Extended Curriculum Vitae
Research Topics and Activities

Susanne Graf — VERIMAG/CNRS

January 2015

www-verimag.imag.fr/~graf

Organisation

Chapter 1

Extended Curriculum Vitae

Address

Verimag - UMR 5104
Centre Équation
2, Avenue de Vignate
F - 38610 Gières

Tel: 04 56 52 03 52
e-mail: susanne.graf@imag.fr
web: http://www-verimag.imag.fr/~graf/

Personal Data

Date of Birth: June 6, 1958
Place of Birt: Langen (Hessen) - Germany
Nationality: German

Present Position

CNRS Senior Researcher (*Directeur de Recherche*) at Verimag

Functions

Deputy Director of Verimag (2001-2004, and since 2007)

Diploma

1982: DEA Informatique (Master), Institut National Polytechnique de Grenoble
1984: Thèse Informatique (PhD), Institut National Polytechnique de Grenoble
2008: Habilitation à diriger des Recherches (Habilitation), Université Joseph Fourier

Positions

1984 - 1985: Attaché de Recherche CNRS, IMAG
1985 - 1992: Chargé de Recherche CNRS, LGI/IMAG
1992 - 2008: Chargé de Recherche CNRS, Verimag
2008 - present: Directeur de Recherche CNRS, Verimag

1.1 Research Highlights and Impact

My research activities have always been dedicated to semantic frameworks, methods and tools allowing to improve the quality of complex distributed or reactive software systems. My main contributions to the domain may be classified as follows:

- **Topic 1**. Study of temporal logics and process algebras: Towards the end of the seventies, temporal logics have been proposed as a means for expressing requirements of reactive systems [Pnu77]. My contributions concern studies of their expressivity and their adequacy for equivalences on behaviours expressed by terms of process algebras.
  3 main publications: [18, 15, 87, 81]

- **Topic 2**. Verification of complex systems: in the late eighties, a few years after the appearance of the first model-checkers for temporal logic, we were interested in applying them to realistic case studies. In order to do so, we proposed methods allowing to increase the efficiency of these tools, in particular by providing more efficient representations of models and by algorithms for compositional minimization of models with a large degree of concurrency with respect to equivalences. In all cases, we were interested in reductions strongly preserving the validity of some set of properties.
  3 main publications: [84, 83, 82]

- **Topic 3**. Abstraction based frameworks for property preservation and methods for the computation of abstractions: more important reductions of state graphs can be obtained when giving up the constraint that reduced models must be equivalent for a notion of equivalence adequate for the set of properties of interest. In particular, we have studied abstractions preserving simulation equivalences and the relationship between these simulation-based abstractions and those obtained by abstract interpretation. We have also proposed methods for computing abstractions, for finite systems and for infinite systems using predicate abstractions.
  5 main publications: [78, 77, 14, 12, 74]

- **Topic 4**. Integration of verification in the system design process: in order to apply verification to realistic detailed design specifications, we have defined "intermediate design model representations" which allow a structure preserving mapping between user languages (with expressive concepts) and verification tools, exploiting a restricted set of structural concepts. We have defined the IF language and a tool set responding to our objective. In particular, we used IF for studying time models for modelling languages such as SDL and UML.

  And finally, in the context of the Persiform project, we propose a method and a tool aiming at a better integration between functional design flow and performance evaluation.
  5 main publications: [72, 10, 7, 56, 5]

- **Topic 5**. Verification for component-based (incremental) design frameworks: It is agreed that in order to make verification scalable to large systems, some kind of compositionality is mandatory. Languages which guarantee that component properties are preserved by composition are often claimed to provide *correctness by construction*. Nevertheless, in general only safety properties are guaranteed to be preserved, at some point some kind of progress property has to be guaranteed globally.

  We have worked on scalable methods for proving progress properties, in particular deadlock freedom and local liveness. In order to avoid the need for global verification and to allow early verification for incremental design approaches we developed a very general notion of *contract framework* that can be defined on top any component framework. And in particular, we have given sufficient condition allowing *circular reasoning*, which means that the in order to discharge the context assumption for some concrete environment one can use the the property promissed by the component. This enabled us defining a joint design and verification approach for incremental design. We have also instantiated the general theory in various ways. In the SPEEDS project we have demonstrated how such contract frameworks can be used to combine verification results obtained by tools based on different notions

of refinement.
3 main publications: [57, 39, 2]

- **Topic 6**. Distributed implementations: as a topic emerging from the previous one, we have started to look into the very interesting area of automatic generation of distributed controllers allowing to impose some global properties on a set of distributed processes by exploiting local knowledge induced by some global invariant. Solutions are often represented by a "protocol" exchanging information between local sites. We started considering a higher level of abstraction: how to transform a Petri Net and a global constraint (e.g. some priority constraint amongst transitions) into a new Petrinet satisfying some progress constraint and obtained from the initial one by eliminating/adding a minimal amount of new transitions (i.e. communication). Later we have also studied distribution protocols, how exploit knowledge to make them more efficient and and how to make easier their proof by means of knowledge. More recently we have applied a similar approach for achieving distributed monitoring.
  3 main publications: [4, 3, 1]

Impact and auto-evaluation: Among the results that I have contributed to, those obtained between 1990 and 1997 on the topic of property preserving abstractions have had the strongest impact on the research community:

The predicate abstraction method [74] developed with Hassan Saidi in the context of his thesis has been and is still used as a starting point for many abstraction methods and tools, in particular in the domain of software model-checking. A number of different heuristics – defined by different abstract property lattices – adaptation to specific theories for the description of concrete systems, usage of different approaches for discharging the constraints, and optimisation of these constraints have been proposed.

Also, the tools InVest [BL98] and CEGAR [CGJ+00] are among the first ones to propose a systematic approach for refining abstractions which are too weak to prove the property. They use spurious counter examples to automatically refine the initial set of predicates, which is indeed a bit different from the systematic strengthening proposed in our method.

The abstraction and verification tool Bebop/SLAM [BR00, BR01] implements the original method almost as is. It uses predicate abstraction to extract abstract boolean programs from C programs, and then uses model-checking and counter-example based automatic refinement if needed.

This paper has over 1400 citations and the number is still growing[1].

The framework for property preserving abstractions [78, 14] which shows the link between simulation-based abstraction and abstract interpretation and which has been obtained with Claire Loiseaux, Saddek Bensalem and Joseph Sifakis in the context of Claire's thesis is often used as a general reference, as a complement or alternative to [CGL94] which defines a more restricted setting.

This paper has almost than 450 citations.

The results on Compositional minimisation of finite state systems [82, 13] based on the use of interfaces obtained together with Bernhard Steffen and Gerald Lüttgen have been quite widely taken up. They have been implemented in several tools, in particular by (1) Antti Valmari in the *ARA tool* for visual analysis by adapting the method to a different equivalence [VKCL93, Val94], (2) by Laurent Mounier and Jean-Pierre Krimm for LOTOS specifications in Aldébaran [KM97], and later adapted for the framework of finite state machines communicating through buffers [KM00], and (3) by Frédéric Lang in the CADP tool [Lan02, Lan06]. Several proposals for improving this method have been made, in particular concerning the automatic construction of interfaces which probably still merits to be exploited in tools.

[1] The citation numbers have been obtained from google scholar and therefore somehow "optimistic"

This paper has almost 300 citations (adding the numbers obtained for the conference and the exteneded journal version).

The work on the characterization of sequential consistency and verification of a cache memory by abstraction presented in [76, 12] reaches also a score of a bit over 100 citations (adding again the numbers for the conference and the journal version). The main impact of this paper on myself is certainly the high number of papers on cache memories that I am asked to review. I believe that such a implementation oriented characterisation of sequential consistency is indeed of interest, in order to provide a generic link between the original requirement and "any" implementation. By looking again at this paper, I have noticed that the "approximate" characterization given in the paper could be quite easily improved to capture a larger number of plausible implementations.

In addition to these works with great evidence of impact, I would like to mention some other results which were either important for myself and helped me to progress, or had some impact, even if the citation numbers do not provide this evidence so clearly.

The earlier work on temporal logic and process algebras includes a few nice results, I believe, in particular the work concerning the adequacy between equivalences and logics or fragments of logics. Indeed, one of the later papers of this period, on the characterisation of Safety for Branching Time Semantics [81] is reasonably cited (80 citations). This work allowed us to progress and thus contributed to the later results, but the direct practical impact of the work on these topics has been indeed rather limited.

I believe that the work done essentially between 1999 and 2006, dealing with the more practical problem of

(1) how to achieve verification of (detailed) design models provided by engineers in practice, and

(2) how to convince designers and engineers that the methods provided by our research community are relevant for them – and not only for hardware and safety critical systems

is also of quite some relevance to the domain, even if in terms of numbers of citations, the impact of this work was for a long time weaker than expected. Today the very first papers, FM'99 [72] and in CAV'00 [70] have together a bit less than 200 citations, the improved language and tool architecture presented in [65] 140 and the extension to UML presented in [42] and [10] around 250.

We have organised this work around the intermediate representation IF and its toolset (see [72, 70] for the seminal papers, and [104] for an overview). This work has been partly influenced by the insight that the proposed method of predicate abstraction and the associated invariant verification method, based on the use of theorem provers (even used in an almost automated way as constraint solvers) can only solve a part of the problem. When starting our work on predicate abstraction, we initially intended to use constraint solvers[2] but they weren't powerful enough at that time.

We are obviously not the first ones to advocate the necessity to exploit the structure for verification. Exploitation of structure has a long tradition: to name just a few, process calculi, PetriNets, Hoare Logic, queuing networks, abstract interpretation, abstract data types, ... have been proposed as means to study structural properties of programs or systems. The problem is generally how to combine the different structures in a meaningful way. In this context, we have contributed to the verification problem of descriptions combining multiple structures rather than the composition problem. The BIP framework [GS05, BBS06, BS07] that has emerged from IF, extends and conceptualises further the ideas put into practise and experimented in IF.

The IF language includes a set of general concepts which are exploited in a consistent manner at different stages of the verification process allowing to handle designs with a heterogeneous structure by providing a smooth transition from systematic "debugging" to exhaustive verification of automatically generated abstractions exploiting the structure. We have not (yet) integrated advance abstraction techniques (besides the one based on static dependency analysis) which would be meaningful for specific contexts in which some domain specific structure can be exploited.

[2] as also suggested already a bit earlier by Wang Yi, I believe

The flexibility of the tool and the underlying language allowed us to build frontends for different modelling frameworks and design approaches (based on SDL or specific UML profiles) in which the original structure relevant for analysis is preserved. This lead to verification tools that could convince the user community of the relevance of the approach. Telelogic's ObjetGeode tool for SDL has taken over some of our proposals and tools, PragmaDev proposes IF as a verification tool for their version of SDL, the case studies carried out in OMEGA project lead to the proposal of the the SPEEDS project where the analysis will be adapted to system design. Finally, the UML frontend has been used successfully in the ASSERT project for platform level analysis, and we are negotiating a contract for commercial exploitation with ESA.

We used IF also as a vehicle for allowing users to experiment with different time concepts. The approach we followed consisted in trying them to show the usefulness of the concepts provided by timed automata by adding them on top of their usual modelling languages, rather than asking them to model their problems using just timed automata. Obviously, the second approach leads to simpler models that are easier to verify, but at the risk that the link with the design is lost.

Among my more recent results, the promissing work on the generation of distributed controllers and monitors which is mainly joint work with Sophie Quinton and Doron Peled has been generally very well published [3, 48, 4, 52] but needs to be better exploited for practical applicability. I believe that exploiting knowledge for optimising protocol, and in particular knowledge of a global specification preserved in a distributed implementation, as we envisage it in [38, 1] can be very interesting.

The work on a contract "meta theory:" [39, 95, 92] has beed hard to get accepted in our scientific community, and is still not appropriately published. We have now published the application of this meta-theory to the complex modelling framework proposed in the SPEEDS project [90, 2] which demonstrates how contracts can be used to compose heterogeneous verification results — here heterogeneity stems from verification tools being based on different notions of satisfaction, and which now can be used jointly, each tool for its particular for its particular purpose. In my opinion, this is one of the most interesting potential applications of contract theory.

1.2 Projects and interaction with industry

1.2.1 Projects

I have been involved in a number of French National, European, and industrial projects. In particular, I was the coordinator of the IST OMEGA project. I participated in the proposal definition or had the responsibility of some activity (work package) or of the coordination of the participation of the Verimag team for the European Projects R&D Delta 4 (1988-1992), LTR REACT (1993-1995), LTR VIRES (1997-2000), IST INTERVAL (2000-2002) and the IP SPEEDS (2006-2011). I also had such responsibilities for the National projects RNRT PROUST (1999-2001), RNRT Persiform (2004-2007) and RNTL OpenEmBeDD (2006-2008). Finally, I have participated in the European projects Esprit-BRA SPEC (1990-1992), IST ADVANCE (2000-2003) and the IP ASSERT (2004-2008). In addition to that, I have negotiated some industry financed contracts with France Telecom, ESA and EADS.

The projects Delta-4, OMEGA, Persiform and SPEEDS are presented in some detail. At the end, a list of all projects with some factual data is provided.

IST OMEGA (2002-2005)

I was the coordinator of this European project on the *Correct Development of Real-Time Embedded Systems*.

