Acronyme	**ECSPER**		
Titre du projet en français	Etude et Conception de Systèmes avec Perturbations		
Titre du projet en anglais	Analysis and Conception of Systems with Perturbations		
CSD principale	☑ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9		
CSD secondaire ***(si interdisciplinarité)***	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9		
Aide totale demandée	269 306 €	**Durée du projet**	48 mois

SOMMAIRE

1. CONTEXTE ET POSITIONNEMENT DU PROJET / CONTEXT AND POSITIONNING OF THE PROPOSAL 3
2. DESCRIPTION SCIENTIFIQUE ET TECHNIQUE / SCIENTIFIC AND TECHNICAL DESCRIPTION 4
2.1. État de l'art / Background, state of art 4
2.2. Objectifs et caractère ambitieux/novateur du projet / Rationale highlighting the originality and novelty of the proposal 7
3. PROGRAMME SCIENTIFIQUE ET TECHNIQUE, ORGANISATION DU PROJET / SCIENTIFIC AND TECHNICAL PROGRAMME, PROJECT MANAGEMENT 9
3.1. Programme scientifique et structuration du projet / Scienctific programme, specific aims of the proposal 9
3.2. Coordination du projet / Project management 11
3.3. Description des travaux par tâche / Detailed description of the work organised by tasks 12
3.3.1 Tâche 1 / Task 1 12
3.3.2 Tâche 2 / Task 2 13
3.4. Calendrier des tâches, livrables et jalons / Planning of tasks, deliverables and milestones 20
4. STRATEGIE DE VALORISATION DES RESULTATS ET MODE DE PROTECTION ET D'EXPLOITATION DES RESULTATS / DATA MANAGEMENT, DATA SHARING, INTELLECTUAL PROPERTY AND RESULTS EXPLOITATION 22
5. ORGANISATION DU PROJET / CONSORTIUM ORGANISATION AND DESCRIPTION 23
5.1. Description, adéquation et complémentarité des participants / Relevance and complementarity of the partners within the consortium 23
5.2. Qualification du porteur du projet / Qualitification of the principal investigator 24

5.3. Qualification, rôle et implication des participants / Contribution and qualification of each project participant 25
6. JUSTIFICATION SCIENTIFIQUE DES MOYENS DEMANDES / SCIENTIFIC JUSTIFICATION OF REQUESTED BUDGET 25
7. ANNEXES 28
7.1. Références bibliographiques / References 28
7.2. Biographies / CV, Resume 31
7.3. Implication des personnes dans d'autres contrats / Involvement of project particpants to other grants, contracts, etc… 35

1. CONTEXTE ET POSITIONNEMENT DU PROJET / CONTEXT AND POSITIONNING OF THE PROPOSAL

General context:
The correctness of software remains a major challenge, in particular in distributed and embedded systems. In the last decades, many works have been devoted to the use of formal methods for correctness proofs of systems, notably automatic methods like model checking.

The promise and nature of these methods is their capability to deal with non-determinism in models and to provide exhaustive analysis. In contrast, simulation and testing methods never capture all possible cases.

Non-determinism is used in modeling for different purposes :

1. modeling open systems where a supposed environment decides on its own operations. In this case, the actions of the environment are modeled as non-deterministic in order to model the behaviour of the system under examination « in an arbitrary environment ».
2. non-determinism introduced by abstraction in order to render the model accessible to the available algorithms. A typical example is the discretization of continuous variables to intervals of values. The abstracted variable merely states an interval (which contains the concrete value of the variable) and this introduces (additional) non-determinism into the model.
3. non-determinism as a model for perturbated or faulty behaviour. While formally, this is a special case of (2), it clearly is a topic of its own right as it is specialized to the deviation of the model from an ideal case. An example of such non-determinism is the modeling of «lossy channels » [AJ96b], which differs from the perfect FIFO channel in that it may at any time lose messages. Another example is « clock drift » in models of timed and hybrid systems [Pur98, Fra99].

