Colloque d'Automne du LIX 2007 — CAL07

Complex Industrial Systems: Modelling, Verification and Optimization

Paris, Carré des Sciences, 3rd and 4th October 2007, Amphitheatre "Stourdzé"

Workshop committee:
L. Liberti (LIX)
H. Gimbert (LIX)
E. Goubault (CEA / MeASI)
D. Krob (LIX)

Programme editor:
Leo Liberti (LIX)

1 Workshop format

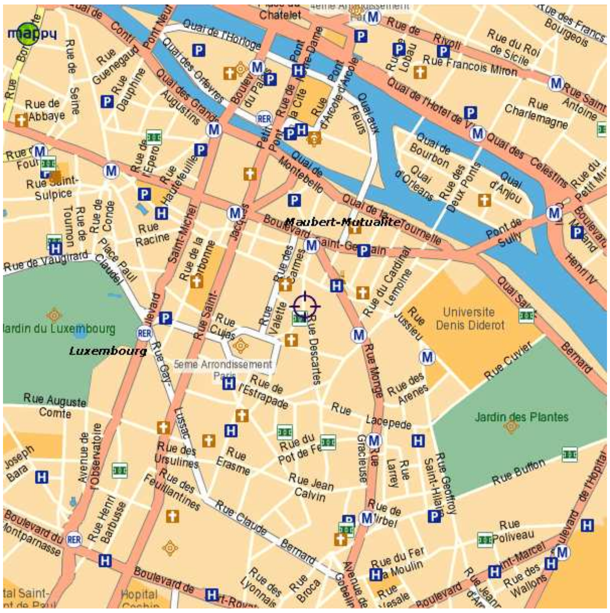
The Laboratoire d'Informatique de l'Ecole Polytechnique (LIX) organizes an international workshop on some aspects of computer science in industry in Paris (France), 3-4 oct. 2007. Three main topics discussed are discussed in the workshop, namely:

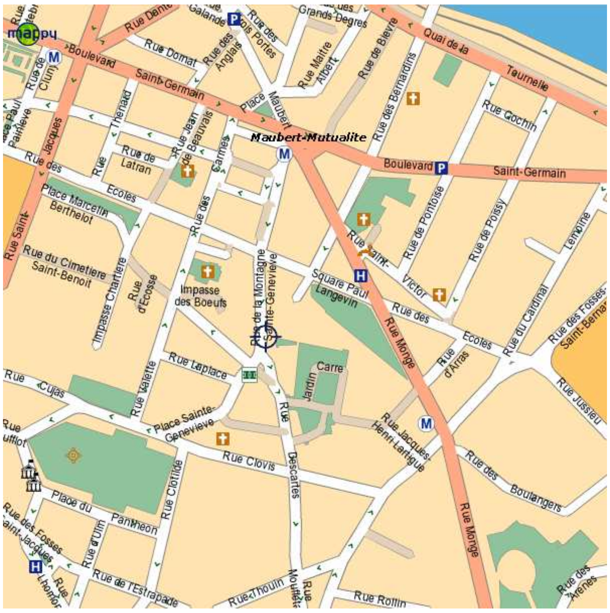
- Modelling of complex industrial systems (5 speakers, label "C")
- Optimization (5 speakers, label "O")
- Software verification (5 speakers, label "V").

Talks are by invitation only, are grouped in a single session and mainly focus on interactions among these three disciplines, each of which has a dedicated stream. Each stream includes three 45-minutes talks (labelled 1-3) given by renowned experts in the field and two 30-minutes talks (labelled 4-5) given by young researchers.