The project aimed at the definition of a UML profile for real-time embedded systems, as well as a tool supported methodology for the development of real-time systems satisfying a set of essential requirements. A detailed description of the project results and motivations can be found in [114] and a short version in [43] or in [19], a special section of the SoSym journal with a few important project results. A special section of the STTT journal with several project results is [20]. The results developed in the project are:

- the definition of an UML profile, OMEGA-RT, adequate for the expression of requirements and (operational) design specifications of real-time embedded systems. This profile is compatible with the UML design tools used in this application domain, in particular Rhapsody. We have given a formal semantics for this profile [HKP04, AHK+04, 10, 10] allowing a consistent usage of combinations of diagrams, and we have defined real-time extension compatible with the UML standard for schedulability, performance and time[3] [64, 9]. Parts of this profile have been taken up in evolutions of the standard.
- a set of methods and tools for the verification of different aspects of systems expressed as UML models, with a special focus on coordination and timing. [HKP04, AHK+04, 63, 42, 10]. These tools are mainly existing state-of-the-art verification tools with a translation front-end and some methods tuned towards some specific properties (see also section 1.2.2)
- on four case studies provided by industrial teams, the profile has shown the usefulness of the developed tools. The different case study address quite different problems and modelling styles. Nevertheless, the motivation of all of them is to replace the purely cyclic approach to programming of embedded systems to a more flexible approach which was well covered by the profile and the tools [HKO+08, CHK08, 59, 96].

  The decision of the project to carry out the case studies by a close collaboration between the users and tool builders turned out to be particularly enriching for both parts and had a very positive impact on the tools, the methodological support, the enthusiasm of all, and last but not least for the final acceptance of the project by the reviewers.

RNRT Persiform (2004-2007)

The aim of this national project has been the development of a user level language, a methodology and a tool chain allowing to derive from functional requirements a performance model analyzable by professional performance analysis tools.

[3] which at this time was not a usable profile, but a set of very abstract domain related concepts which needed to be specialized to a usable language

I coordinated the participation of Verimag of this project that terminated with success. We have developed jointly with France Telecom R&D, a UML profile for the expression of functional requirements based on a rich subset of hierarchical activity diagrams (extended with variables end additional termination nodes) and deployment diagrams for the representation of resources and mappings of activities to resources. Performance related information is added for simplicity in the form of opaque expressions

Any legal model of this UML profile is then translated via a series of transformations to a subset of procedural colored Petri Nets, defining the semantics, and then via a general format for queuing networks into the input format of a specific tool (Hyperformix workbench) [94, 113] (see also paragraph 1.2.2). In addition, we have done some initial study showing the usability of the functional model represented by the intermediate Petri Net model [Jar07].

The tool developed corresponds to a real demand in industry, and the tool has a realistic performance. It has been further adapted for usage in the context of the development of embedded system (for Airbus) in the context of the OpenEmBeDD project. We intended to put up a project directly with Hyperformix, but they decided to take off the market this generic tool, and to build and sell such specific purpose tools as we had proposed on their own.

IP SPEEDS (2006-2011)

The preparation of this project on (*SPEculative and Exploratory Design in Systems Engineering*) has started to emerge right after the beginning of OMEGA, as we felt the need to enlarge the scope of OMEGA to obtain a real impact. The objective of SPEEDS is, as also the one of the ASSERT IP project, a new approach to the development of heterogeneous embedded systems, with a particular accent on **system modelling** and **process modelling**. Another aim is **heterogeneity** including the heterogeneity discrete/continuous, the heterogeneity of granularity and of abstraction, heterogeneity of interaction and execution.

The academic partners of the project have collaborated to define an initial version of a modelling language, structured in layers and including the necessary concepts for a component-based modelling heterogeneous designs and requirements [BCP+07]). The lowest level $L0$ represent a "synchronous" kernel language extended with continuous time and probabilities; it defines the semantics and is used directly by some of the tools based on synchronous languages. The level language $L1$ enriches the semantic format with more structural concepts needed for a structural analysis of models (e.g. the UML communication mechanisms and the BIP interaction model [BBS06, GS05]). The level $L2$ contains more user oriented concepts, considered by the tools as "syntactic sugar", but allowing the users the use of their preferred UML or SysML tools. The compatibility of tools is guaranteed by the existence of library elements mapping higher level constructs to lower level patterns. This kind of extendibility preserving the usability of tools despite the introduction of language extensions is largely ignored by standard UML approaches.

A notion of contract attaching requirements with components and subcomponents allows "handing out" subsystem specifications with all the relevant requirements concerning the subsystem and its environment.

The role of the subproject for analysis and validation, which I coordinated, wass providing a set of "analysis services", such as verification of contracts or requirements on implementations, consistency of contracts, dominance between contracts,.... These contracts can be manipulated in the process tool in order to monitor and orient the progress of the development.

The aim of Verimag, whose participation I coordinated, was the development and promotion of the ideas on the construction of component-based systems on the basis of BIP [BBS06, BS07] and on methods for structural verification as those sketched in [57, 39]

We have developed a notion of contract framework [55, 50], a design and verification methodology [93, 92] and a tool-chain (see figure 1.1).

EU Projects

- IP SPEEDS (2006-2011): `http://www.speeds.eu.com`
  Partners : coordinator: Airbus (D); users: Airbus (F), Bosch (D), Carmeq (D), EADS (D), Knorr Bremse (D), IAI (Isr), Magna Steyr (H), SAAB (S); tool builders: Esterel Technologies (F), Extessy

(D), Telelogic (Isr), TNI Software (F); academics: INRIA (F), OFFIS (D), Parades (I), Verimag (F)
Global grant : 8 Meuro
Grant for Verimag: 800 Keuro.
Topic addressed: Modelling for systems engineering (see paragraph 1.2.1)
Personal role: coordination of the subproject on Analysis and validation, coordination of the Verimag team

- STREP COMBEST (2006-2010): `http://www.combest.eu`
  Partners : coordinator: VERIMAG; users: Airbus (F), EADS (D), IAI (Isr); academics: INRIA (F), OFFIS (D), ETHZ (CH)
  Global grant : 4 Meuro
  Grant for Verimag: 300 Keuro.
  Topic addressed and personal role: Computational and Analytical models for non-functional properties of embedded systems. This project built to large extend upon results obtained in SPEEDS, and my role concerned mainly the liaison with SPEEDS.

- IP ASSERT (2004-2008) `http://www.assert-project.net/`
  In this large project, Verimag contributed methods and tools for synchronous and asynchronous languages. In particular, this project was important for the dissemination of our results obtained in OMEGA. E.g., we started to look into contract-based approaches and we adapted the OMEGA UML profile to describe a system at platform layer and used IFx (see section 1.2.2) for validation. My own role was relatively limited, I was responsible for this OMEGA related contribution.

- IST OMEGA (2002-2005) `http://www-omega.imag.fr`
  Partners : Verimag (coordination), CWI, EADS, Israeli Aircraft Industries, France Telecom R&D, U. Kiel, U. Nijmegen, NLR, OFFIS, Weizmann Institut, **Global grant** : 3 Meuro
  Grant for Verimag: 550 Keuro
  Personal role: coordination of the project and of Verimag's participation
  Topic addressed: see paragraph 1.2.1 **Personal Role**: I was the coordinator of this project

- Esprit IST INTERVAL (2000-2002): `http://www-interval.imag.fr`
  Partners : Telelogic (coordination sci.), ITM Luebeck (coordination fin.), Ericsson, France Telecom R&D, SOLINET, Teletel, Verimag
  Grant for Verimag: 500KF
  Topic addressed: A real-time profile and verification and test case generation for SDL
  Personal role: coordination and management of Verimag's participation; responsible of the WP "SDL for real-time".

- IST ADVANCE (2000 - 2003) `http://www.liafa.jussieu.fr/~haberm/ADVANCE/main.html`
  Topic addressed: verification of infinite state systems
  Personal role: participant in the WP for abstraction based methods and of state-space exploration based methods.

- Esprit LTR VIRES (1997-2000)
  Partners: TU Eindhoven (coordination), Inst. of CS of FORTH, U. Kiel, U. Liège, Verimag
  Global grant : 1 M Ecu
  Grant for Verimag: 240 K Ecu
  Topic addressed: follow-up of REACT with the aim to apply verification to software development (based on SDL). Use of the Spin model-checker and fisrst developments of the IF language and tools.
  Personal role: Responsible for Verimag, for the development of IF and the case studies.

- Esprit LTR REACT (1993-1995)
  Partners: U. Liège (coordination), Inst. of CS of Crète FORTH, U. Kiel, U. Oxford, Swedish Institute of Computer Science, Weizmann Institute, Spectre project of IMAG

Topic addressed: this was still an old times project wiht topic "do good research"
Personal role: participation in proposal writing and in the coordination of Verimag's contribution.

- Esprit-BRA SPEC (1990-1992)
  This was one of the most exciting EU projects we had. At that time a project was excellent when it had excellent collaborations and excellent papers.
  Personal role: my papers corresponding to that period.

- Esprit Delta 4 - 1 & 2 (1988-1992)
  Partners: academic and industrial partners. Our closest collaborations were with Bull, LAAS (David Powell, Toulouse), INESC (P. Verissimo, Lisbon), Fraunhofer Institute Karlsruhe and Ferranti Comp. Group Limited (Manchester).
  Topic addressed: Demonstrate the applicability of model-checker Xesar [QS82, RRSV87] to realistic case studies based on relatively detailed design specifications, in particular a fault tolerant atomic multicast protocol
  Personal role: modelling methodology, improved verification methods, analysis of the case studies, representation of Verimag in project meetings.

National Projects

- RNTL OpenEmBeDD (2006-2008): `http://openembedd.inria.fr/`
  Partners: INRIA (coordination), INRIA (6 teams), CEA, LAAS, Verimag; industrials: Airbus, Anyware, CS, FT, Leiros, PSA, Thales,
  Global grant : 2,3 Meuro
  Grant for Verimag: 170 Keuro
  Topic addressed: tool platform including generic software engineering tools and modelling and validation for embedded systems
  Personal role: coordination of the Verimag contribution and team

- RNRT Persiform (2005-2008): `http://www-persiform.imag.fr/`
  Partners : France Telecom R&D (coordination), IRISA, INT, Orpheus, Verimag
  Global grant : 500 Keuro
  Grant for Verimag: 130 Keuro
  Topic addressed: Deriving from functional requirements (in UML) performance models analyzed by professional performance analysis tools **Personal role**: coordination of Verimag's contribution, responsible of the workpackage on the semantic representation and model transformations; strong support of the coordinator

- ACI INRIA ModoCop (2002-2003)
  The topic of this small academic project was Model-checking of Concurrent Object-Orientet Programs.

- RNRT PROUST (1999-2001); `http://www-verimag.imag.fr/PROUST`
  Partners : Telelogic (coordination), France Telecom R&D, SEMA Group, Verimag
  Grant for Verimag: 1 MF
  Topic addressed: preparation of the INTERVAL project.
  Personal role: coordination and management of the local participation and workpackage on time extensions of SDL.

Industrial Projects

- FullMDE (2010-2012):
  This is another follow-up project to ASSERT financed by ESA **Partners** : coordinator: EADS;

IRIT, Verimag (Research Institues: Praxis, Esterel Technologies (Technology providers for Spark, Scade)
Grant for Verimag: 100 Keuro.
Personal role: coordination of the participation of Verimag, mainly a case study
Topic addressed: This project allowed us to integrate the new IF tool adapted to the current version of UML into a larger tool chain and to apply it to some small case study

- Porting Omega to Rhapsody (2010-2011)
  An industrial contract directly financed by the European Space Agency (ESA) **Partners** : coordinator: Verimag
  Grant for Verimag: 100 Keuro.
  Personal role: global coordination
  Topic addressed: This is a follow-up project of the ASSERT IP that allowed us to significantly the IF tool-set for UML and to update it to the current UML standard. It led also to a PhD grant of Iulian Ober in Toulouse which will be defended soon

- Cooperation Pragmadev (2006-2016)
  ThePragmadev company distributes some of the validation components of the IF tool-box (static analysis, model-checking, simulation). See `http://www.pragmadev.com`.

- Contract between VERIMAG-France Telecom R&D for the development of a tool for the execution of tests of vocal services based on IF (2005-2007)
  grant for Verimag: 100 Keuro

- Contract VERIMAG - CNET *Pro INTERVAL* (2000-2002).
  The objective of this project was to apply the SDL timing extensions defined in the INTERVAL project and the IF tool-box to a case study. Another objective was the collaboration of Verimag with France Telecom at ITU. I was the coordinator of this project,

- Contract VERIMAG-EADS (2000-2001) for the validation of the Ariane 5 flight software described in SDL and SCADE

Consulting activities

- Formal Methods for Safe and Secure Computers Systems (2011-2013)
  A formal consulting contract with BSI (Bundesanstalt für Sicherheit in der Informationstechnik, the German Federal Office for Information Security). The aim of this study on *Formal Methods for Safe and Secure Computers Systems* was to achieve a state-of-the-art account on formal methods used in academia, industry, and governmental institutions in charge of certifying information technology products, and to infer where and how formal methods can be deployed to improve over current development practices. This contract has resulted in a book [103].

1.2.2 Contributions to Design and Validation Tools

I have importantly contributed to the development of several model-checking tools representing different generations of state-of-the-art tools. Some of the tools are still maintained today, in particular the IF tool. Other tools are now outdated but their functionalities have been reimplemented in our own more recent tools or elsewhere.

XESAR, version 3.1 (1988-1990)

Xesar [RRSV87] was a reimplementation of the CESAR model-checker [QS82] meant as an industrial strength tool. It allowed the verification of requirements expressed in the temporal logic Ltac — semantically equivalent to Ctl, but developed independently using different notations and binary modalities

— on Kripke structures generated from descriptions in a rendez-vous based version of Estelle[4]. The initial version of the tool is limited to Kripke structures with 64K states and generates a Kripke structure allowing the evaluation of any state predicate definable on the initial Estelle program.

The enhancement developed in the Delta 4 project (see section 1.2.1), called version 3.1 [121], improves the efficiency considerably: (1) we propose high-level patterns for the expression of properties to improve the acceptance by the users. (2) We implement a model generation algorithm for a fixed set of a priori defined state predicates and we use on-the-fly evaluation for enhancing the performance of the tool in the debugging phase.