The emphasis of this project is on the third kind of non-determinism which we call « perturbation » here. This is in contrast to approaches using probabilistic models as predominant in the domain of fault tolerance. Defining perturbations in terms of an alternative semantics based on non determinism allows to use techniques devoted to non deterministic systems (such as symbolic techniques) which allow an exhaustive analysis, unlike what is comonly done for probabilistic models.

A major challenge with respect to automatic verification is the availability of decision procedures and ultimately efficient algorithms for the problems examined. Whereas classical model checking was originally invented for finite state systems, today there exist extensions for certain types of systems with infinite state spaces (dense time variables, unbounded counter, channels, stacks...).

In this light, perturbations have shown to be both, a source of problems (increased difficulty or complexity), but on the other hand they sometimes allow for easier analysis than unperturbed systems. As an example, whereas the safety problem for hybrid systems is knwn to be undecidable, even for automata with only two clocks and a single stop-watch, [Fra99] shows that for hybrid systems that are robust, i.e. that are tolerant to pertubations, the problem becomes decidable.

Similar observations have been made for other models and in different contexts, but to our knowledge, very little effort has been invested into a cross examination of the different kinds of perturbations and algorithms involved. On the other hand, several of these works have been done on a purely technical/theoretical level without consideration of the practical usefulness of the perturbations for systems modeling. E.g. the above mentioned lossy channel that does not guarantee to ultimately deliver a message can actually stop delivering messages on the whole, is probably of limited use in applications.

Project aims:
This project aims at improving the understanding of perturbations with respect to automatic verification and to modeling. We want to understand if and how different kinds of perturbations and the corresponding algorithms are linked, study their interaction and propose new kinds of perturbations with desirable properties. We want to evaluate the usefulness of perturbation models for modeling of realistic applications and, if there is a discrepancy, see if the models can be adapted to obtain increased usefulness while maintaining desirable properties for automatic verification. Finally, we intend to implement some of the developed algorithms for a pragmatic evaluation of their potential.
More spcifically, we intend to look at models based on infinitely valued data, such as timed or hybrid systems, counter systems, etc. and on models based on message passing, such as message sequence charts, channel systems and more general models of distributed systems.

Positionning of the project:
As far as we know, this is the first french project devoted to the analysis of systems with perturbations. Some of the aspects of the project are however also mentionned in other projects, but not in the same setting. For example, a small part of the ARA DOTS project (DOTS stands for Distributed, Open and Timed Systems) is interested in imprecisions in timed systems. Similarly, the european project Quasimodo, which studies quantitative aspects in model-driven design of embedded systems, looks only at timed systems. In a general way, these projects only care of the applications and development of these models of faults, but never on their theoretical foundations neither of the systems with faults in their globality.

Potential economic impact:
Perturbations and faults are a major concern in the safety of forthcoming embedded systems. It is foreseeable that the modeling of technical deficiancies and the formal proof of the effective handling of perturbations of the systems will play an increasing role in future certification procedures. While this project is basic research in nature, we expect it to contribute to the capability of formal methods to meet the challenges arising from these future needs. Likewise, the locally acquired expertise in the domain may be put to the use of small innovative companies of the regional Competitivity pools SCS and Pégase, which intend to improve the quality of their products in highly competitive markets.

2. DESCRIPTION SCIENTIFIQUE ET TECHNIQUE / SCIENTIFIC AND TECHNICAL DESCRIPTION

2.1. ÉTAT DE L'ART / BACKGROUND, STATE OF ART

Although there are very few works studying in a global a way at the different models of perturbations, there are several works introducing and studying perturbations for one or another type of systems, for example for timed automata, channel systems... We present a survey of the different such works we are aware of.

Infinite State Systems: There have been several attemps for introducing perturbations in systems with infinitely valued data by modifying their updates. We survey them here.