2 Arrival

The workshop takes place at the Carré des Sciences in Paris, at the old École Polytechnique site in the 5th *arrondissement*, which is now occupied by the research ministry. The ministry allocates a 70-seat lecture theatre (called "Amphitheatre Stourdzé") for this workshop. All registered participants and invited speakers will be admitted. The rest of the places will be allocated on a first-come, first-served basis up to capacity. For security reasons, under no circumstances will the 70 people capacity limit be bypassed. The address of the venue is *1, rue Descartes, 75005 Paris*, but the entrance is located at *25, rue de la Montagne Sainte Geneviève* (which is around 10-20m from the official address). A staffed welcome desk will be open for the whole length of the workshop. As the neighbourhood is literally crawling with small restaurants, bars and bistrots, no "conference lunch" is provided for.





To arrive from the Charles de Gaulle Paris airport take the RER "B" train towards Paris and get off at either (a) Luxembourg station and walk to the venue (refer to the map on the left) or (b) St. Michel-Notre Dame station, change on the "10" line towards Gare d'Austerlitz, get off at Maubert-Mutualité and then walk to the venue.

3 Speakers list

- Complex Industrial Systems
  1. *C1 3/10@0915-1000*: Y. Caseau (Bouygues Telecom)
  2. *C2 3/10@1515-1600*: C. Feliot (Alstom Transport)
  3. *C3 4/10@1400-1445*: J. Printz (CNAM, Paris)
  4. *C4 3/10@1400-1430*: H. Gimbert (LIX, Palaiseau)
  5. *C5 4/10@0930-1000*: S. Bliudze (VERIMAG, Grenoble)
- Optimization
  1. *O1 3/10@1000-1045*: P. Hansen (GERAD, Montreal)
  2. *O2 4/10@1115-1200*: O. de Weck (MIT, Cambridge)
  3. *O3 4/10@1545-1630*: G. Cornuéjols (CMU / Université de Marseille)
  4. *O4 4/10@0900-0930*: G. Nannicini (LIX / Mediamobile, Paris)
  5. *O5 3/10@1430-1500*: F. Marinelli (LIX, Palaiseau)
  6. *O6 4/10@1630-1700*: F. Messine (ENSEEIHT, Toulouse, France)
- Software Verification
  1. *V1 3/10@1115-1200*: C. Cuiller (Airbus)
  2. *V2 4/10@1000-1045*: S. Gaubert (INRIA)
  3. *V3 4/10@1500-1545*: TBA
  4. *V4 4/10@1600-1630*: O. Bouissou (CEA / MeASI)

4 Timetable

3/10	0830-0900	coffee		
	0900-0915	opening	D. Krob	
	0915-1000	C1	Y. Caseau	Self-Adaptive Middleware: a contribution towards taming the complexity of distributed information systems
	1000-1045	O1	P. Hansen	Primal-Dual Variable Neighborhood Search for the Simple Plant Location Problem
	1045-1115	coffee		
	1115-1200	V1	C. Cuiller	System validation and verification process owner
	1200-1400	lunch		
	1400-1430	C4	H. Gimbert	Systems as Dataflow Machines
	1430-1500	O5	F. Marinelli	A mathematical programming model for computing fixed points in static program analysis
	1500-1515	coffee		
	1515-1600	C2	C. Feliot	Toward a formal theory of systems
	1600-1630	V4	O. Bouissou	A Denotational Semantics for Hybrid Systems
	1630-1700	O6	F. Messine	Some Interval Branch and Bound Algorithms to solve Electro-mechanical Inverse Problems of Design
4/10	0830-0900	coffee		
	0900-0930	O4	G. Nannicini	Fast Computation of Time-dependent Shortest Paths in Large Road Networks
	0930-1000	C5	S. Bliudze	The Algebra of Connectors – Structuring Interaction in Behaviour-Interaction Priority
	1000-1045	V2	S. Gaubert	From non-linear Perron-Frobenius theory to static analysis
	1045-1115	coffee		
	1115-1200	O2	O. de Weck	Change Propagation Analysis in Complex Technical Systems
	1200-1400	lunch		
	1400-1445	C3	J. Printz	Software systems architecture — Elements to define a natural complexity measure for software systems and their architecture
	1445-1500	coffee		
	1500-1545	V3	TBA	TBA
	1545-1630	O3	G. Cornuéjols	Valid Inequalities for Mixed Integer Linear Programs
	1630-1645	closing	E. Goubault	