Impact of the tool: Using the enhanced Xesar tool together with an appropriate validation methodology, we succeeded in verifying the service properties of several variants of a fault tolerant atomic broadcast protocol [84].

The functionalities of the *Xesar* tool have been later integrated in the *Aldebaran* [Fer90] and *Caesar* [FGM+92] tools, later called CADP [FGK+96] which is still widely used and actively developed.

Abstractor and Oscar (1991-1998)

These tools have been developed in the context of the thesis of Claire Loiseaux [101, 78, 77, Loi94]. Abstractor allows, given (1) a *Boolean transition system* in the form of a union of transition relations R_i described by a set of guarded commands on boolean variables and (2) an abstraction relation given in the form of a boolean expression relating abstract and concrete boolean variables, to automatically calculate an abstract boolean transition system of the same form.

Oscar allows evaluating on such boolean transition systems properties expressed by the Ltac-extensions developed in the Delta 4 project. It applies symbolic model-checking techniques [BCM+90] based on pre-image computations. In particular, we have defined some efficient algorithms for specific property patterns.

Impact of the tool: Using this prototype, we have verified a set of safety properties of non trivial examples, in particular a token ring protocol and a non trivial toy service in the context of an automated highway, managing overtaking manoeuvres [101, 78, 77].

Oscar has not been exploited in its original form for a long period, but it is the kernel of Smi, the Symbolic model interface, an API for several BDD packages, and it is the basis on which is based the first symbolic model-checkers of IF and Cadp. This symbolic model-checker has however been relatively little used over a long period, as for the case studies we were faced with, the enumerative model-checkers turned out to be more efficient.

Invariant checker (1995-1999)

This tool has been developed in the context of Hassen Saidi's PhD thesis [75, 74, LS97, Saï97, Sai00]. It takes as inputs the same kind of descriptions as Oscar, extended to the set of types and functions that can be used in PVS.

It consists of a checker and an abstractor tool (see also at `http://www-verimag.imag.fr/~graf/INVARIANT-CHECKER/presentation.html` for a figure with the tool's functional architecture). The checker extends the BDD-based boolean symbolic model-checking technique for invariants of the form $\forall\Box p$ to unions of guarded commands describing symbolic transition systems expressible in the PVS expression language. It is based on the backwards computation of the greatest fix-point of the transition relation that is included in a state predicate. The termination condition of this algorithm is submitted as a verification condition to the theorem prover PVS [SRSS96], using as a semi-decision procedure a proof tactic combining boolean simplifications, rewriting strategies, decision procedures, inductive proofs for theorems on inductive types as well as a user definable set of auxiliary theorems which are sometimes necessary.

[4]Estelle is an extension of Pascal to describe systems of extended state machines communicating through message buffers, standardized by the International Telecommunication Union (ITU)

The ABSTRACTOR has the same functionality as the ABSTRACTOR tool coupled with OSCAR (paragraph 1.2.2) but for the richer symbolic transition systems. Abstraction mappings are given by PVS definable predicates on concrete variables that are mapped to a set of boolean variables defining the abstract domain. The tool constructs an abstraction representing a Boolean transition system. It is approximation of the exact abstract transition relation which is computed proving that certain sets of abstract states cannot be reached from certain sets of other abstract states (using similar verification conditions as those for invariant proofs).

Invariant checker uses the ABSTRACTOR to compute a good global control graph which is used as a global invariant. Alternatively, abstract boolean transition systems are analyzed using the model-checker Aldébaran integrated in CADP [FGK+96] and in IF (see paragraph 1.2.2).

Impact of the tool: We have demonstrated the usefulness of the implemented method on several case studies [LS97, Saï97, Sai00]. In particular, we have used this tool to verify a Bounded Retransmission Protocol (BRP) (see also `http://www-verimag.imag.fr/~graf/INVARIANT-CHECKER/BRP/index.html` for a more detailed description of the case study).

The method implemented by the ABSTRACTOR of the *Invariant-checker* has been taken over in many successor tools which use different representations of symbolic transition systems and differ in the heuristics used for calculating approximations of the exact abstract transition relation.

The *Invariant checker* had been maintained for many years by Hassen Saidi at SRI. Its functionalities have been implemented in the InVesT [BLO98] which then has been extended to the verification of parameterized systems in the PAX tool [BBLS00].

See also `http://www-verimag.imag.fr/~graf/INVARIANT-CHECKER/` for a more complete description of the tool and its architecture.

IF toolbox (since 1998)

IF is a language for the structured representation of concurrent real-time systems and a set of tools allowing the analysis and verification of requirements on such systems [72, 65].

The tool evolved from the CADP toolset [FGK+96]. Its development was motivated by the need for a structured representation of systems, allowing the application of simplifications — for avoiding state explosion — before its translation into a global (symbolic) transition relation. In particular, we aimed at the modelling and the verification of designs of real-time systems represented in SDL[5]. The toolset consists of:

- *Front-ends* consisting of translators from user level languages into the IF language.
- *Core components* which include several modules, each one having well defined APIs. These APIs are used by
  - Syntactic transformation tools from IF to (subsets of IF) representing semantically transformation representing abstractions or equivalences. They are based on static analysis and aim at state space reductions and at format translation for languages with less structural concepts.
  - A state space exploration engine with an API for defining arbitrary exploration strategies
  - A stats space repository used by the state space exploration engine which is based on a structured state representation and maximal sharing of substructures of states.
- *Back-end* simulation, analysis, verification and transformation engines including those implemented in CADP, the test-case generation engine TGV [FJJV96] and a set of external tools, connected either to the simulation engine or via model transformations, such as (1) SPIN [Hol99], connected via a translation defined in [BDHS00] and later in [PCDR02], (2) LASH, the Liège Automata-based Symbolic Handler [BL02], a tool for exact symbolic reachability analysis for specification with integer variables and (3) TREX [ABS01], a similar tool that handles specifications with queues.

[5] another ITU standard formal description technique

The first version of the IF tool with a front-end for SDL is presented in [72, 70, 67]. This SDL front-end uses the abstract syntax tree API of Verilog's ObjectGeode tool[6].

It allowed increasing importantly the verification capacities of ObjectGeode. We have used this SDL front-end in several case studies, including for the verification of MASCARA, an extension of ATM to wireless connections [71], and an SDL description of the flight software of the European Launcher Ariane 5 [BLM01].

A second version of IF [65] has been partly developed in the European Ist Advance project, especially the extensions for capturing dynamic systems. In this project, the connections of Lash and TreX to IF were realized.

Later we have extended the IF language with a notion of *observer* allowing an operational expression of requirements which has always been appreciated by users. We have also developed the *front-end* IFx, providing a translation of the OMEGA UML profile for real-time to IF [63, 42, 10]. IFx allows the user to use the analysis and verification engines in a partly transparent manner, as simulation traces and counter examples are presented in terms of the user's UML constructs.

This front-end has been used for all case studies within the OMEGA project, in particular a more complete model of the Ariane 5 flight software including also the cyclic behavior [59, 104] and the MARS software that counteracts the image quality degradation by creating a compensating motion of the film for high-resolution images taken from an airplane [96]. Later, it has been extended for taking account better architecture (software and physical), first in the ASSERT then in the OMEGA for Rhapsody project.

Impact of the tool:

In addition to the before mentioned case studies, the IF tool has been and is still used locally at VERIMAG in the context of a large number of research projects and thesis projects to prototype verification methods or to carry out case studies. For a more complete overview of the IF tool-set see also `http://www-if.imag.fr`.

Since its first release in 1998, the toolbox has been acquired by about 250 groups and is still used, also outside Verimag. In fact, several groups have adapted the tool to their needs. It has been transferred to Pragmadev.

The IF tool-set with the SDL front-end has been the object of several industrial research contracts and licence agreements. Presently, we are negotiating several industrial contracts for the exploitation of the IFx front-end of OMEGA as a consequence of the ASSERT project.

Persiform tool for performance analysis (2005-2008)

In the context of the Persiform project (see section 1.2.1), we have defined a tool chain allowing to derive from functional requirements expressed in an appropriate UML profile a performance model analyzable by the commercial performance analysis tool Hyperformix workbench.

Any legal model of this UML profile is translated via a series of transformations to a subset of procedural colored Petri Nets, defining the semantics, and then via a general format for queuing networks into the input format of Hyperformix workbench. In addition the tool performs some graphical layout for increasing the usability [94, 113].

Impact of the tool:

This tool correspends to a user need when a user with specific needs in terms of modelling is confronted with a generic performance modeller, the tool has a realistic performance and can be easily adapted due to the modularity of the transformation chain. It had been planned to adapt the tool for the usage in the context of the development of embedded system (for Airbus and France Telecom). We have done the adaptation for Airbus in the OPENEMBEDD project, but then the generic performance modeller on which the tool is based was taken more or less off the market

[6] which has been taken off the market shortly after

SPEEDS model transformation and verification tool box (2006 - 2011)

The SPEEDS tool box is based on quite similar ideas as already used in the IF tool, that is using a right tool interan intermediate format that allows to connecta number of analysis and and verification engines as backend tools and different user formalisms as frontend tools. The originality here was to systematically use model transformation technology to increase the maintainability in case of evolution of the user language.

As one can see in Figure 1.1, the number of transformation steps is relatively high, which is not necessarily a problem but some of the steps are critical, they lead to the explosion of the model size and are morover not really in the scope of simple model transformation technologie. For example the pattern-based constraint language CSL that the users wanted to use[7] is radically different from the HRC meta model chosen as intermediate formate. Also HRC extends components with contracts whereas Maude and BIP which we used as back-end engines are more appropriate for encoding verification problems which cannot be explicitly represented in HRC.

Impact of the tool:

Overall, we could use the tool for some small examples. In particular, we could validate our idea of composition of verification results in order to avoid semantic integration of heterogeneous specification languages and verification methods [2]. But the tool doesn't scale for somewhat realistic examples which is partly due to the fact that HRC is too low level. Wich itself is due to the requirement that it should allow semantic integration of very heterogeneous languages. Which we believe can be avoided at least at tool level. It is only needed to prove the correctness not as a "common language" in tools.

1.2.3 Contributions to standards

The experiments with the IF language and tool for modelling and verification of SDL specification of real-time systems which had been carried out in the PROUST and INTERVAL projects, have lead to a proposal for enhancing the expression of real-time properties in SDL. In collaboration with France Telecom R&D and Telelogic, this proposal has been elaborated into a proposal for an extension of a standard *SDL for Real Time* which was discussed at the ITU[8] [100, 117]. Together with Daniel Vincent from France Telecom I have been "rapporteur" for the Question of SDL for Real Time.

1.3 Teaching Activities

1.3.1 PhD students

I have fully supervised the following PhD students

- Sophie Quinton defended her PhD on "*Design, verification and implementation of systems of components*" in January 2011 (see also [51, 52, 50, 93, 55, 95, 39]) (after a postdoc with Rolf Ernst in Braunschweig she has now a position a researcher at INRIA)
- Imen Ben Hafaied defended her PhD on "*Component-based Systems: from Design to Implementation*" in February 2011 (see also [4, 5, 49, 92, 50, 53]) (today Maître Assistant at Institut Supérieur d'Informatique de Tunis)
- Manuel Aguilar *Contribution à la validation de systèmes de processus communiquant par files d'attente : analyse statique pour la réduction de files* [Agu03], 2003 (today: lecturer at Mexico university)
- Hassen Saidi, *Combinaison de Méthodes Déductives et Arithmétiques pour la Vérification* [Sai98], 1998 (today: senior researcher at SRI, Stanford)

[7] without ever understanding really its semantic
[8] International Telecommunications Union

- Claire Loiseaux, *Vérification symbolique de programmes réactifs à l'aide d'abstractions* [Loi94], 1994 (today: General Director of Trusted Labs)

In addition, I have co-supervised several PhD students in an inofficial manner. I regularly propose projects for third year students (master, DEA).

1.3.2 Courses

My position does not imply any teaching obligation. Nevertheless, I always have proposed some courses at Master level :

- "Specification of reactive systems", DEA Informatique (1988 to 1995)
- A 25 hours course for doctoral students at the Central University of Caracas (Venezuela) on "Temporal logics and model-checking" in January 1992
- "Semantics and program analysis" Maitrise Informatique (1994 to 2000)
- "Verification of Infinite state systems", DEA Informatique (1999 and 2001)
- "Model-checking of finite state systems", DEA Informatique (2003 to 2007)
- "Méthodes de Test" Master 2 in 2005 and 2007

From 2007 to 2010, I have had the responsibility for the *parcours Verification of critical systems* of the Master in computer science, common to Université Joseph Fourier and Grenoble INP, and I still teach a Master course on Verification and Testing from time to time.

1.3.3 PhD thesis and habilitation (HDR) committees

- Roland Kindermann (PhD), December 2014, University Aalto, Helsinki (opponent)
- Iuliana Dragomir (PhD), December 2014, University Toulouse
- Martin Stigge (PhD), April 2014, University of Uppsala
- Stefan Neumann (PhD), February 2014, Hasso Plattner Institute, Potsdam (rapporteur)
- Kais Klai (HdR), December 2013, Université Paris 13 (rapporteur)
- Marc Schickling (PhD), December 2012, Universität Saarbrücken (rapporteur)
- Fares Chucri (PhD), November 2012, Université Bordeaux I (rapporteur)
- Iulian Ober (HDR), December 2011, Université de Toulouse
- Frederic Mallet (HDR), November 2010, Université de Nice (rapporteur)
- Joseph Okika, June 2010, University of Aalborg (rapporteur)
- Steffen Prochnov, September 2008, Kiel University (rapporteur)
- Olivier Constant, 12 April 2006, Université de Pau et des Pays de l'Adour
- Jean-François Couchot, 6 April 2006, Université de Franche-Comté (rapporteur)
- Tong Zeng, January 2004, Concordia University at Montréal (rapporteur)
- Konsta Karsisto, February 2003, University of Tampere, Finland (rapporteur)
- Iulian Ober, 21 September 2001, Université Paul Sabatier de Toulouse.
- Brahim Mammas, September 1999, Université Pierre et Marie Cury, Paris 6 (rapporteur)
- David Cachera, January 1998, Lip at Ens de Lyon.
- Dennis Dams, July 1996, Eindhoven University (rapporteur)
- Thierry Jéron, May 1991, IRISA Rennes (rapporteur)

1.4 Animation, Dissemination and Management of Research

1.4.1 Organization of Workshops and Conferences

- 10th International Federated Conference on *Distributed Computing Techniques, DISCOTEC*, June 2015, Grenoble
  I participate at the organisation of this Federated conference and I am also PC chair of one of the conferences, FORTE.