Timed automata. Timed automata [AD94] constitute a very well established formalism for modelling systems including dense-time variables. One of their properties, which justifies the interest for this model, is the decidability of the emptiness problem, using an abstraction based on so-called regions. However, the class of timed languages they recognize suffers from poor closure properties, what contrasts whith the case of regular languages. For example, the universality and inclusion problems are undecidable, the timed regular languages are not closed under complementation, nor under determinization... Many of the examples on which proofs of these results are based rely on punctuality testing. Thus, some researchers have tried to introduce perturbations so as to remove this ability of punctuality checking, with the hope that the resulting model would have better closure properties. First, a notion of robust timed automata has been proposed by Henzinger et al [GHJ97] and further studied in [HR00,OW03]. In this definition, a timed word is accepted if and only if almost all timed words in its neighboorhood are accepted. Unfortunately, the authors have proven that this new definition does not lead to better closure properties. Another approach, introduced by Puri in [Pur98], proposes to consider perturbations in the model itself and not only in the accepted language. More precisely, given some parameter $\varepsilon>0$, Puri defines an alternative semantics allowing clocks to evolve with some drift, inside interval $[1-\varepsilon, 1+\varepsilon]$. In its paper, he proposed alternative algorithms for checking safety, showing that for this problem the complexity was the same as for standard semantics. More recently, several authors have pursued the study of this semantics, looking at another presentation based on guard enlargment. First, Raskin et al have shown in [DDR05a,DDR05b] that this semantics is in some sense pragmatic as it can be used to prove the implementability of the system. Second, much progress has been done in analyzing these perturbed timed systems w.r.t. complex properties. Whereas [Pur98,DDMR04] proposes an algorithm for simple reachability properties, we proposed in [BMR06] an extension to repeated reachability properties and more recently in [BMR08] an algorithm for a large subset of the logic MTL, without sacrifying complexity with regard to standard semantics. In the last years, several works have also looked at symbolic approaches for robust model checking [DK06,SF07,SFK08], which we will detail later. Third, other works are related to language theoretical properties of this model of perturbation, such as [ALM05,Dim07].

Hybrid systems. Drifts of variables have also been introduced in hybrid systems by Fränzle. In [Fra99], he shows that using some realistic hypotheses of robustness, with regard to the introduction of perturbations as drifts of variables, the analysis of systems may be dramatically simplified. However, the criterion of robustness he introduces remains undecidable, thus forbidding any automatic approach based on this result. Another semantics with perturbations for hybrid systems has been proposed and studied by Thiagarajan et al in [AT04,AT05,ASTY06]. In these works, perturbations are introduced through a fuzzy semantics, based on a rough discretization. More precisely, the system operates its action within some bounded delay and the values of continous variables can be observed only with finite precision. As a consequence, the authors prove that the discrete time semantics of these systems is simpler than the one for corresponding standard hybrid systems, and in particular can be effectively analyzed.

Other infinite state systems. Pursuing on hybrid systems, we mention the interesting work [AB01] of Asarin and Bouajjani in which the authors build some links between different forms of perturbations. More precisely, their results concern on one side different formalisms of hybrid systems, and on the other side Turing machines. They prove that, roughly, systems which are tolerant to perturbations, say robust, are more decidable that general ones. Finally, let us mention a definition of perturbations in counter automata proposed by Demri and Lazic in [DL06]. In this paper, the authors are interested in proving decidability results for

verification of systems with registers. Therefore, they introduce counter automata with incrementation errors, that is when incrementing, the machine may, non deterministically, choose to increment arbitrarily the counter. They then show an equivalence with lossy channel systems, thus obtaining decidability results. These two last papers are interesting examples of the kind of crossing results we aim at obtaining in this project.

Message Passing Automata: A second major way of introducing perturbations is in the delivery of messages. We survey here the different approaches we are aware of.