5 Abstracts

5.1 C5: S. Bliudze (4/10@0930-1000)

The Algebra of Connectors – Structuring Interaction in Behaviour-Interaction Priority

Simon Bliudze
VERIMAG, Grenoble, France
simon.bliudze@imag.fr

We provide an algebraic formalisation of connectors in BIP. BIP (Behaviour-Interaction-Priority) is a three-layer component based framework, whereof connectors represent the second layer, and are used to structure the interactions on typed communication ports. Types are used to describe different modes of synchronisation, notably rendezvous and broadcast.

Connectors on a set of ports P are modelled as terms of the algebra $AC(P)$, generated from P by using an binary fusion operator and a unary typing operator. Typing associates with terms (ports or connectors) synchronisation types – trigger or synchron – that determine modes of synchronisation. Broadcast interactions are initiated by triggers. Rendezvous is a maximal interaction of a connector including only synchrons.

The semantics of $AC(P)$ associates with a connector the set of its interactions. It induces on connectors an equivalence relation which is not a congruence as it is not stable under fusion. We provide a number of properties of $AC(P)$ used to symbolically simplify and handle connectors. We provide examples illustrating applications of $AC(P)$, including a general component model encompassing synchrony, methods for incremental model decomposition, and efficient implementation by using symbolic techniques

5.2 V4: O. Bouissou (3/10@1600-1630)

A Denotational Semantics for Hybrid Systems

Olivier Bouissou
CEA[1], France
olivier.bouissou@cea.fr

In this talk, I will present a model and a denotational semantics for hybrid systems made of a continuous and a discrete subsystem. This model is designed so that it may be easily used for modeling large, existing, critical embedded applications, which is a first step toward their validation. The discrete subsystem is modeled by a program written in an extension of an imperative language and the continuous subsystem is modeled by differential equations. I will give to both subsystems a denotational semantics inspired by what is usually done for the semantics of computer programs and then show how the semantics of the whole system is deduced from the semantics of its two components.

The semantics of the continuous system is computed as the fix-point of a modified Picard operator which increases the information content at each step. This fix-point is computed as the supremum of a sequence of approximations and we show that this supremum exists and is the solution of a differential equation using Keye Martin's measurement theory. The semantics of the discrete system is given as a classical denotational semantics, except that special denotations are given for the actions of sensors and/or actuators.

5.3 C1: Y. Caseau (3/10@0915-1000)

Self-Adaptive Middleware: a contribution towards taming the complexity of distributed information systems

Yves Caseau
Bouygues Telecom, France
ycaseau@bouyguestelecom.fr

Large-scale, distributed, information systems exhibit many behaviors which may be characterized as "complex systems". This paper deals with quality of service, defined from business constraints related to business processes, and how it may be preserved in complex situations. We present a set of adaptive methods and rules for routing messages in an integration infrastructure that yields

[1]Member of MeASI, Common Research Team at LIX, École Polytechnique and LIST, CEA.

a form of autonomic behavior, namely the ability to dynamically optimize the flow of messages in order to respect SLAs (Service Level Agreements) according to business priorities. EAI (Enterprise Application Integration) infrastructures may be seen as component systems that exchange asynchronous messages over an application bus, under the supervision of a processflow engine that orchestrates the messages. The QoS (Quality of Service) of the global IT system is defined and monitored with SLAs that apply to each business process. We propose routing strategies for message handling that maximize the ability of the EAI system to meet these requirements, in a self-adaptive and self-healing manner, which is the ability to cope with sudden variations of the event flow or temporary failures of a component system. These results are a first contribution to deploy autonomic computing concepts into BPM (Business Process Management) architectures. This work is a first step in the exploration of the links between "biomimetics" and information systems: how does one exploit the properties of emergence and adaptability of "live" systems to "grow" a new breed of information systems that are autonomous, resilient and adaptive to their environments.