- Workshop for celebrating the *20 years of TACAS*, April 2014 in Grenoble
  I have co-organised this workshop jointly with some members of the TACAS steering committe which took place jointly with ETAPS 2014 in Grenoble. `http://www.etaps.org/index.php/20yrsTACAS`

- Workshop for celebrating the 20 Years of the existence of Verimag in September 2012.
  Verimag was created in 1993. To celebrate its 20th anniversary, we have organised a workshop that consisted of invited talks by outstanding international scientists together with communications by Verimag researchers. We were happy to have a large number of participants. `http:www-verimag.imag.fr/20-years-of-Verimag.html`

- The International Workshop on Model Based Architecting and Construction of Embedded Systems (ACES^MB 2009)in October 2009. The objective of this workshop is to bring together researchers and practitioners interested in model-based software engineering for real-time embedded systems. We are seeking contributions relating to this subject at different levels, from modelling languages and semantics to concrete application experiments, from model analysis techniques to model-based implementation and deployment. Given the criticality of the application domain, we particularly focus on model-based approaches yielding efficient and provably correct designs. Concerning models and languages, we welcome contributions presenting novel modelling approaches as well as contributions evaluating existing ones [23]. The workshop is still organised every year but after these first edition I got less involved in actual organisation. I am still involved in the steering committe. `http://www.artist-embedded.org/artist/Overview,1706.html`

- Dagstuhl Seminar *Design and Validation of Concurrent Systems*, September 2009 in Dagstuhl, Germany. I have organised this Dagstuhl seminar together with Shaz Qadeer (Microsft reasearch), Madhusudan Parthasarathy (Illinois) and Cormac Flanagan (Santa Cruz). This seminar has gathered around 40 specialists on the topic of building correct concurrent systems and programs who enjoyed this week of lively discussions. `http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=09361`

- 1st International Workshop on Model Based Architecting and Construction of Embedded Systems (ACES^MB 2008) in October 2008. The objective of this workshop is to bring together researchers and practitioners interested in model-based software engineering for real-time embedded systems. We are seeking contributions relating to this subject at different levels, from modelling languages and semantics to concrete application experiments, from model analysis techniques to model-based implementation and deployment. Given the criticality of the application domain, we particularly focus on model-based approaches yielding efficient and provably correct designs. Concerning models and languages, we welcome contributions presenting novel modelling approaches as well as contributions evaluating existing ones [24]. `http://www.artist-embedded.org/artist/Overview,1425.html`

- Int Workshop on "*Tool Platforms for Embedded Systems Modelling, Analysis and Validation*", organised in the context of the NoE ARTIST 2 (see section 1.4.2) as a satellite event of CAV 2007 in Berlin. I have organised this workshop jointly with Kim Larsen and Jan Madsen with the objective to increase the interactions between the model-checking and the control communities. `http://www.artist-embedded.org/artist/Aims-and-Scope.html`

- International Workshop "*Towards a Systematic Approach to Embedded System Design - Bringing Leading-Edge Embedded Systems Design Tools to Industrial Users*", organised as satellite event of DATE 2007 in the context of the NoE ARTIST 2.

  I have organised this workshop jointly with Martin Torngren from KTH to allow the potential industrial users — who are well represented at DATE — to know more about the functionalities and capacities of the tools developed in academia to support the design of embedded systems. `http://www.artist-embedded.org/artist/ARTIST2-Workshop-at-Date-07.html`

- Int. workshop MARTES on "Modelling and Analysis of Real-time Embedded Systems", a satellite event of the Models/UML conferences in 2005 and 2006. In 2005 asked the organisers of the SIVOES workshop to join our forces, as SIVOES and our own predecessor SIVOES shared most of the topics and participants. See also [62, 26] or `http://www.martes.org/`

- Workshop for the presentation of the results of OMEGA (`http://www-omega.imag.fr/workshop.php`) close to the final project review. This workshop was a mixture of presentations of project results and high level invited talks of topics related the component-based approach which was one of the issues which we could only partly address in the project itself and remained still to be done.

- I have initiated the international workshop "*Specification and Validation of UML models for Real Time and Embedded Systems*" organised in 2003 and 2004 as satellite of the UML conference, jointly with Oystein Haugen (U. Oslo), Bran Selic (IBM) and my postdoc Ileana Ober.

  The main objective was the dissemination of the work of OMEGA on the integration of verification tools with UML and on the real time profile for UML. See [20, 33] or `http://www-verimag.imag.fr/EVENTS/2004/SVERTS/`

- The international Symposium on " Formal Methods for Components, Objects and their Implementation", FMCO which has taken place each year in Leiden or Amsterdam between 2002 and 2007, is an initiative of Frank de Boer (CWI), Willem-Paul de Roever (Kiel), Marcello Bonsangue (Leyden) and myself as a cooperation between our joint EU-project OMEGA and the germano-dutch MOBI-J projects. One of the main objective was to gather main contributors to the domain of component-based design in general, and of real time and distributed systems in particular. The symposium is still run today and serves as a meeting point for European projects in these domains. See also [34, 32, 30, 28, 27, 25] or `fmco.liacs.nl/fmco07.html`

- ETAPS 2002. I chaired the organisation committee of the European Joint Conferences on Theory and Practice of Software, ETAPS 2002, which drains since 1998 an almost constantly growing number of participants around five main conferences and a variable number of workshops and tutorials.

  The preparation of this event started three years ahead at ETAPS'99. The organisation committee consisted of 9 local researchers in the domain of ETAPS and a technical team of three persons. We organised 13 workshops of a duration of 1 to 3 days, 9 tutorials attended by over 600 participants from all over the world.

  Contrary to several of our predecessors, we succeeded in well involving the local and regional community by solicitating them to propose workshops and associating them with the organisation. We also succeeded to attract a number of local students by negotiating with the doctoral school that the attendance of tutorials could contribute to the student's mandatory credits.

  See also [116] and `http://www-etaps.imag.fr/`

- Int. Workshop on the "Specification and Verification of Reactive Systems" organised for the final review of the VIRES project in June 2000 by Yassine Lakhnech and myself `http://www-verimag.imag.fr/~lakhnech/vires.html`

- International workshop SaM 2000, "SDL and MSC", organized jointly with Claude Jard (IRISA) in June 2000 which takes place every second year and gathered almost 100 participants `http://www-verimag.imag.fr/~graf/SAM2000/index.html`

- Participation in the organization of the European Summer school on "Methods for the Verification of Infinite Systems" which has taken place in Grenoble in March 1997 and has gathered 120 participants.

- Participation in the organization of the franco-canadien workshop on "Communicating Informatics and Distributed Systems, new Technologies, new Requirements" organised in the context of the 7th "Entretiens du Centre Jacques Cartier" in December 1994 in Grenoble.

- Participation in the organisation of the first CAV in July 1989 in Grenoble, which was called *Workshop on Automatic Verification Methods for Finite State Systems* before becoming CAV, the *Conference on Automatic Verification*. This was a kind of foundational conference, many papers presented there are still cited today. I took there a few pictures, from which I made posters for the 20 years of CAV in 2009, and for which I get regularly requests ...

1.4.2 Animation oriented projects

ARTIST Network of excellence

I have participated in elaboration of the proposal for the European Networks of Excellence (NoE) on the design of Embedded systems coordinated by Joseph Sifakis (ARTIST 1 (2002-2004), ARTIST 2 (2004-2008) and ARTIST Design (2008-2012) — `http://www.artist-embedded.org/FP6/`).

The aim of these NoEs was the emergence of a well identified scientific community in this multidisciplinary domain requiring expertise of a large number of thematic domains around which the scientific communities are traditionally organized. This aim was more than fully achieved.

In ARTIST Design, I coordinated the Modelling Activity of the Modelling & Verification Cluster whereas Kim Larsen was responsible for the Validation activity.

In ARTIST 1 and 2, I coordinated a *Platform for Component Modelling and Verification* which had as a long term objective a better integration of the different tools proposed by the research community in the context of the design of real time and embedded systems. We achieved in particular some interesting connection to industrial standards (UML, SysML) and commercial development environments. In ARTIST 1, I have contributed to the *ARTIST roadmap* [106].

With the objective of dissemination of results, I have organized several workshops these ARTIST collaborations[9].

Animation of the research community on embedded systems at national level

Jointly with Pierre Paradinas, I had defined within the national animation project "Architecture, Système et Réseau" (GDR ASR) a proposal of a subproject on embedded systems design (ASERT 2006-2009).

The objective is building a well identified scientific community on embedded systems from the communities existing on the traditional research themes. This task turned out to be more difficult than anticipated. The reason is probably the lack of manpower and budget. Whereas the ARTIST Network of Excellence had an overall budget of several man years for the organization of the animation and coordination activities, this national initiative essentially counts on the good wills of the community. The available money allows the animation of existing communities and provides limited support to young researchers but is not attractive enough for allowing the reorganization of the community. Also both, Pierre Paradinas and myself had too many other tasks.

1.4.3 Invited seminars and conferences

More complete lists can be found in Appendix 2.

[9] as well as many others, I mention here only those in which I was personnally involved

Selection of summer schools and tutorials

- Marktoberdorf Summerschool 2010 on "Software Systems Safety — Specification and Verification", I gave a course on "Abstraction for system verification", August 2010 `https://asimod.in.tum.de/2010/index.shtml`
- Ivited Tutorial at the workshop on Automated Formal Methods AFM 2009 associated with the CAV Conference in June 2009 in Grenoble
- Tutorial at "École Jeunes Chercheurs en Programmation", Toulouse, June 2006. `http://www.irit.fr/ejcp2006/`
- Tutorial at the ARTIST Summer School *Verification of UML models with timing constraints using IF*, Naesslingen, Suede, 2005 `http://www.artist-embedded.org/artist/Programme,595.html`
- Tutorial at the Int. Doctoral School "Chambéry - Torino" in Theoretical Computer Science and in Semantic Web (12 hours), Aussois, France, June 21-25, 2004
- One day course at the TYPES Summer school on "*Theory and practice of formal proofs*", Giens, September 2-13, 2002

Selection of invited presentations and panels in international conferences

- Invited Talk at the conference ISPDC 2014 in Marseille [37] (see also `http://eriscs.luminy.univ-amu.fr/ISPDC2014-TM/bienvenue.html`)
- Invited Talk at the Workshop FSFMA, affiliated with FM 2014 in Singapore (see `http://lipn.univ-paris13.fr/fsfma2014/`)
- Invited Talk at the conference iFM 2013 [38] (see `http://www.it.abo.fi/iFM2013`), the 10th Int. Conference on integrated Formal Methods in June 2013 in Turku, Finland
- Invited Presentation at the LCCC Focus Period and Workshop on Formal Verification of Embedded Control Systems in April 2013 in Lund (see `http://www.lccc.lth.se/index.php?page=april-2013`)
- Invited Presentation at the INCOSE Industrial Day in March 2010 in Tel Aviv
- Presentation of the SPEEDS contract-based design and verification methodology at the system engineering event INCOSE 2008 in the Netherlands
- Invited Presentation of our contract-framework at the conference FDL 2008 in Stuttgart
- Int. IFIP Conference on Formal Methods for Networked and Distributed Systems Special focus on service oriented computing and architectures, FORTE 2007, June 27-29 2007, Tallinn, Estonia [39]
- Workshop QAPL 2006, Vienna in April 2006, satellite event of ETAPS.
- Panel *COTS Component-Based Embedded Systems - A Dream or Reality?*, International conference on COTS-Based Software Systems ICCBSS, Bilbao, January 2005 [41]
- Invited presentation at the EWSA 2004 European workshop on software architectures, St. Andrews (Scotland), Mai 2004 [43]
- Invited presentation at the Telelogic user conference, Paris (France), October 6, 2004
- Symposium "10 years of TACAS" with ETAPS 2004 *Modelling and Validation of real-time systems with IF*, Barcelona, March 2004
- Panel "*Time in abstract state machines*" at the workshop on Abstract State Machines, Taormina, March 2003 ... followed a few years later by a publication: [7]

1.4.4 Scientific committees and Editorial activities

Steering Committees

- Steering and organisation committee of the LCCC Focus Period and Workshop on Formal Verification of Embedded Control Systems in April 2013 in Lund, Sweden
- Co-founder and Steering Committee of the Workshop on Model-Based Architecturing and Construction of Embedded Systems ACES that takes place since 2008 every year together with the MODELS conference (see `http://emsig.embedded-systems-portal.org/index.php/hosted-events/all/2012/aces-mb-2012`)
- Steering Committee of SPIN, Int. Symposium on software model-checking, since 2003 (see `http://www.spinroot.com/spin/whatispin.html#D`).
- Co-founder and Steering Committee of FMCO, Symposium on Formal Methods for Objects and Components, from 2002 to 2007 (see `http://fmco.liacs.nl`).
- *Member of Board* of the European Association of Software Science and Technology (EASST) since 2002 (see `http://easst.net`).
- Steering Committee of ETAPS (European joint conferences on Theory and Practice of Software) between 1999 and 2003 (see `http://www.etaps.org`)

PC chairs

- FORTE 2015, 35th IFIP Int. Conference on Formal Techniques for Distributed Objects, Components and Systems that will take in June 2015 in Grenoble.
- ATVA 2006, 4th Int. Symposium on Automated Technology for Verification and Analysis, October 2006 in Beijing, China (jointly with Wenhui Zhang) [29]
- Int. Symposium on software model-checking, SPIN, in 2004 (jointly with Laurent Mounier) [31]
- TACAS, *Tools and Algorithms for the Construction and Analysis of Systems*, 2000 (jointly with Michael Schwartzbach) [35]

Editorial Activities

- Editorial Board of Springers Journal STTT (Software Tools for Technology Transfer).
- Editorial activities bound to the activity as a program committee chair of a conference with published proceedings (see above)
- Editor of a *special section* on the OMEGA project in Springer's SoSyM journal [19]
- Editor of a *special section* as a follow-up of the organization of the SVERTS workshop in Springer's STTT journal [20]
- Editor of a *special section* on the 2000 Edition of TACAS in Springer's STTT journal [21]

Program Committees

I am regularly solicited to participate in programme committees of scientific conferences and workshops. In particular, I have participated regularly in the PC of important conference of my domain, such as CAV, TACAS, CONCUR, SAS, FMCAD, FM, Models/UML, VMCAI, RV, CBSE ...

