austria), Open-Synergy(Germany), Jemm Research(France), EADS, Airbus(France), Thales (France), DFKI Saarbrücken (Germany), Universiteit Gent(Belgium), Open University(Netherlands), T-Systems (Germany)

See [https://www.euromils.eu](https://www.euromils.eu)

Secure European virtualisation for trustworthy applications in critical domains. The mission of the EURO-MILS project is to develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods. ForTesSE is involved in particular as part of the activity to use model-based testing techniques to establish conformance of the real code to the projects system models. Part of the research is oriented to the question, how can tests be organized in a format such that it is useable in an Common Criteria EAL5+ certification process.

**HOL-TestGen XT**

*Partners:* LRI

See ---

The ultimate goal of this research proposal is to extend the realm of feasible state-spaces for HOL-TestGen by 4 orders of magnitude - thus offering even more potential for industrial applications in realistic model-based test-scenarios. We suggest a combination of 3 techniques to achieve this goal: - We will combine HOL-TestGen with reasonably integrated and configured automated provers from the SAT solver system family, in particular Z3. - With increasing complexity, there will always remain unresolvable constraints. We will use new Isabelle code-generators to convert constraint-systems...
of unknown logical status into optimized random test code. In our experience, the success depends substantially on derived rules from the test domain that help to detect unsatisfiable test-cases early. We will explore ways to derive such forms of domain-specific simplification rules can be automated.

**HOL-TestGen XT (supplement)**

*Partners: LRI*

See ***

Financing supplement of the Chaire d’Excellence HOL-TestGen XT

**ICTSSv3**

*Partners: LRI*


Subvention of the organization of the conference ICTSS, collocated with FM.

**Paral-ITP**

*Partners: LRI (coord.), INRIA Saclay, INRIA Roquencourt*


The proposed project intends to overcome the sequential execution model for the interactive theorem proving systems Coq and Isabelle, to make the resources of multi-core hardware available for even larger proof developments. Beyond traditional processing of proof scripts as sequence of proof commands, and batchloading of theory modules, there is a large space of possibilities and challenges for pervasive parallelism. This affects many layers of each prover system: basic computational structures, inference kernel, tactical programming, proof command language, and interactive front-ends. Some of these aspects need to be addressed for Coq and Isabelle in slightly different ways, to accommodate different approaches in either system tradition. These substantial extensions of the operational aspects of interactive theorem proving shall retain the trustability of LCF-style proving at the very core. The parallelization mechanisms are of foundational importance for HOL-TestGen, a modeling and test data generation environment based on Isabelle.

**WebMov**

*Partners: LRI - Université de Paris-Sud,TSP(coord.), LaBRI - Université de Bordeaux I, Unicamp (Brésil), SOFTEAM (PME), Montimage (PME), LIMOS - Université de Clermont Ferrand 1, L3I - Université de la Rochelle*

See [http://webmov.lri.fr](http://webmov.lri.fr)

The main objective of WebMoV is to contribute to the design, composition and validation of Web Services through a high level of abstraction view and a SOA based logical architecture vision. In this domain, industry usually constructs new services by composition of modules which describe existing Web Services. These composition mechanisms are called orchestration. In this proposal, we are interested in the design and composition mechanisms for Web Services as well as their validation using different types of testing techniques.

**SysMLTests**

*Partners: Partenaires*

The contract finances the thesis "Automated Generation of Timed Tests with Isabelle and HOL-TestGen" attempts to apply "proof-based testing techniques" on concrete embedded real-time systems to be concretized by project partners. The Isabelle/HOL-TestGen-system (a plugin in Isabelle/HOL) will be used to formalize wide-spread specification languages (UML, OCL, SysML, Scade) as logical embeddings and to extend them by techniques to generate tests from models involving real-time constraints, currently used in distributed and massively parallel processors. Particular emphasis will be put on integration of visualization techniques to be integrated into the platform Isabelle/PIDE underlying HOL-TestGen.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Managing Institution</th>
<th>Start / Duration</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industriel</td>
<td>CIFRE ALL4TEC</td>
<td>CEPHYTEN</td>
<td>11.2011 / 36 mo.</td>
<td>21.99 k€</td>
</tr>
<tr>
<td>Industriel</td>
<td>Usine Logicielle</td>
<td>Université Paris XI</td>
<td>04.2006 / 24 mo.</td>
<td>107.00 k€</td>
</tr>
</tbody>
</table>

**CIFRE ALL4TEC**

*Partners: All4Tec*

See ---

Convention CIFRE: the subject of the thesis was the definition of quality criteria for models, in the context of Matelo, a test generation tool based on stochastic models. The contract was canceled in November 2013, after one year, due to the departure of the student.