5.4 O3: G. Cornuéjols (4/10@1545-1630)

Valid Inequalities for Mixed Integer Linear Programs

Gerard Cornuéjols

Carnegie-Mellon University, USA and LIF, Université de Marseille, France

gc0v@andrew.cmu.edu

This tutorial presents a theory of valid inequalities for mixed integer linear sets. It introduces the necessary tools from polyhedral theory and gives a geometric understanding of several classical families of valid inequalities such as lift-and-project cuts, Gomory mixed integer cuts, mixed integer rounding cuts, split cuts and intersection cuts, and it reveals the relationships between these families. The tutorial also discusses computational aspects of generating the cuts and their strength.

5.5 V1: C. Cuiller (3/10@1115-1200)

System validation and verification process owner

Claude Cuiller
Airbus, France
claude.cuiller@airbus.com

The talk is focused on aircraft embedded systems, meaning a consistent set of sensors, actuators and computers implementing an aircraft function. System validation is first taken from a complete development process. Then, companion activities are presented, such as certification. An overview of different validation means, such as test, will conclude.

L'exposé est centré sur les systèmes embarqués aéronautiques, donc un ensemble cohérent de capteurs, actionneurs et calculateurs implantant une fonction avion. La validation des systèmes est tout d'abord placée dans le contexte d'un développement complet. Les processus connexes telle que la certification sont ensuite évoqués. L'exposé se termine par un aperçu des divers moyens utilisés, tel que le test.

5.6 O2: O. de Weck (4/10@1115-1200)

Change Propagation Analysis in Complex Technical Systems

Olivier de Weck
MIT, Cambdrige, USA
deweck@mit.edu

Understanding how and why changes propagate during engineering design of complex software and hardware systems is critical because most products and systems emerge from predecessors and not through clean sheet design. This paper examines a large data set from industry including 41,500 change requests that were generated during the design of a complex sensor system spanning a period of 8 years. In particular the networks of connected parent, child and sibling changes are resolved over time and mapped to 46 subsystem areas. These networks of changes are then decomposed into 1-, 2- and 3-node motifs which are proposed as the fundamental building blocks of change activity. Furthermore, a set of indices is developed to help classify areas of the system as acceptors or reflectors of change and a normalized change propagation index (CPI) shows the relative strength of each area on the absorber-multiplier spectrum between

-1 and +1. Another interesting finding is the quantitative confirmation of the "ripple" change pattern previously proposed. Unlike the earlier prediction, however, it was found that the peak of cyclical change activity occurred late in the program driven by rework discovered during systems integration and functional testing.

5.7 C2: C. Feliot (3/10@1515-1600)

Toward a formal theory of systems

Claude Feliot
ALSTOM, St-Ouen, France
claude.feliot@transport.alstom.com

The word "system" that one, so intensively, calls on for denoting either a large variety of ideas, of concepts, and of things, or uses to qualify a method, an approach, or else a theory, rightfully leads to ask if there is, behind the term of "system", a real concept or just a vacuous or mistakenly used word. However, if we admit the term "system" as denotation of a way of thinking or as a problem solving approach, a system theory is nothing else but a modelling theory, as far as reasoning rests on more or less abstract representation of reality. Therefore, as a modelling theory, such a system theory requires that three components: semantic, syntactic and pragmatic aspects of this modelling approach are investigated and formally defined. In this presentation we will present *ProSE* (Proved System Engineering), which is the current state of our interpretation and development of the SAGACE methodology [Pen94,Fel97] into a formally defined modelling theory. The Refinement calculus [Back98] that provides the theoretical foundations of our approach leads to a system engineering approach that can be guarantied by proof and demonstrated to be sound and meaningful is a product or else software engineering perspective.