Overall, I have participated in program committees of over 50 international conferences and over 40 international workshops, where the satellite events of important conferences or other initiatives which I liked and wanted to support through my PC-participation. A more exhaustive list can be found in Appendix 1or on my web page.

Reviews for scientific journals

Too regularly, I am asked to write reviews for articles submitted to the following journals (non exhaustive): Theoretical Computer Science (TCS), Formal Methods in System Design, Formal Aspects of Computation, Journal on Software Tools and Technology Transfer (STTT), Journal on Software and System Modelling (SoSyM), ACM Transactions on Software Engineering and Methodology (TOSEM), Journal of Communication Networks, TSI, TSE, SCP, Distributed Computing et TOPLAS.

1.4.5 Management of Research

Local Responsibilities

From 2001 to 2005, and since 2007 I have been the Deputy Director of VERIMAG. In this context, I have managed the administrative and technical team.

I have always been strongly involved in the management of the research related activities of VERIMAG. I have been participating in the "conseil du laboratoire" since its existence. I have taken care of the website and played the role of the editor of the periodic activity reports for many years.

I am member of the scientific board of the Department of Mathematics and Informatics of Université Joseph Fourier.

I have been managing the CADP group of Verimag for 2 years before taking the responsibility as deputy director, which has then become the present group on Distributed and Complex Systems (DCS). In the context of the different research projects, I have managed the activities of small teams consisting of permanent researchers, postdocs or research engineers and doctoral students.

National level

My involvement at the national level may be considered as not very strong, indeed most of my activities are rather internationally oriented.

I have been a member of the selection committee for a Project Call of the Excellence lab *Sorbonne Paris Centre* (2013, 2014, 2015).

In 2007/08, I led an expert group on embedded systems on the account of CNRS.

On a very regular basis, I am involved as an expert in the evaluation of project proposals submitted to the programs RNTR, RNTL, ANR, ... and I am also often involved in evaluation activities for the national evaluation agency AERES (e.g. the AERES evaluation of IRIT in 2009 and INRIA Sophia Antipolis in 2011) and in committees for the recruitment of lecturers, professors and researchers at french universities and INRIA.

International level

Member of the Project Committee of the Swedish Research Council in 2013 and 2014.

From 2010 to 2013, I have been a reviewer of the European STREP project CONNECT for the overall duration of the project. I have also been involved in the final evaluation for several other projects and short-term actions.

Evaluation of project proposals submitted to the Excellence Initiative of the German DFG[10] where each financed project gets a budget of around 30 Meuro over 5 years, and each accepted "doctoral school" project a budget of around 5 Meuro over 5 years (2006, 2007 and 2011).

Member of the evaluation committee for the Norvegian excellence programme VERDIKT *ICT-knowledge for innovation and electronic co-operation in the networked society* (2005)

Evaluation of many research grants every year: NWO grants (The Netherlands), Great Britain (promotions), SNF grants (Switzerland), Canada (promotion), DFG grants (Germany), ISF (Israel), Austrian FWF, ...

Member of hiring and promotion committees in Great Britain (2008), Denmark (2008), Switzerland (2010,2011), Germany (2015) and Sweden (2009,2010, 2011, 2012, 2013, 2015)

[10] Deutsche Forschungsgemeinschaft

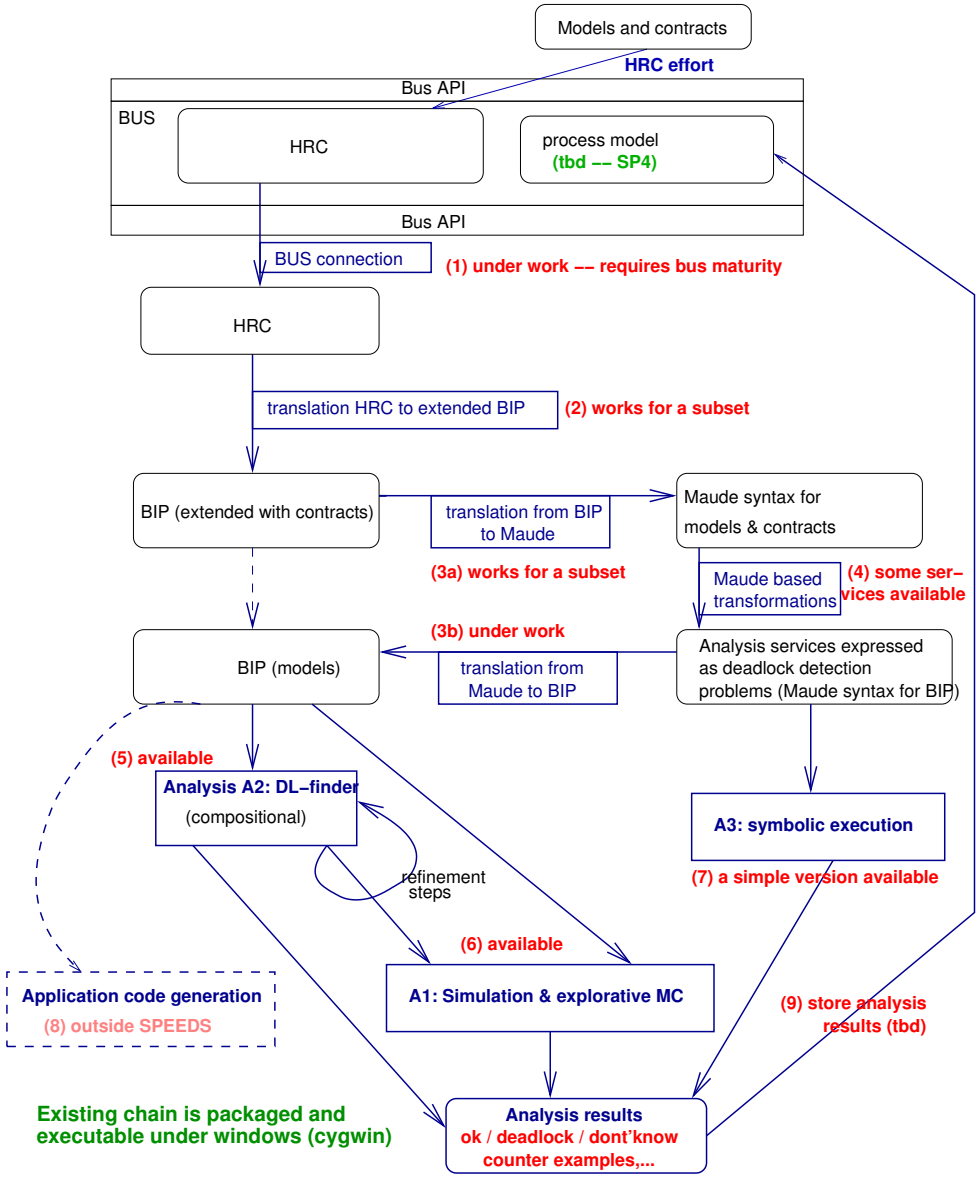

Figure 1.1: Tool chain developed in SPEEDS

1.5 External References

[ABS01] Aurore Annichini, Ahmed Bouajjani, and Mihaela Sighireanu. TReX: A tool for reachability analysis of complex systems. In *Computer Aided Verification, 13th International Conference, CAV 2001, Paris*, volume 2102 of *Lecture Notes in Computer Science*, pages 368–372, 2001.

[Agu03] Manuel Aguilar. *Contribution à la validation de systèmes de processus communiquant par files d'attente : analyse statique pour la réduction de files*. PhD thesis, Institut Polytechnique de Grenoble, December 2003.

[AHK+04] T. Arons, J. Hooman, H. Kugler, A. Pnueli, and M. van der Zwaag. Deductive verification of UML models in TLPVS. In *Proceedings UML 2004*, pages 335–349. LNCS 3273, Springer-Verlag, 2004.

[BBLS00] Kai Baukus, Saddek Bensalem, Yassine Lakhnech, and Karsten Stahl. Abstracting ws1s systems to verify parameterized networks. In *Tools and Algorithms for Construction and Analysis of Systems, 6th International Conference, TACAS 2000, Held as Part of the European Joint Conferences on the Theory and Practice of Software, ETAPS 2000, Berlin*, volume 1785 of *Lecture Notes in Computer Science*, pages 188–203, 2000.

[BBS06] A. Basu, M. Bozga, and J. Sifakis. Modeling heterogeneous real-time systems in BIP. In *4th IEEE International Conference on Software Engineering and Formal Methods (SEFM06), Invited talk, September 11-15, 2006, Pune, pp 3-12*, 2006.

[BCM+90] J.R. Burch, E.M. Clarke, K.L. McMillan, D.L. Dill, and J. Hwang. Symbolic model checking: 10^{20} states and beyond. In *Intl Conf. on Logic in Computer Science, Philadelphia*, pages 428–439. IEEE Computer Society, 1990.

[BCP+07] Albert Benveniste, Benoit Caillaud, Roberto Passerone, Eric Badouel, Bernhard Josko, and al. Heterogeneous Rich Component definition: HRC behavioural core, mathematical semantics. Speeds project deliverable d2.1.a, December 2007.

[BDHS00] Dragan Bosnacki, Dennis Dams, Leszek Holenderski, and Natalia Sidorova. Model checking sdl with spin. In Susanne Graf and Michael I. Schwartzbach, editors, *TACAS, Tools and Algorithms for Construction and Analysis of Systems, 6th International Conference, Berlin*, volume 1785 of *Lecture Notes in Computer Science*, pages 363–377. Springer, 2000.

[BL98] S. Bensalem and Y. Lakhnech. Automatic generation of invariants. *Formal Methods in System Design*, 1998. To appear.

[BL02] B. Boigelot and L. Latour. The Liege Automata-based Symbolic Handler LASH. http://www.montefiore.ulg.ac.be/ boigelot/research/lash, 2002.

[BLM01] M. Bozga, D. Lesens, and L. Mounier. Model-checking Ariane-5 flight program. In *Proceedings of FMICS'01 (Paris, France)*, pages 211–227, 2001.

[BLO98] S. Bensalem, Y. Lakhnech, and S. Owre. Invest : A tool for the verification of invariants. In *Accepted in CAV'98*, 1998.

[BR00] Thomas Ball and Sriram K. Rajamani. Bebop: A symbolic model checker for boolean programs. In *Model Checking and Software Verification, 7th International SPIN Workshop, Stanford, CA*, volume 1885 of *Lecture Notes in Computer Science*, pages 113–130, 2000.

[BR01] Thomas Ball and Sriram K. Rajamani. The slam toolkit. In *Computer Aided Verification, 13th International Conference, CAV 2001, Paris, France, July 18-22, 2001, Proceedings*, volume 2102 of *Lecture Notes in Computer Science*, pages 260–264, 2001.

[BS07] Simon Bliudze and Joseph Sifakis. The algebra of connectors — structuring interaction in BIP. In *Emsoft '07, Oct. 1-3, 2007, Salzburg, Austria*, LNCS, pages 11–20, 2007.

[CGJ+00] Edmund M. Clarke, Orna Grumberg, Somesh Jha, Yuan Lu, and Helmut Veith. Counterexample-guided abstraction refinement. In *Computer Aided Verification*, LNCS 1855, pages 154–169, 2000.

[CGL94] E.M. Clarke, O. Grumberg, and D.E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, September 1994.

[CHK08] Pierre Combes, David Harel, and Hillel Kugler. Modeling and verication of a telecommunication application using live sequence charts and the play-engine tool. *SoSyM, Software and Systems Modeling*, this issue, 2008.

[Fer90] J.C. Fernandez. An implementation of an efficient algorithm for bisimulation equivalence. *Science of Computer Programming*, 13(2-3), May 1990.

[FGK+96] Jean-Claude Fernandez, Hubert Garavel, Alain Kerbrat, Radu Mateescu, Laurent Mounier, and Mihaela Sighireanu. CADP (CÆSAR/ALDEBARAN Development Package): A protocol validation and verification toolbox. In Rajeev Alur and Thomas A. Henzinger, editors, *Proceedings of the 8th Conference on Computer-Aided Verification (New Brunswick, New Jersey, USA)*, volume 1102 of *LNCS*, pages 437–440. Springer Verlag, August 1996.

[FGM+92] Jean-Claude Fernandez, Hubert Garavel, Laurent Mounier, Anne Rasse, C. Rodriguez, and Joseph Sifakis. A tool box for the verification of Lotos programs. In *14th International Conference on Software Engineering, ICSE, Melbourne*, May 1992.