Message sequence charts. A communicating finite state machine (CFM) [BZ83] consists of a set of processes that communicate asynchronously with each other over reliable (possibly) unbounded (FIFO or non FIFO) channels. The only actions performed by such a system are sending and receiving typed messages. In a CFM, each process is provided with its set of local states and its local transition relation, contrary to lossy channel systems where the transition relation is global. Moreover no messages are lost. Semantics of CFMs are based on the popular design of Message Sequence Charts (MSC). MSCs are a model often used for the documentation of telecommunication protocols. They profit by a standardized visual and textual presentation (ITU-T recommendation Z.120 [IUT]) and are related to other formalisms such as sequence diagrams of UML. An MSC gives a graphical description of communications between processes along some particular scenario. Channels in MSCs are supposed to be reliable. Yet, this formalism can be used at a very early stage of design to detect errors in some specification.
As a concurrency model, CFMs and MSCs have been widely used to specify and validate communication protocols. In this direction, several studies have already brought up methods and complexity results for the model checking and implementation of MSCs viewed as specification language [AY00, BM03, BM04, GMSZ02, GMK04, HMNST05, MP99]. However, in our knowledge, very few papers deal with MSCs (or CFMs) and loss of messages together. In [PM04], a new model (called LCFM) based on CFMs with loss of messages (or dropping messages) is defined. It allows more succinct specification than CFMs, which aids to improve verification of communication protocols. On other hand in [BM07], the authors attempt to extend the models of MSCs to loss of messages. More precisely a new model unifying numerous concurrency models (and in particular lossy MSCs) is provided. This model can be characterized by weighted existential MSO formulae. However, this work doesn't deal about analysis and construction of systems based on lossy MSCs specifications.

Lossy channel systems. Channel systems are composed of finite state automata communicating over asynchronous unbounded FIFO channels. Introduced by Abdulla and Jonsson [AJ96b], lossy channel systems, in which the channels may abritrarily lose messages, are the natural model for fault-tolerant protocols where the communication channels are unreliable. This model can be used for many interesting systems, e.g. link protocols such as the Alternating Bit Protocol and HDLC. In contrast to classical channel systems, many verification problems are decidable for lossy channel systems: termination, reachability, safety properties over traces, inevitability properties over states, and several variants of these problems [Fin94, AK95,CFP96,AJ96b,MS02]. However, the verification of recurrent reachability properties remains undecidable, so that model checking of liveness properties is undecidable too [AJ96a]. This model has permitted to verify safety properties for asynchronous communication protocols, however, it is too pessimistic when liveness is considered, because it introduces marginal behaviors very unlikely (such as executions where all messages are systematically lost). A solution recently studied is to consider probabilistic lossy channel systems where message losses are viewed as some kind of faults having a probabilistic behaviour. This idea, due to [PN97], led to the introduction of the first Markov chain model for lossy channel systems. Results about probabilistic lossy channel systems are surveyed in [Sch04]. Another solution, much less studied, is to add some fairness assumptions on the channel message losses. A first negative result is presented in [AJ96a], where the authors

show the undecidability of the verification of eventuality properties with fair channels: do all computations eventually reach a given set of states if the unreliable channels are fair in the sense that they deliver infinitely many messages if infinitely many messages are transmitted. More recently, a positive result has been presented in [MS02] which shows that there exist natural fairness properties that are decidable for lossy channel systems. E.g., termination under the assumption of fair scheduling ("fair termination") is decidable for a large and natural class of lossy channel systems.