**Usine Logicielle/Software Factory**

*Partners: Thales, Dassault, MBDA, Hispano-Suiza, IFP, CEA-LIST, Supelec, LIP6*


Within this big project of the Systematic "Pole de compétitivité" the LRI contributors developed with CEA-LIST a tool for statistical testing of reactive systems described in Lustre. The project lasted from 02/2006 to 02/2009.

5/ Annexe 6: Réalisations

**Software Licensing and Distribution**

**RUKIA** - Random Uniform walk in Automata


Contact: GAUDEL

**Isabelle/HOL** - Isabelle/HOL

[http://www.cl.cam.ac.uk/research/hvg/isabelle/](http://www.cl.cam.ac.uk/research/hvg/isabelle/)

Contact: WENZEL

**Le Système HOL-Z** - The HOL-Z System


Contact: WOLFF

**HOL-TestGen** - A generator of test-data from HOL specifications


Contact: WOLFF
Publications

Journal articles

Major international journals


Other journals


Invited conferences


Conference articles

Major international conferences and workshops


Other conferences and workshops


Edited books


Dissemination


Other publications


---

**Theses and habilitations**


(80) **Fatiha Zaidi**, From Active to Passive Testing. Thèse d’habilitation (HDR), Université Paris-Sud / LRI, 2010.


(85) **Paulo Salem da Silva**, Verification of behaviourist multi-agent systems by means of formally guided simulations. These, Université Paris Sud; Université de Sao Paulo, co-tutelle, nov 2011.
Shared publications

Journal articles

Major international journals


Invited conferences


Conference articles

Major international conferences and workshops


Major national conferences and workshops


Other conferences and workshops


(10) Johan Oudinet, Alain Denise, and Marie-Claude Gaudel. A new dichotomic algorithm for the uniform random generation of words in regular languages. In Conference on random and exhaustive generation of combinatorial objects (GASCom), Montreal, Canada, September 2010. 10 pages.


Other publications

Annexe 7: Thèses
## Thesis

### Habilitation à Diriger des Recherches

<table>
<thead>
<tr>
<th>Name</th>
<th>Defense</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatiha ZAIDI</td>
<td>12.2010</td>
<td></td>
</tr>
<tr>
<td>Pascal POIZAT</td>
<td>12.2011</td>
<td></td>
</tr>
</tbody>
</table>

### Defended thesis

<table>
<thead>
<tr>
<th>Name</th>
<th>Start</th>
<th>Defense</th>
<th>Funding</th>
<th>Advisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthias KRIEGER</td>
<td>01.01.2009</td>
<td>09.12.2011</td>
<td>CDD sur contrat UPS</td>
<td>WOLFF</td>
</tr>
<tr>
<td>Johan OUDINET</td>
<td>01.10.2007</td>
<td>19.11.2010</td>
<td>Alloc. Ministère</td>
<td>GAUDEL</td>
</tr>
<tr>
<td>Paulo SALEM DA SILVA</td>
<td>10.01.2009</td>
<td>28.11.2011</td>
<td>autre</td>
<td>GAUDEL</td>
</tr>
</tbody>
</table>

### Thesis in progress

<table>
<thead>
<tr>
<th>Name</th>
<th>Start</th>
<th>Funding</th>
<th>Advisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Romain AISSAT</td>
<td>01.10.2012</td>
<td>Alloc. Ministère</td>
<td>WOLFF</td>
</tr>
<tr>
<td>Rania KHEFFI</td>
<td>15.11.2011</td>
<td>CDD sur contrat UPS</td>
<td>POIZAT</td>
</tr>
<tr>
<td>Yakoub NEMOUCHI</td>
<td>01.10.2012</td>
<td>CDD sur contrat UPS</td>
<td>WOLFF</td>
</tr>
<tr>
<td>Huu Nghia NGUYEN</td>
<td>01.01.2010</td>
<td>Alloc. Ministère</td>
<td>DAGUE</td>
</tr>
<tr>
<td>Frederic TUONG</td>
<td>01.02.2013</td>
<td>autre</td>
<td>WOLFF</td>
</tr>
</tbody>
</table>