[FJJV96] Jean-Claude Fernandez, Claude Jard, Thierry Jéron, and César Viho. Using on-the-fly verification techniques for the generation of test suites. In Rajeev Alur and Thomas A. Henzinger, editors, *Computer Aided Verification, 8th International Conference, CAV '96, New Brunswick, NJ, USA, July 31 - August 3, 1996, Proceedings*, volume 1102 of *Lecture Notes in Computer Science*, pages 348–359. Springer, 1996.

[GS05] G. Goessler and J. Sifakis. Composition for component-based modeling. *Science of Computer Programming*, pages 161–183, March 2005.

[HKO+08] Jozef Hooman, Hillel Kugler, Iulian Ober, Angelika Votintseva, and Yuri Yushtein. Supporting UML-based development of embedded systems by formal techniques. *SoSyM, Software and Systems Modeling*, this issue, 2008.

[HKP04] David Harel, Hillel Kugler, and Amir Pnueli. Smart playharelkp04-out extended: Time and forbidden elements. In *4th International Conference on Quality Software (QSIC 2004), 8-10 September 2004, Braunschweig, Germany*, pages 2–10. IEEE Computer Society, 2004.

[Hol99] G. J. Holzmann. The model-checker SPIN. *IEEE Trans. on Software Engineering*, 23(5), 1999.

[Jar07] Claude Jard. Transformation from colred petrinets to spin. Deliverable of the persiform project, IRISA, 2007.

[KM97] Jean-Pierre Krimm and Laurent Mounier. Compositional state space generation from Lotos programs. In Ed Brinksma, editor, *Proceedings of TACAS'97, Enschede, The Netherlands*, LNCS 1217. Springer Verlag, 1997.

[KM00] J.P. Krimm and L. Mounier. Compositional State Space Generation with Partial Order Reductions for Asynchronous Communicating Systems. In S. Graf and M. Schwartzbach, editors, *Proceedings of TACAS'2000 (Berlin, Germany)*, volume 1785 of *LNCS*, pages 266–282. Springer, March 2000.

[Lan02] Frédéric Lang. Compositional verification using svl scripts. In *Tools and Algorithms for the Construction and Analysis of Systems, 8th International Conference, TACAS 2002, Held as Part of the Joint European Conference on Theory and Practice of Software, ETAPS 2002, Grenoble, France, April 8-12, 2002, Proceedings*, volume 2280 of *Lecture Notes in Computer Science*, pages 465–469, 2002.

[Lan06] Frédéric Lang. Refined interfaces for compositional verification. In *Formal Techniques for Networked and Distributed Systems - FORTE 2006, 26th IFIP WG 6.1 International Conference, Paris, France, September 26-29, 2006*, volume 4229 of *Lecture Notes in Computer Science*, pages 159–174, 2006.

[Loi94] C. Loiseaux. *Vérification symbolique de programmes réactifs à l'aide d'abstractions.* PhD thesis, Université Joseph Fourier, Grenoble, February 1994.

[LS97] David Lesens and Hassen Saïdi. Automatic verification of parameterized networks of processes by abstraction. In *Proceedings of the 2nd International Workshop on the Verification of Infinite State Systems (INFINITY'97, Bologna, Italy)*, July 1997.

[PCDR02] Armelle Prigent, Franck Cassez, Philippe Dhaussy, and Olivier Roux. Extending the translation from sdl to promela. In *SPIN, Model Checking of Software, 9th International SPIN Workshop, Grenoble*, volume 2318 of *Lecture Notes in Computer Science*, pages 79–94, 2002.

[Pnu77] A. Pnueli. The Temporal Logic of Programs. In *18th Symposium on Foundations of Computer Science (FOCS 77)*. IEEE, 1977. Revised version published in Theoretical Computer Science, 13:45–60, 1981.

[QS82] J-P. Queille and J. Sifakis. Specification and verification of concurrent systems is cesar. In *International Symposium on Programming, LNCS 137*, pages 337 – 351. Springer Verlag, 1982.

[RRSV87] J.L. Richier, C. Rodriguez, J. Sifakis, and J. Voiron. Verification in Xesar of the sliding window protocol. In *Int. Symp. Protocol Specification Testing and Validation*, may 1987.

[Saï97] Hassen Saïdi. The invariant checker: Automated deductive verification of reactive systems. In *Computer Aided Verification, 9th International Conference, CAV '97, Haifa, Israel, June 22-25, 1997, Proceedings*, volume 1254 of *Lecture Notes in Computer Science*, pages 436–439, 1997.

[Sai98] Hassen Saidi. *Combinaison de Méthodes Déductives et Arithméthiques pour la Vérification*. PhD thesis, Université Joseph Fourier, Grenoble I, January 1998.

[Sai00] Hassen Saidi. Model checking guided abstraction and analysis. In Jens Palsberg, editor, *7th International Static Analysis Symposium (SAS'00), Santa Barbara*, volume 1824 of *Lecture Notes in Computer Science*, pages 377–339. Springer-Verlag, July 2000.

[SRSS96] S.Owre, J. Rushby, N. Shankar, and M. Srivas. PVS: Combining specification, proof checking and model-checking. In *CAV'96*, volume 1102 of *LNCS*, 1196.

[Val94] Antti Valmari. Compositional analysis with place-bordered subnets. In *Application and Theory of Petri Nets 1994, 15th International Conference, Zaragoza, Spain, June 20-24, 1994, Proceedings*, volume 815 of *Lecture Notes in Computer Science*, pages 531–547, 1994.

[VKCL93] Antti Valmari, Jukka Kemppainen, Matthew Clegg, and Mikko Levanto. Putting advanced reachability analysis techniques together: the "ara" tool. In *FME '93: Industrial-Strength Formal Methods, First International Symposium of Formal Methods Europe, Odense, Denmark, April 19-23, 1993, Proceedings*, volume 670 of *Lecture Notes in Computer Science*, pages 597–616, 1993.

Chapter 2

List of Publications

2.1 Journal articles

[1] S. Graf, S. Quinton, "Knowledge-based Construction of Distributed Constrained Systems", *SoSyM, int. Journal on Software & Systems Modelling* , en attente de publication 2015.

[2] S. Graf, R. Passerone, S. Quinton, "Contract-Based Reasoning for Component Systems with Complex Interactions", To be published in *SoSyM, int. Journal on Software & Systems Modelling* , 2014.

[3] S. Graf, D. Peled, S. Quinton, "Achieving distributed control through model checking", *Formal Methods in System Design 40*, 2, 2012, p. 263–281.

[4] I. Ben-Hafaiedh, S. Graf, S. Quinton, "Building Distributed Controllers for Systems with Priorities", *Journal of Logic and Algebraic Programming*, 3, 2011, p. 194–218.

[5] R. Passerone, I. Ben-Hafaiedh, S. Graf, A. Benveniste, D. Cancila, A. Cuccuru, S. Gérard, F. Terrier, W. Damm, A. Ferrari, L. Mangeruca, B. Josko, T. Peikenkamp, A. L. Sangiovanni-Vincentelli, "Meta-models in Europe: Languages, Tools and Applications", *IEEE Design & Test of Computers 26*, 3, 2009, p. 38–53.

[6] I. Ober, S. Graf, Y. Yushtein, I. Ober, "Timing analysis and validation with UML: the case of the embedded MARS bus manager", *Innovations in Systems and Software Engineering 4*, 3, septembre 2008, or here: http://www-verimag.imag.fr/ graf/PAPERS/GrafOberYushtein-STTT08.pdf.

[7] S. Graf, A. Prinz, "Time in Abstract State Machines", *Fundamentae Informaticae, Special issue on ASM 2005 77* 1-2, 2007.

[8] S. Graf, I. Ober, "Software and architecture modelling with Omega-UML and validation with IF", *Génie Logiciel 1*, 80, 2007, p. 21–26.

[9] S. Graf, I. Ober, I. Ober, "Timed annotations in UML", *STTT, Software Tools for Technology Transfer 8*, 2, 2006,

[10] S. Graf, I. Ober, I. Ober, "Validating Timed UML models by simulation and verification", *STTT, Software Tools for Technology Transfer 8*, 2, 2006,

[11] I. Ober, S. Graf, I. Ober, D. Lesens, "Un profil UML et un outil pour la modélisation et la validation de systèmes temps-réel", *Numéro spécial du journal Génie Logiciel consacré à la Journée NEPTUNE 05 : Ingénierie des Modèles - vérification de modèles 73*, 2005, p. 33–38.

[12] S. Graf, "Characterization of a sequentially consistent memory and verification of a cache memory by abstraction", *Distributed Computing 12*, 1999,

[13] S. Graf, G. Lüttgen, B. Steffen, "Compositional Minimisation of Finite State Systems using Interface Specifications", *Formal Aspects of Computation 8*, 1996.

[14] C. Loiseaux, S. Graf, S. Bensalem, A. Bouajjani, J. Sifakis, "Property Preserving Abstractions for the Verification of Concurrent Systems", *Formal Methods in System Design, Vol 6, Iss 1, January 1995*, 1995.

[15] S. Graf, J. Sifakis, "A Logic for the Description of non Deterministic Programs and their Properties", *Information and Control 68*, 1986.

[16] S. Graf, J. Sifakis, "A Modal Characterization of Observational Congruence on Finite Terms of CCS", *Information and Control 68*, 1986.

[17] S. Graf, J. Sifakis, "A logic for the specification and proof of regular controllable processes of CCS", *Acta Informatica 23*, 1986.

[18] S. Graf, "On Lamport's comparison between linear and branching time logic", *RAIRO Informatique Théorique 18*, 4, 1984.

2.2 Introductions to special sections (editor and author of an introduction article)

[19] S. Graf, "Omega – Correct development of Real Time Embedded Systems", *SoSyM, int. Journal on Software & Systems Modelling 7*, 2 (under press), (4 pages) 2008.

[20] S. Graf, I. Ober, O. Haugen, B. Selic, "Specification and Validation of Models of Real Time and Embedded Systems in UML", *STTT, Software Tools for Technology Transfer, a special issue on the SVERTS 2003 workshop 8*, Vol 2, avril 2006, http://www-verimag.imag.fr/ graf/PAPERS/GHOS-Sverts03-05.pdf.

[21] S. Graf, "Introduction to Tools and Algorithms for the Construction and Analysis of Systems: An STTT special section", *STTT, Software Tools for Technology Transfer vol. 4, n. 2*, (3 pages) 2003.

2.3 Conference Proceedings (editor)

[22] I. Ober, F. Noyrit, S. Graf, G. Karsai (Eds.), Proceedings of the 6th Intl Workshop *ACES^{MB} Model Based Architecting and Constructing of Embedded Systems* co-located w ACM/IEEE Conf MODELS 2013, Miami, Sept. 29 2013.

[23] S. Van Baelen, I. Ober, S. Graf, M. Filali, T. Weigert (Eds.), *ACES^{MB} 2009 Second International Workshop on Model Based Architecting and Constructing of Embedded Systems, Toulouse, 29/09/2008*, IRIT Press, September 2009.

[24] S. Van Baelen, I. Ober, S. Graf, M. Filali, T. Weigert (Eds.), *ACESMB 2008 First International Workshop on Model Based Architecting and Constructing of Embedded Systems, Toulouse, 29/09/2008 - 29/09/2008*, IRIT Press, September 2008.

[25] F. De Boer, M. Bonsangue, S. Graf, W.-P. De Roever (Eds.), *6th Symposium on Formal Methods for Components and Objects, October 24-26, 2007, Revised Lectures*, *Lecture Notes in Computer Science*, *5382*, 2008.

[26] S. Graf, S. Gérard, O. Haugen, I. Ober, B. Selic, "MARTES - Modelling and Analysis of Real Time and Embedded Systems Using UML", *en: MoDELS 2006 International Workshops, Doctoral Symposium, Educators Symposium; Genoa, October 2006, Revised Selected Papers*, *LNCS*, *4364*, 2006.

[27] F. De Boer, M. Bonsangue, S. Graf, W.-P. De Roever (Eds.), *5th Symposium on Formal Methods for Components and Objects, November 7-10, 2006, Revised Lectures*, *Lecture Notes in Computer Science*, *4709*, 2007.

[28] F. de Boer, M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *4th Symposium on Formal Methods for Components and Objects, revised lectures*, *LNCS State-of-the-art surveys*, *4111*, 2006.

[29] S. Graf, W. Zhang (Eds.), *Automated Technology for Verification and Analysis, 4th International Symposium, ATVA 2006, Beijing, China, October 23-26, 2006. Proceedings*, *LNCS*, *4218*, 2006.

[30] F. de Boer, M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *3rd Symposium on Formal Methods for Components and Objects, revised lectures*, *LNCS Tutorials*, *3657*, 2005.

[31] S. Graf, L. Mounier (Eds.), *11th International SPIN Workshop on Model Checking of Software, 2004*, *Lecture Notes in Computer Science*, *LNCS 2989*, 2004.

[32] F. de Boer, M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *2nd Symposium on Formal Methods for Components and Objects, revised lectures*, *LNCS Tutorials*, *3188*, 2004.

[33] S. Graf, O. Haugen, I. Ober, B. Selic (Eds.), "SVERTS - Specification and Validation of Real-time and Embedded Systems, workshop overview", *Workshops with UML 2004, Overviews and selected publications, LNCS 3297*, 2004.

[34] F. de Boer, M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *1st Symposium on Formal Methods for Components and Objects, revised lectures*, *LNCS Tutorials*, *2852*, 2003.

[35] S. Graf, M. Schwartzbach (Eds.), *Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS2000*, *LNCS*, *1785*, March 2000.

[36] S. Graf, C. Jard (Eds.), *SDL and MSC Workshop SAM 2000*, *IMAG Research report series*, June 2000.

2.4 Invited Papers

[37] S. Graf, "Distributed Implementation of Constrained Systems based on Knowledge", *IEEE 13th Int. Symposium on Parallel and Distributed Computing, ISPDC 2014, Marseille*, 2014.