Distributed systems. The reachability in lossy channels systems is decidable and this is good for verification purposes. However, from the result of Fischer, Lynch and Paterson [FLP85] that states that consensus cannot be solved in an asynchronous message passing system where one process may crash, we easily see that consensus cannot be solved in an arbitrary lossy channel system. In our opinion, it shows that this model cannot be useful for practical purposes since basic distributed problems cannot be solved in this model.
In the distributed algorithms community, several models of communication have been proposed to deal with communication failures. Due to the impossibility result of [FLP85], these models are generally synchronous. In probabilistic approaches (like [PP07], for example), there exists generally a known value $p < 1$ such that each transmission fails with probability p. The drawback of this model is that the solutions derived for it have no deterministic guarantee of correctness. In the deterministic setting, either faults are localized (i.e., they represent static faults), or the number of faults that can occur at the same time is bounded. For example, there may exist a bound L in the model such that at each time step, at most L messages are lost. In [DKKS08,DKP08], Dobrev et al. consider a new kind of model where at each time step at least a message is delivered if at least k messages are sent where k is the edge connectivity of the underlying communication graph (with such a bound k, the adversary cannot permanently disconnect the network). Contrary to the model of lossy channel systems, some algorithms have been given to solve basic distributed tasks (broadcast, consensus, election, for example) in these models.
Another approach of failures in distributed computing is the self-stabilization approach, introduced by Dijkstra [Dij74]. In this approach, one consider that there are only transient failures in the system, but we are interested in recovering a correct behaviour once there is no more failure, i.e., the algorithm should reach a correct configuration from any initial (possibly incorrect) configuration. There have been many works done about self-stabilization, and in particular Boldi and Vigna have characterized in [BV02] what can be computed in a self-stabilizing way in synchronous networks.

2.2. OBJECTIFS ET CARACTÈRE AMBITIEUX/NOVATEUR DU PROJET / RATIONALE HIGHLIGHTING THE ORIGINALITY AND NOVELTY OF THE PROPOSAL

The ECSPER approach via an example :
A very old « case study » of protocol verification is the « alternating bit protocol » (ABP), which is meant to implement a reliable communication over an unreliable synchronous channel. The lack of reliability is expressed in terms of lost messages. However, when modeling the loss of messages by non-determinism (rather than by probabilities), the ABP can no longer guarantee eventual delivery of messages, i.e. the abstraction of error probability to pure non-determinism has destroyed the essential property of the protocol. If however Büchi liveness conditions are added, the lossy channel may lose an arbitrary yet only finite of messages in a row : from time to time at least, a message will pass and this property is sufficient for proving the correctness of the ABP.

Passing from synchronous to asynchronous communication, the channel is represented by a a FIFO buffer, which outputs messages in the same order it received them. However, a finite state automaton equipped with a FIFO buffer is Turing complete and has an undecidable reachability problem. A surprising approach to this problem was to assume a lossy channel (some messages in the FIFO stream get lost), yielding a decidable reachability problem.

However, as with the lossy synchronous channel, the untamed loss of messages prevents effective use in modeling and analysis. The ECSPER approach is to evaluate the lossy channel with respect to algorithms, but also with respect to modeling. For the latter, a particular case study will concern the possibility to implement and prove correctness of certain distributed algorithms. From the impossibility result of Fischer, Lynch and Paterson [FLP85], we know that consensus cannot be solved in a network with fully lossy channels. A logical step is to investigate modified models of FIFOs that are « a bit less lossy ». Now we are faced with three questions :

(a) Does this extension allow to model the case studies impossible with the base model?
(b) Can the decidability proof of the case without Büchi conditions be preserved/adapted?
(c) Beyond (b), do feasible algorithms exist, and how do they behave on the examples?

In analogy to the ABP above would one might try Büchi-like conditions on message loss, but this turns out to be too naïve : As can be seen in [AJ96a], naïvely doing so yields undecidable systems. It is a major scientific challenge to determine the border between decidable and undecidable in this domain.

Scientific and technical objectives, originality and novelty:
The lossy channel is just one of many examples of non-deterministic fault models where a similar situation arises. We will identify and study in the same spirit a collection of non-deterministic fault models in the domain of distributed systems and real-time/hybrid systems. An example of fault models in real-time systems is *clock-drift*, where the clocks of different processes in a distributed systems need not run at the same speed. We may also look at fault models that have not been explored at all, e.g. stacks (LIFO).