5.8 V2: S. Gaubert (4/10@1000-1045)

From non-linear Perron-Frobenius theory to static analysis

Stephane Gaubert
INRIA, Rocquencourt, France
`stephane.gaubert@inria.fr`

Static analysis by abstract interpretation leads to find the smallest fixed point of an order preserving self-map of a lattice. Important cases include lattices of intervals, lattices of "zones" (potential constraints), and more generally the lattices of "templates" (discretized support functions of polyhedra) introduced by Manna and his collaborators. For all these lattices, we eventually get a fixed point problem for an order preserving self-map of R^n. Such maps have received much attention in the nonlinear analysis community, since they can be thought of as non-linear extensions of the order preserving linear maps studied in the Perron-Frobenius or Krein-Rutman theory.

I will present some applications to static analysis of methods from non-linear Perron-Frobenius theory and game theory. Fixed points problems from static analysis are seen to be equivalent to computing the value of zero-sum stochastic games, sometimes with a somehow unphysical "negative discount rate", leading to unfamiliar situations and new difficulties from the dynamic programming point of view, like a disconnected fixed point set. This equivalence has inspired the development of fast policy iteration algorithms, combining techniques from game theory and convex programming. Policy iteration offers an alternative to the methods of acceleration of convergence traditionally used in static analysis. It often leads to a smaller fixed point, and hence to a more accurate approximation of the program behavior.

These results belong to joint works with E. Goubault, S. Putot, S. Zennou, A. Taly, and A. Assale.

5.9 C4: H. Gimbert (3/10@1400-1430)

Systems as Dataflow Machines

Hugo Gimbert
LIX, École Polytechnique
`hugooooo@gmail.com`

We develop a unified functional formalism for modelling complex systems, that is systems composed of a number of components, including software and physical devices. Continuous time is modelled as a discrete sequence by using non-standard analysis techniques.

We define systems as generalised Turing machines with temporised operation, and input and output channels. Behaviours of systems are represented by transfer functions. A transfer function is said to be implementable if it is associated with a system. This also allows to define A notion of computable functions on reals.

We show that these notions are robust: the class of implementable transfer functions is closed under abstraction and integration; the class of computable functions includes analytical functions whose coefficients are computable, and is closed under addition, multiplication, differentiation and integration. In particular, the class of computable functions includes solutions of dynamical and Hamiltonian systems defined by computable functions. Thus, our notion of system is suitable for modelling logical as well as physical systems.

5.10 O1: P. Hansen (3/10@1000-1045)

Primal-Dual Variable Neighborhood Search for the Simple Plant Location Problem

Pierre Hansen
GERAD and HEC, Montreal, Canada
pierre.hansen@gerad.ca

The variable neighborhood search metaheuristic is applied to the primal simple plant location problem and to a reduced dual obtained by exploiting the complementary slackness conditions. This leads to (i) heuristic resolution of (metric) instances with uniform fixed costs, up to $n = 15000$ users and $m = n$ potential locations for facilities with an error not exceeding 0.04%; (ii) exact solution of such instances with up to $m = n = 7000$; (iii) exact solution of instances with variable fixed costs and up to $m = n = 15000$.

5.11 O5: F. Marinelli (3/10@1430-1500)

A mathematical programming model for computing fixed points in static program analysis

Fabrizio Marinelli
LIX, École Polytechnique
marinelli@lix.polytechnique.fr

The main goal of static analysis is to discover invariant relationships between the variables of a given computer program. In practice, an invariant is an over-approximation of the sets of values that the program variables can take at each control point of the code, and can be obtained by determining a fixed point, preferably the least one in a set-theoretical inclusion lattice, of a system of (approximate) semantic equations. We formulate the determination of invariants in the abstract domain of intervals as a mathematical programming problem. We show some preliminary computational results and investigate the extension of this method to relational abstract domains.