[38] S. Graf, S. Quinton, "Deriving distributed implementation from global specifications", *iFM 2013, Turku* 2013.

[39] S. Graf, S. Quinton, "Contracts for BIP: hierarchical interaction models for compositional verification", *FORTE 2007, Talinn*, *LNCS*, *4574*, 2007.

[40] G. Gössler, S. Graf, M. Majster-Cederbaum, M. Martens, J. Sifakis, "Ensuring Properties of Interaction Systems by Construction", *Program Analysis and Compilation, Theory and Practice*, *LNCS*, 4444, 2006.

[41] I. Crnkovic, J. Axelsson, S. Graf, M. Larsson, R. C. van Ommering, K. C. Wallnau, "COTS Component-Based Embedded Systems - A Dream or Reality?", *ICCBSS 2005, Bilbao, 2005*, 2005. LNCS Volume 3412.

[42] M. Bozga, S. Graf, I. Ober, I. Ober, J. Sifakis, "The IF toolset", *4th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Real Time, SFM-04:RT, Bologna, Sept. 2004*, *LNCS Tutorials, Springer*, 3185, 2004.

[43] S. Graf, J. Hooman, "Correct Development of Embedded Systems", *European Workshop on Software Architecture: Languages, Styles, Models, Tools, and Applications (EWSA 2004), co-located with ICSE 2004, St Andrews, Scotland*, *LNCS 3047*, 2004.

[44] S. Bensalem, S. Graf, Y. Lakhnech, "Abstraction as the Key for Invariant Verification", *Int. Symposium on Verification celebrating Zohar Manna's 64th Birthday*, LNCS 2772, 2003.

[45] A. Bouajjani, S. Graf, J. Sifakis, "A Logic for the description of Behaviours and Properties of Concurrent Systems", *Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency, School/Workshop, Noordwijkerhout*, *LNCS*, *354*, May 1988.

2.5 Publications in formal proceedings of conferences

[46] E. Conquet, F. Dormoy, I. Dragomir, S. Graf, D. Lesens, P. Nienaltowski, I. Ober, "Formal Model Driven Engineering for Space Onboard Software" *en : International Congress on Embedded Real Time Software and Systems (ERTS2, Toulouse)*, *French Society for Electricity, Electronics, and Information and Communication Technologies*, 2012.

[47] I. B. Hafaiedh, S. Graf, N. Mazouz, "Distributed Implementation of Systems with Multiparty Interactions and Priorities", *en : Software Engineering and Formal Methods - 9th International Conference, SEFM 2011, Montevideo, Uruguay, November 14-18, 2011. Proceedings*, G. Barthe, A. Pardo, G. Schneider (réd.), *Lecture Notes in Computer Science*, *7041*, Springer, p. 38–57, 2011.

[48] S. Graf, D. Peled, S. Quinton, "Monitoring Distributed Systems Using Knowledge", *en : Formal Techniques for Distributed Systems - Joint 13th IFIP WG 6.1 International Conference, FMOODS 2011, and 31st IFIP WG 6.1 International Conference, FORTE 2011, Reykjavik, Iceland, June 6-9, 2011.*, R. Bruni, J. Dingel (réd.), *Lecture Notes in Computer Science*, *6722*, Springer, p. 183–197, 2011.

[49] I. B. Hafaiedh, S. Graf, M. Jaber, "Model-based design and distributed implementation of bus arbiter for multiprocessors", *en : 18th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2011, Beirut, Lebanon, December 11-14, 2011*, IEEE, p. 65–68, 2011.

[50] I. Ben-Hafaiedh, S. Graf, S. Quinton, "Reasoning about Safety and Progress Using Contracts", *en : Formal Methods and Software Engineering - 12th International Conference on Formal Engineering Methods, ICFEM 2010, Shanghai, China, November 17-19, 2010. Proceedings*, J. S. Dong, H. Zhu (réd.), *Lecture Notes in Computer Science*, *6447*, Springer, p. 436–451, 2010.

[51] S. Bensalem, M. Bozga, S. Graf, D. Peled, S. Quinton, "Methods for Knowledge Based Controlling of Distributed Systems", *en : Automated Technology for Verification and Analysis - 8th International Symposium, ATVA 2010, Singapore, September 21-24, 2010. Proceedings*, A. Bouajjani, W.-N. Chin (réd.), *Lecture Notes in Computer Science*, *6252*, Springer, p. 52–66, 2010.

[52] S. Graf, D. Peled, S. Quinton, "Achieving Distributed Control through Model Checking", *en : Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*, T. Touili, B. Cook, P. Jackson (réd.), *Lecture Notes in Computer Science*, *6174*, Springer, p. 396–409, 2010.

[53] I. Ben-Hafaiedh, O. Constant, S. Graf, R. Robbana, "A Model-Based Design and Validation Approach with the OMEGA-UML Profile and the IF Toolset", *en : 2nd Mediterranean Conference on Intelligent Systems and Automation, CISA 2009, March 23-25, Zarzis, Tunesia*, *AIP Conference Proceedings*, *1107*, American Institut of Physics, 2009.

[54] I. Ober, S. V. Baelen, S. Graf, M. Filali, T. Weigert, S. Gérard, "Model Based Architecting and Construction of Embedded Systems", *en : Models in Software Engineering, Workshops and Symposia at MODELS 2008, Toulouse, France, September 28 - October 3, 2008. Reports and Revised Selected Papers*, M. Chaudron (réd.), *Lecture Notes in Computer Science*, *5421*, Springer, p. 1–4, 2009.

[55] S. Quinton, S. Graf, "Contract-Based Verification of Hierarchical Systems of Components", *en : 6th IEEE Int. Conferences on Software Engineering and Formal Methods, SEFM08, Cape Town, South Africa, 10-14 November 2008*, IEEE Computer Society Press, p. 377–388, 2008.

[56] Olivier Constant, Wei Monin, and Susanne Graf. A model transformation tool for performance simulation of complex uml models. In *ICSE 2008, tool track*, LNCS, 2008.

[57] G. Gössler, S. Graf, M. Majster-Cederbaum, M. Martens, J. Sifakis, "An Approach to Modeling and Verification of Component Based Systems", *Current Trends in Theory and Practice of Computer Science, SOFSEM'07*, *LNCS*, 4362, 2007.

[58] G. Gössler, S. Graf, M. Majster-Cederbaum, M. Martens, J. Sifakis, "Ensuring Properties of Interaction Systems by Construction", *en : Program Analysis and Compilation, Theory and Practice*, *LNCS*, *4444*, 2006.

[59] I. Ober, S. Graf, D. Lesens, "A case study in UML model-based validation: The Ariane-5 launcher software", *FMOODS 2006*, *LNCS*, *4037*, 2006.

[60] S. Graf, S. Gérard, O. Haugen, I. Ober, B. Selic, "MARTES - Modelling and Analysis of Real Time and Embedded Systems Using UML", *en : MoDELS 2006 International Workshops, Doctoral Symposium, Educators Symposium; Genoa, October 2006, Revised Selected Papers*, *LNCS*, *4364*, 2006.

[61] S. Graf, A. Prinz, "Time in Abstract State Machines", *ASM 2005 conference proceedings, Paris*, 2005.

[62] S. Graf, S. Gérard, O. Haugen, I. Ober, B. Selic, "MARTES - Specification and Validation of Real-time and Embedded Systems, workshop overview", *MoDELS 2005 International Workshops, Doctoral Symposium, Educators Symposium; Montenegro Bay, Jamaica, Revised Selected Papers*, *LNCS 3844*, 2005.

[63] I. Ober, S. Graf, I. Ober, "Model Checking of UML Models via a Mapping to Communicating Extended Timed Automata", *11th International SPIN Workshop on Model Checking of Software*, *LNCS 2989*, 2004.

[64] S. Graf, I. Ober, "A Real-time profile for UML and how to adapt it to SDL", *SDL Forum 2003, July 1-4, Stuttgart*, *LNCS*, 2708, 2003.

[65] M. Bozga, S. Graf, L. Mounier, "IF-2.0: A Validation Environment for Component-Based Real-Time Systems", *Proceedings of Conference on Computer Aided Verification, CAV'02, Copenhagen*, *LNCS*, 2404, 2002.

[66] S. Graf, "Expression of time and duration constraints in SDL", *3rd SAM Workshop on SDL and MSC, University of Wales Aberystwyth*, *LNCS*, 2599, 2002.

[67] M. Bozga, S. Graf, L. Mounier, "Automated validation of distributed software using the IF environment", *2001 IEEE International Symposium on Network Computing and Applications (NCA 2001)*, IEEE, 2001.

[68] M. Bozga, S. Graf, L. Mounier, "Automated validation of distributed software using the IF environment", *Workshop on Software Model-checking, associated with CAV 2001, Paris*, S. D. Stoller, W. Visser (réd.), *Electronic Notes in Theoretical Computer Science*, *55*, Elsevier, 2001.

[69] M. Bozga, S. G. A. Kerbrat, L. Mounier, I. Ober, D. Vincent, "Timed Extensions for SDL", *SDL Forum 2001*, *LNCS 2078*, 2001.

[70] M. Bozga, L. Ghirvu, S. Graf, L. Mounier, "IF: A Validation Environment for Timed Asynchronous Systems", *Proceedings of Conference on Computer Aided Verification, CAV'00, Chicago*, *LNCS* 1855, 2000.

[71] S. Graf, G. Jia, "Verification Experiments on the Mascara Protocol", *Spin Workshop 2001, Toronto*, *LNCS* 2057, 2001.

[72] M. Bozga, J. Fernandez, L. Ghirvu, S. Graf, J. Krimm, L. Mounier, "IF: An Intermediate Representation and Validation Environment for Timed Asynchronous Systems", *Proceedings of Symposium on Formal Methods 99, Toulouse*, *LNCS* 1708, 1999.

[73] M. Bozga, J. Fernandez, L. Ghirvu, S. Graf, J. Krimm, L. Mounier, J. Sifakis, "IF: An Intermediate Representation for SDL and its Applications", *Proceedings of SDL Forum 99, Montreal*, Elsevier, 1999.

[74] S. Graf, H. Saidi, "Construction of abstract state graphs with PVS", *Conference on Computer Aided Verification CAV'97, Haifa*, *LNCS 1254*, 1997.

[75] S. Graf, H. Saidi, "Verifying invariants using theorem proving", *Conference on Computer Aided Verification CAV'96*, *LNCS 1102*, 1996.

[76] S. Graf, "Verification of a distributed Cache memory by using abstractions", *Conference on Computer Aided Verification CAV'94, Stanford*, LNCS 818, 1994.

[77] S. Graf, C. Loiseaux, "A tool for symbolic program verification and abstraction", *Conference on Computer Aided Verification CAV 93, Heraklion Crete*, LNCS 697, 1993.

[78] S. Graf, C. Loiseaux, "Program Verification using compositional Abstraction", *TAPSOFT 93, joint conference CAAP/FASE*, LNCS 668, 1993.

[79] C. Courcoubetis, S. Graf, J. Sifakis, "An Algebra for Boolean Processes", *Workshop on Computer-Aided Verification CAV'91, Aalborg (Denmark)*, LNCS 575, 1991.

[80] K. Kanoun, J. Arlat, L. Burrill, Y. Crouzet, S. Graf, E. Martins, A. MacInness, D. Powell, J.-L. Richier, J. Voiron, "Delta-4 Architecture Validation", *ESPRIT Conference Week 91*, 1991.

[81] A. Bouajjani, J.-C. Fernandez, S. Graf, J. Sifakis, C. Rodriguez, "Safety for branching Semantics", *18th ICALP, Madrid*, LNCS 510, 1991.

[82] S. Graf, B. Steffen, "Compositional Minimisation of Finite State Processes", *Workshop on Computer-Aided Verification, Rutgers*, LNCS 531, 1990

[83] M. Baptista, S. Graf, J.-L. Richier, L. Rodrigues, C. Rodriguez, P. Verissimo, J. Voiron, "Formal Specification and verification of a Network Independent Atomic Multicast Protocol", *IFIP Conf. FORTE 90, Madrid*, North Holland, 1990.

[84] S. Graf, J.-L. Richier, C. Rodriguez, J. Voiron, "What are the limits of model checking methods for the verification of real life protocols?", *1st CAV, Grenoble*, LNCS 407, 1989.

[85] S. Graf, J. Sifakis, "An expressive logic for a process algebra with silent actions", *Int. Colloquium on Temporal Logic in Specification*, LNCS 398, 1987.

[86] S. Graf, J. Sifakis, "Readiness Semantics for Regular Processes with Silent Actions", *ICALP 87, Karlsruhe*, LNCS 267, 1987.

[87] S. Graf, "A complete inference system for an algebra of regular acceptance models", *MFCS 1986*, LNCS 223, p. 386–396, 1986.

[88] S. Graf, J. Sifakis, "From synchronization tree logic to acceptance model logic", *Workshop on logics of programs, Brooklyn*, LNCS 193,

1985.

[89] S. Graf, J. Sifakis, "A Modal Characterization of Observational Congruence on Finite Terms of CCS", *ICALP 84, Antwerpen*, LNCS 172, 1984.

2.6 Communications to workshops (with PC and published proceedings)

[90] S. Graf, R. Passerone, S. Quinton, "Contract-Based Reasoning for Component Systems with Complex Interactions", *en : TIMOBD'11*, 2011.

[91] I. Ben-Hafaiedh, S. Graf, H. Khairallah, "Implementing Distributed Controllers for Systems with Priorities", *en : Proceedings Ninth International Workshop on the Foundations of Coordination Languages and Software Architectures, FOCLASA*, *EPTCS*, *30*, p. 31–46, 2010.

[92] I. Ben-Hafaiedh, S. Graf, S. Quinton, "Contract-Based Reasoning about Progress: Application to Resource Sharing in a Network", *en : Proc. of FLACOS'10*, 2010.