For all these models, we want to explore alternative fault models under the crossed perspective of the criteria (a)-(c) above. We aim at progressing in the algorithmic issues associated with these models and finally validate these models by implenting these algorithms and tools and aplly them on academic case studies.

This is a totally new line of research and it may open up new interesting perspectives on these models. Though almost all members of the project have already worked on perturbations, this direction has never been studied for its own in our laboratory nor in our MoVe team. We believe that the porject can be the origin of a new research axis in our team.

Scientific and technical obstacles:
The project aims to develop and explore algorithms and decision procedures that may be both based on previous work or completely new. The invention and the correctness proof of such methods is a major scientific challenge. In particular, the gap between theoretically analysed perturbation models and application domains has yet to be scientifically explored. Application driven model propositions might turn out to be challenging from an algorithmic point of view. To find the compromise between the pragmatically useful and the technically feasable may turn out to be difficult. Finally, a decision procedure does not directly provide an efficient algorithm. While the experimental implementation of algorithms will be based on a good code base, new data structures may have to be invented for efficient implementations.

The aimed final result :

The study opens a new line of research. At the end of four years, we hope that our effort will shed significant light on the questions and answers given which will be presented in an integrated report on fault models, accompanied by an experimental platform and case studies. The project will also allow to further develop our experimental tools by added functionality and maturity.

Evaluation approach:
The project is evaluation driven from the start. A detailed survey of the state of the art will allow to evaluate concretely the progress achieved within the project. The project is accompanied by an effort in case studies and application domains which will allow at the end of the project an assessment of the pragmatic potential both in terms of modeling and effective analysis. Algorithms are implemented and experiments are conducted on the case studies. The modeling methodology will be presented to local innovative companies for feedback which will be joined to the final report.

3. PROGRAMME SCIENTIFIQUE ET TECHNIQUE, ORGANISATION DU PROJET / SCIENTIFIC AND TECHNICAL PROGRAMME, PROJECT MANAGEMENT

3.1. PROGRAMME SCIENTIFIQUE ET STRUCTURATION DU PROJET / SCIENTIFIC PROGRAMME, SPECIFIC AIMS OF THE PROPOSAL

As we said before, the main objectives of the project can be divided in three aspects: definition of models, algorithmical progress and experimental validation. We detail here each part of these objectives.

Scientific Program. The project will of course start by the elaboration of a survey of known works related to systems with perturbations. We have already mentionned several works we are aware of, we will thus look for other works. We will then try to solve each of our objectives as follows:

- *Models.* From the survey we will build a list of existing models in order to evaluate them. In our goal of finding adequate models of faults, which both satisfy practical requirements (amenable to modelization of concrete systems) and theoretical requirements (perturbations allow efficient algorithms for analysis and do not unable the implementation of standard distributed algorithms), we will evaluate these models w.r.t. these two criteria. For the first one, we wil use relevant case studies, and for the second one we will refer to exisiting works which give complexities for analysis or, when necessary, try to evaluate the gain or loss of complexity w.r.t. corresponding problems for standard model. Once the models have been analysed, we should be able to propose adaptations of these models to patch some weaknesses, or to imagine combinations of existing models with good properties.
- *Algorithms and decidability.* To progress in algorithmic purposes, we will first look at existing open problems for systems with perturbations. We are already aware of some of these problems, and the results of the survey will probably suggest some other interesting problems. These problems may be related to standard verification problems, such as reachability analysis, or to synthesis issues. For example, in the framework of control synthesis, one would like to be sure that, even in presence of perturbations, the system, under the supervision of the controller, will have a safe behaviour. Second, we will be interested in the original models we will propose to

confirm their interest by proving some properties, such as decidability. For example, the introduction of perturbations in timed automata has not yet yield interesting results w.r.t. decidability. Third, we will look at the implementation of distributed algorithms (such as concensus or leader election) in systems with perturbations. It is well known that synchrony has a strong impact on existence of such distributed algorithms, it is then relevant to study intermediary frameworks, in which only a weak form of synchrony is ensured.