5.12 O6: F. Messine (4/10@1630-1700)

Some Interval Branch and Bound Algorithms to solve Electro-mechanical Inverse Problems of Design

Frédéric Messine
ENSEEIHT, Toulouse, France
frederic.messine@n7.fr

In some fields of design, such as in electro-mechanic, interval Branch and Bound algorithms have shown their intrinsic interest by solving exactly some difficult global optimization problems. Since the first results, which are obtained ten years ago, a lot of extensions of analytical models and of the interval Branch and Bound algorithm have been performed including steps using a finite element methods and some heuristics. In this paper, I will present a synthesis of all my work on this subject.

5.13 O4: G. Nannicini (4/10@0900-0930)

Fast Computation of Time-dependent Shortest Paths in Large Road Networks

Giacomo Nannicini
LIX, École Polytechnique, and Mediamobile, Paris, France
giacomo.nannicini@v-trafic.com

In recent years the diffusion of GPS devices and route planners has increased the need for fast shortest paths computations on road networks with several millions of nodes. Although there are already very fast algorithms for the static graphs, the time-dependent variant has received much less attention, and is still an open challenge. We examine the main differences between the static and the time-dependent case, so to point out what makes the problem's difficulty increase, and we discuss the efficient extension of goal-directed search to the time-dependent case, as well as promising research directions.

5.14 C3: J. Printz (4/10@1400-1445)

Software systems architecture — Elements to define a natural complexity measure for software systems and their architecture.

Jacques Printz
CNAM, Paris, France
printz@cnam.fr

The seminar is devoted to the presentation of two key concepts of software engineering concerning: 1) Software system architecture, and 2) Textual measure of the complexity of the system built on the specified architecture. It is based on my two last books: Software architecture, designing simple, reliable and adaptable applications (Architecture logicielle, concevoir des applications simples, sres et adaptables, Dunod, 2007) and Software projects ecosystem, agility and discipline (Ecosystme des projets informatiques, agilit et discipline, Herms, 2006).

In a first part, it is shown how system architecture can be considered as the design of an abstract machine, with all the key elements of a real machine. The control block of the abstract machine is based of the programmed monitoring of the execution of building-blocks which are the elementary pieces of the semantic of the application. These building-blocks play the role of machine instructions which are in fact elementary transformations, mainly a translation of the input data of the building-blocks to the result output data. More precisely, building-blocks have to behave as classical ACID short transactions. Input data are checked according to the rules and constraints of the interface contracts. The translation itself is a step by step process like in a translator, with its external and internal interfaces, and intermediary languages.

In a second part, it is explained how the abstract machine instructions set, i.e. the elementary building-blocks, may be used to define two types of text whose "length/size" denotes a natural measure of what could be called textual complexity of the system. The first text is the programming text written down by the programmers, with some caution to obtain a real measure. The second one is the text of tests used to verify and validate the system, and more particularly the tests developed to integrate the system from its elementary building-blocks to the whole system. Enough tests must be written to warrant the service level agreement and quality of service required by the users of the system. Achieving hierarchical structure of the information is a key point of the organization of the abstract machine and it is shown that it determines the form of the complexity function. It is claimed that the "length/size" of these IVV tests is a natural measure of the system complexity as it is perceived by a project manager and/or a software architect. They make the complexity visible.

5.15 V3: To be announced (4/10@1500-1545)

[TBA]