[93] S. Quinton, I. Ben-Hafaiedh, S. Graf, "From Orchestration to Choreography: Memoryless and Distributed Orchestrators", *en : Proc. of FLACOS'09*, 2009.

[94] M. Bozga, P. Combes, S. Graf, W. Monin, N. Moteau, "Qualification d'architectures fontionnelles", *Notere'06*, 2006.

[95] S. Quinton, S. Graf, "A Framework for Contract-Based Reasoning: Motivation and Application", *en : Second Workshop on Formal Languages and Analysis of Contract-Oriented Software, FLACOS, Malta, november 2008*, 2008.

[96] I. Ober, S. Graf, Y. Yushtein, "Using an UML profile for timing analysis with the IF validation toolset", *Proc. of Model-Based Development of Embedded Systems, MBEES, Dagstuhl*, *Technical Report SSE, U. Braunschweig*, 2006/01, 2006.

[97] I. Ober, S. Graf, Y. Yushtein, "Timing analysis and validation of the embedded MARS bus manager", *Proc. of Intl Workshop on Modeling and Analysis of Real Time Embedded Systems, MARTES 2005, associated with MoDELS*, *Technical Report* 2006.

[98] S. Graf, I. Ober, "How useful is the UML real-time profile SPT without Semantics?", *SIVOES 2004, associated with RTAS 2004, Toronto Canada*, 2004. position paper.

[99] M. Bozga, S. Graf, L. Mounier, I. Ober, "IF Tutorial", *9th SPIN'04 Workshop on Model-Checking of Software, Barcelona, Spain*, *LNCS*, *2989*, 2004.

[100] M. Bozga, S. G. A. Kerbrat, L. Mounier, I. Ober, D. Vincent, "SDL for Real Time: What is missing?", *Workshop SAM 2000*, 2000.

[101] S. Graf, C. Loiseaux, "A tool implementing a method for symbolic program verification", *Formale Methoden zum Entwurf korrekter Systeme, Bad Herrenalb*, 1993.

2.7 Book chapters

[102] S. Graf, R. Passerone, S. Quinton, *Contract-Based Reasoning for Component Systems with Rich Interactions*, Embedded Systems Development, Springer New York, pages 139–164 2014.

[103] S. Graf, H. Garavel, *Formal Methods for Safe and Secure Computers Systems - BSI Study 875*, BSI German Federal Office for Information Security (362 pages) 2013.

[104] M. Bozga, S. Graf, L. Mounier, I. Ober, *Real Time Systems 1: Modeling and verification techniques*, Hermes, Lavoisier, 2008, ch. Modeling and Verification of Real Time Systems Using the IF Toolbox, under press.

[105] M. Bozga, S. Graf, L. Mounier, I. Ober, *Systèmes temps réel 1: Techniques de description et de vérification (Traité IC2, Série Informatique et systèmes d'information)*, Hermes, Lavoisier, 2006, ch. La boîte à outils IF pour la modélisation et la vérification de systèmes temps réel.

[106] B. Jonsson, E. Brinksma, G. Coulson, S. G. et I. Crnkovic, S. Gérard, H. Hermanns, J.-M. Jezequel, A. Ravn, P. Schnoebelen, F. Terrier, A. Votintseva, "Roadmap: Component based design and Integration platforms", *Embedded Systems Design: The ARTIST Roadmap for Research and Development*, *LNCS*, *3436*, 2005.

[107] S. Graf, J.-L. Richier, J. Voiron, "Verification of systems with time-constraints", *en : "Delta-4 Architecture Guide", collection ESPRIT*, Springer Verlag, 1991.

[108] S. Graf, J. Sifakis, "A logic for the specification and proof of regular controllable processes of CCS", *NATO ASI Series F, Vol. 13, Springer Verlag*, 1985.

2.8 Thesis and Habilitation

[109] S. Graf, *Models and Methods for the Construction and Verification of Complex Reactive Systems*, Habilitation à diriger des recherches, Université Joseph Fourier, Grenoble, 2008.

[110] S. Graf, *Logiques du temps arborescent pour la spécification et la preuve de programmes*, Thèse de Doctorat, Institut National Polytechnique de Grenoble, February 29, 1984.

2.9 Technical reports - some not (yet) published work

[111] S. Quinton and S. Graf, "Analysis of the semantic of BIP in view of achieving compositionality ", *Rapport de recherche TR-2011-xx*, Verimag, 2011,

[112] S. Graf and S. Quinton, "Contract-Based Verification of Hierarchical Systems of Components ", *Rapport de recherche TR-2009-12*, Verimag, 2009, updated 2012

[113] O. Constant, W. Monin, S. Graf, "From Complex UML Models to Systematic Performance Simulation", *Rapport de recherche TR-2007-10*, Verimag, 2007, submitted for publication.

[114] S. Graf, F. de Boer, P. Combes, J. Hooman, H. Kugler, M. Kyas, D. Lesens, I. Ober, A. Votintseva, Y. Yushtein, M. Zenou, "Omega Final Project Report", *OMEGA IST project*, 2005.

[115] S. Graf, "States and events in the context of timed systems", *contribution to the workshop ST.EVE on state based versus event based approach, a satellite event of FM 2003*, Verimag, 2003.

[116] S. Graf, "Report on the organisation of ETAPS 2002 in Grenoble", Verimag, 2002.

[117] S. Graf, "Timed Extensions for SDL", *Document temporaire, ITU, secteur de standardisations des télécommunications, groupe d'étude 17*, 2001.

[118] S. Graf, Y. Lakhnech, P. Wolper, "Coping with Process Identities in Networks of Similar Processes", *Technical report*, Verimag, 1999.

[119] S. Graf, "Efficient Automata Encoding of Arithmetic expressions", *Spectre technical report*, VERIMAG, 1995.

[120] S. Graf, C. Rodriguez, J. Voiron, "Verification of the MAC tokenring protocol", *Deliverable of Esprit Delta 4*, LGI, Grenoble, 1989.

[121] C. Rodriguez, J. Richier, J. Voiron, S. Graf, "XESAR version 3.1", *Research report Spectre C-11*, LGI, Grenoble, 1988.

[122] S. Graf, Alfred Schmitt, "Simulationsmodell für die Studie von Laufzeiten auf Hardware-Ebene", *Interner Bericht des Instituts für Programmiersysteme*, Fakultät für Informatik, Universität Fredericiana, Karlsruhe, 1980.

Appendix 1: Program Committees - almost exhaustive list

- CAV, Int. Conf. on Computer Aided Verification: 2011, 2007, 2005, 1997
- TACAS, Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems, part of ETAPS: 2015, 2014, 2013, 2012, 2010, 2007, 2003, 2001, 1996 - 1998,
- FORTE, IFIP International Conference on Formal Techniques for Distributed Systems 2015 (PC-chair), 2014, 2012, 2009, 2008
- FASE, International Conference on Formal Aspects in Software Engineering, part of ETAPS: 2011
- CBSE ACM Sigsoft Symposium on Component-Based Software Engineering, 2013
- RV, Conference on Runtime Verification 2013, 2011, 2010 (since its creation)
- iFM, Int. Conf. on industrial Formal Methods: 2014
- TCS, IFIP Conference on Theoretical Computer Science 2012
- SAS, International conference on Static analysis 2010
- MoDELS/UML, Conf. on Model Driven Engineering Languages and Systems: 2010, 2009, 2007, 2006, 2005
- TOOLS 2012, Int. Conference on Objects, Models, Components, Patterns
- SPIN, Int. Workshop on Software Model Checking: 2011, 2009, 2008, 2007, 2002 - 2005
- FM, Int. Conf. on Formal Methods (formerly Formal Methods in Europe): 2006

- ATVA, Int. Symposium on Automated Technology for Verification and Analysis: 2005 - 2013 (PC chair in 2006)
- FMCAD, Int. Conf. on Formal Methods in Computer-Aided Design: 2006, 2004, 2002
- ASM, track on Abstract state Machines of the intern. ABZ conference: 2010, 2008, ASM workshop 2001
- SEFM, Int. Conference on Software engineering and Formal methods: 2006
- ICCP, Int. Conference on Intelligent Computer Communication and Processing, track on Static and Runtime Verification: 2006
- FACS, Workshop on Formal Aspects of Component Software: 2006, 2005
- FMICS, Int. Workshop on Formal Methods for Industrial Critical Systems: 2006
- ISORC, Int. Symposium on Object-oriented Real-time distributed Computing, Industrial track: 2006, 2005
- MBT, Workshop on Model Based Testing, associated with ETAPS: 2004 - 2007
- Workshop OMER on "Object-oriented Modeling of Embedded Real-Time Systems": 2005 - 2007
- IDM, Journée sur l'Ingénierie Dirigée par les Modèles: 2005 - 2007
- ICTAC, Int. Colloquium on Theoretical Aspects of Computing: 2009, 2004-2006
- ESWA, European Workshops on Software Architecture: 2006
- SDL forum on Integration of System Design Languages: 2009, 2005, 2003
- SAM, Workshop on System Analysis and Modelling (formerly SDL and MSC Workshop): 2006, 2004, 2002
- VMCAI conference: 2004
- Software Model Checking, a workshop associated with CAV: 2003, 2001
- ST.EVE , Workshop on State-oriented vs Event-oriented thinking in Requirements Analysis, Formal Specification and Software Engineering, a satellite event of FME: 2003
- SIVOES-MDA - Model Driven Architecture in the Specification, Implementation and Validation of Object-oriented Embedded Systems" avec la conférence UML: 2003
- ACM SIGPLAN "Workshop on Languages, Compilers, and Tools for Embedded Systems", LCTES: 2000
- CONCUR, Int. Conf. on Concurrency Theory: 1995
- German Workshop "Formale Methoden zum Entwurf korrekter Systeme": 1993

Appendix 2: Invited Conferences and Seminars - a more complete list

2.9.1 Invited Presentations at International Conferences

- Invited Presentation at the ISPDC conference that took place in June 2014 in Marseille (`http://eriscs.luminy.univ-amu.fr/ISPDC2014-TM/bienvenue.html`)
- Invited Presentation at the FSFMA workshop, affiliated with FM'14 in May 2014 in Singapour (`http://lipn.univ-paris13.fr/fsfma2014/`)
- Invited Presentation at the 10th International Conference on integrated Formal Methods in June 2013 in Turku, Finland.
- Invited Presentation at the Workshop on Formal Verification of Embedded Control Systems of the *LCCC Focus Period* in April 2013 in Lund, Sweden,
- Invited Presentation at the *INCOSE Industrial Day* in March 2010 in Tel Aviv.
- Invite Presentation at FDL conference that took place in September 2008 in Stuttgart ; a first presentation of our contract-framework
- Presentation of the SPEEDS contract-based design and Verification methodology at the system engineering conference INCOSE 2008 in Utrecht
- Invited Presentation at the IFIP Conference, FORTE 2007, June 27-29 2007, Tallinn, Estonia "A speculative design approach for embedded systems" [39]
- Invited Presentation at the Workshop "UML and AADL" ENST, Paris, October 9 2006. `http://www.see.asso.fr/htdocs/main.php/articles.php/1238`
- Invited Presentation at "A Formal Semantics for UML Symposium", satellite workshop of MODELS 2006, Genova. `http://www.disi.unige.it/researchsites/models06/s3.php`
- Workshop QAPL 2006 that took place at Vienna in April 2006, as a satellite event of ETAPS. "Modelling and verification of real-time systems: a framework, experimental results and extensions"
- Invited Presentation at the workshop "Beyond Autosar", organised in Innsbrück in April 2006, `http://www.artist-embedded.org/artist/Overview,337.html`
- Invited Presentation at the Workshop on "A semantics for UML", associated with the ECMDA conference, Nuremberg, November 2005. "Semantic needs for a design tool of real-time embedded systems"
- Panel *COTS Component-Based Embedded Systems - A Dream or Reality?*, at the ICCBSS int. conference, Bilbao, January 2005 [41]
- Invited presentation at the EWSA 2004 European workshop on software architectures, St. Andrews (Scottland), Mai 2004 "The Omega project: Correct Development of Embedded Systems using UML" [43]
- Invited Presentation at the *Telelogic user conference*, Paris (France), "OMEGA: a verification toolset for Real-time UML" October 6, 2004
- Invited Presentation at the "10 years of TACAS" Symposium, Barcelona , mars 2004. "IF: a language and tool-set for model-based validation of systems of heterogeneous components"
- Invited presentation at the ST.EVE Workshop on State-oriented vs Event-oriented thinking in Requirements Analysis, Formal Specification and Software Engineering, satellite event of FME 2003 "Events in the context of real-time systems"

- Panel "*Time in abstract state machines*" at the workshop on Abstract State Machines, Taormina, March 2003
- Invited Presentation Communication at the "Workshop on Automated Formal Methods" organised by Mike Reed in Oxford in June 1996, financed by the US Office of Naval Research.

2.9.2 Invited Presentations in Summerschools and Tutorials

- Marktoberdorf Summerschool 2010 on "Software Systems Safety — Specification and Verification", I gave a course on "Abstraction for system verification", August 2010
- Course at the Summerschool "École Jeunes Chercheurs en Programmation", Toulouse, June 5 to 16 juin 2006. `http://www.irit.fr/ejcp2006/`
- Tutorial at the ARTIST Summerschool *Verification of UML models with timing constraints using IF*, Naesslingen, Sweden, September 2005
- Tutorial at the Int. Doctoral School "Chambéry - Torino" in Theoretical Computer Science and in Semantic Web, Aussois, France, June 21-25, 2004
- One day course at the TYPES Summerschool, "*Theory and practice of formal proofs*", Giens, September 2-13, 2002
- Tutorial on "Temporal Logics and automated Verification", at the University of Clermont-Ferrand, en mars 1993
- Invited one week course on "Temporal Logic and verification" at UCV (Universidad Central de Caracas) in January 1993