- *Experimental validation.* All along the project, we will keep a link with experiments. When evaluating the existing and the new models we propose, we will use case studies to determine whether these models are or not adapted for modelization, and more precisely to determine for which kind of applications they are well suited. Second, once models have been choosen and algorithms proposed, we will look again at experiments by first developing tools implementing our algorithms and second testing our tools and algorithms on different case studies.

Methodology and Structuration of the project. To achieve the aims of the project, we have identified 5 separate tasks, which are listed below :

1. Elaboration of an extensive survey
2. Models evaluation and proposal
3. Algorithmic and decidability procedures
4. Case Studies and applications
5. Tools developments

The dependancies of these tasks are represented on Figure 1. The methodology of the project is then as follows:

- First, an extensive survey of existing works (Task 1) will give a presentation of existing systems with perturbations, but also indications on existing case studies and/or applications and algorithms associated with these models. It is preliminary to many of further works.
- Then, an important part of the project will be devoted to the models, gathered in task 2. This will cover the two aspects described above, the evaluation of models and, using this experience, the proposal of new models. This task will be in strong relation with two other tasks, namely task 3 related to algorithmical issues, in which we will study the algorithmical properties of the models, in terms of decidability and of efficiency , and task 4 devoted to case studies, which will allow to verify the relevance of the models w.r.t. modelization.
- More precisely, we believe that the interactions between these tasks will be both way. Indeed, as we just said, the evaluation of exisiting models will be based on theoretical and modelization evaluations, and conversely the original models that will be proposed will give raise to new algorithmic and decidability issues, and also in new challenges of modelization.
- Finally, we defined task 5 devoted to the realization of tools and their use for experiments. This task will use algorithms proposed in task 3 and aims at applying them on case studies identifed in task 4.

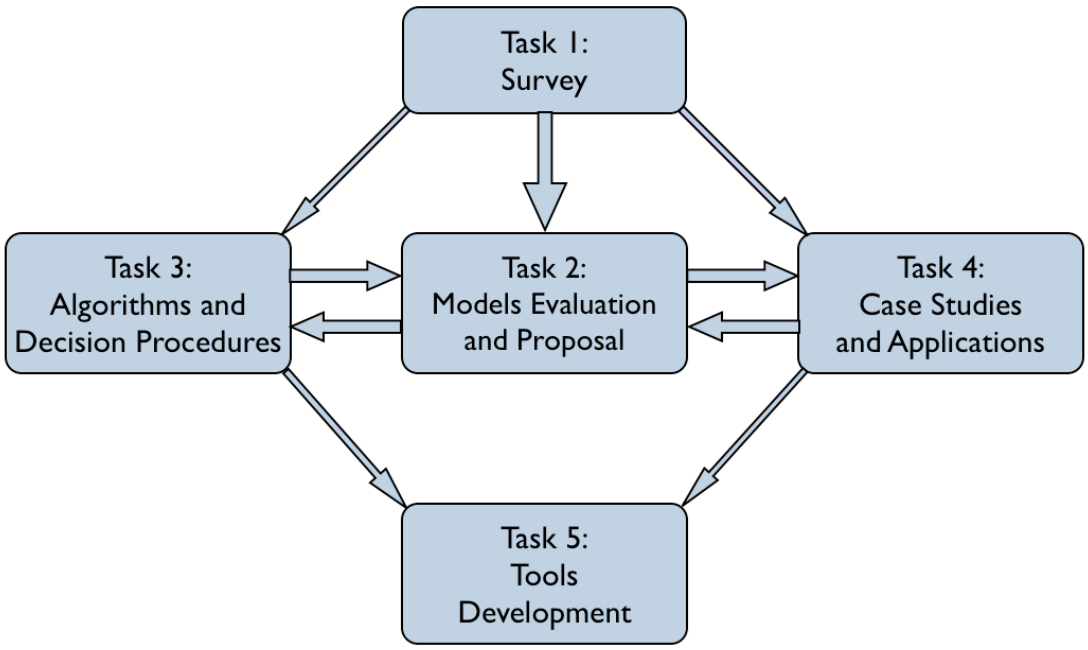

Figure 1: Dependancies between the different tasks.