6 List of registered participants

Andronick	June	Formal Methods, GEMALTO, Meudon	june.andronick@gemalto.com
Aranda	Jesus	LIX	jesus.aranda@lix.polytechnique.fr
Baptiste	Philippe	LIX	baptiste@lix.polytechnique.fr
Benoist	Thierry	BOUYGUES e-lab	
Bouissou	Olivier	CEA / MeASI	olivier.bouissou@cea.fr
Bounova	Gergana	MIT	gergana@mit.edu
Brenaut	Jean-Philippe	RENAULT	jean-philippe.brenaut@renault.com
Bricard	Herve	RENAULT	herve.bricard@renault.com
Ceselli	Alberto	Università di Milano	ceselli@dti.unimi.it
Chapoutot	Alexandre	CEA / MeASI	alexandre.chapoutot@cea.fr
Chauvet	Fabrice	Gaz de France	fchauvet@scientifique.com
Cho	SongYean	LIX	cho@lix.polytechnique.fr
D'Ambrosio	Claudia	Università di Bologna	cdambrosio@deis.unibo.it
Deluca	Dorotea	Università di Firenze	dorotea.deluca@gmail.com
Deschinkel	Karine	Université de Versailles	karine.deschinkel@prism.uvsq.fr
Dhyani	Kanika	Politecnico di Milano	dhyani@elet.polimi.it
Di Giacomo	Laura	Università di Roma La Sapienza	l.digiacomo@caspur.it
Durr	Christophe	LIX	durr@lix.polytechnique.fr
Gardi	Frédéric	BOUYGUES e-lab	fgardi@bouygues.com
Gimbert	Hugo	LIX	hugo.gimbert@lix.polytechnique.fr
Goubault	Eric	CEA / MeASI	eric.goubault@cea.fr
Gravot	David	ROSTUDEL	dgravot@noos.fr
Hirschowitz	Michel	CEA / MeASI	mh@lix.polytechnique.fr
Jeanjean	Antoine	BOUYGUES e-lab	
Jost	Vincent	INRIALPES	vincent.jost@inrialpes.fr
Jouannaud	Jean-Pierre	LIX	jouannaud@lix.polytechnique.fr
Kopetz	Radu	INRIA Nancy, LORIA, équipe Protheo	radu.kopetz@loria.fr
Krob	Daniel	LIX	daniel.krob@lix.polytechnique.fr
Lassaigne	Richard	Equipe de Logique, Paris 7	lassaign@logique.jussieu.fr
Létocart	Lucas	LIPN, Paris 13	lucas.letocart@lipn.univ-paris13.fr
Liberti	Leo	LIX	leoliberti@gmail.com
Marinelli	Fabrizio	LIX	marinelli@lix.polytechnique.fr
Messine	Frederic	ENSEEIHT, Toulouse	frederic.messine@n7.fr
Moreau	Pierre-Etienne	INRIA Nancy, LORIA, équipe Protheo	pierre-etienne.moreau@loria.fr
Moy	Yannick	France Telecom / Université Paris-Sud	yannick.moy@gmail.com
Nannicini	Giacomo	LIX	giacomo.nannicini@v-trafic.com
Nguyen	Alain	RENAULT	alain.nguyen@renault.com
Nordh	Gustav	LIX	gusno@ida.liu.se
Nucci	Francesco	Dep. of Innovation Eng., Univ. di Lecce, Italia	francesco.nucci@unile.it
Olarte	Carlos	LIX	carlos.olarte@lix.polytechnique.fr
Plateau	Marie-Christine	CNAM	mc.plateau@cnam.fr
Putot	Sylvie	CEA / MeASI	sylvie.putot@cea.fr
Rueher	Michel	ESSI, Université de Nice	rueher@essi.fr
Sadykov	Ruslan	LIX	sadykov@lix.polytechnique.fr
Sourd	Francis	LIP6	Francis.Sourd@lip6.fr
Zennou	Sarah	CEA / MeASI	zennou@lix.polytechnique.fr

Acknowledgements

We gratefully acknowledge the generous funding of the CNRS, and the administrative help of Mrs. E. Rayssac and Miss C. Bellasio.

Index

Bliudze, S., 6
Bouissou, O., 7

Caseau, Y., 7
Cornuéjols, G., 8
Cuiller, C., 9

de Weck, O., 9

Feliot, C., 10

Gaubert, S., 11
Gimbert, H., 11

Hansen, P., 12

Marinelli, F., 13
Messine, F., 13

Nannicini, G., 14

Printz, J., 14

Notes