Apart from these five technical tasks, there will also be a task devoted to coordination of the project (task 0), and a task devoted, in the last six months of the project, to an overall evaluation of the project (task 6).

3.2. COORDINATION DU PROJET / PROJECT MANAGEMENT

The coordination of the project will be isolated in a separate task, task 0. It will be realized by two persons, Pierre-Alain Reynier and Peter Niebert. First note that since the team is rather small, and all the members belong to the same group MoVe of the Laboratoire d'Informatique Fondamentale, located in Marseille, the interactions between the members of the project will be rather easy.

Meetings. Concerning interactions between members, the following additional elements will be settled to achieve the objectives of the project :

- *Monthly meeting:* we plan to organize a half day meeting each month for the whole team. This meeting will be located in our laboratory. The objectives of this meeting will be as follows : first, for each task, the person in charge of this task will present its advances. We could for example have a one-hour presentation per meeting and several shorter presentations. Second, we will have discussions on interactions and cooperations between tasks and members inside tasks, to stimulate crossing works.
- *Milestones:* every six months, we will have special meetings during which we will have time for evaluating the advances of the project, task by task, w.r.t. the intial planning. After this evaluation, we will discuss to decide , if it is necessary, redefinitions of the objectives of tasks. We also plan for these meetings to have external guests such as senior reasearchers to obtain external feedback on our work.

Practical aspects. To simplify material exchanges, and to enhance visibility of the project, we will realize a website for the project. Peter Niebert will be the responsible of this part of work. The website will be based on CMS technology to include a public part, used for

external communication, and a private one, used for internal communication. It will also be used as a SVN depository for shared ressources.

3.3. DESCRIPTION DES TRAVAUX PAR TÂCHE / DETAILED DESCRIPTION OF THE WORK ORGANISED BY TASKS

3.3.1 TACHE 0 / TASK 0 : MANAGEMENT

Person in charge and involved members:
Pierre-Alain Reynier will be in charge of this task and Peter Niebert will also be involved.

Objectives and detailled program:
The aim of this task is to perform the coordination of the project. This includes leading the project to on-time schedule fulfilment of the goals and request of approvals, driving and encouraging cooperation and coordination both within the project as well as with other ongoing projects and appropriate research activities.

Methods, technical choices and solutions:
As described in section 3.2, the management will be based internaly on two types of meetings. Monthly meetings, during one half day, will be focused on interations between members, and internal presentations of advances. Antoher type of meetings, occuring every six months, will be devoted to evaluation of the advances of the project, and to discussions on eventual updates in the scientific objectives. These meetings will be the opportunity to have external guests such as senior reasearchers to obtain external feedback on our work.
Concerning the practical aspects, a website will be realized to simplify internal communication and sharing of ressources. The website will also be for external communication in order to enhance the visibility of the project.

Risks:
This task should be amenable with no particular risk.

Deliverables:
The first deliverable will be the website which should be issued after six months.
The other deliverables associated with this task are the activity reports which will be produced every year.

Individual contributions:
Pierre-Alain Reynier will be responsible of the synthesis of reports, and their transmission to the ANR. He will also be in charge of the interactions with other research groups with close activities.
Peter Niebert will be responsible of the realization of the website, and of its mangement during the project, wih the actualisation of the communications and other productions of the project.

3.3.2 TACHE 1 / TASK 1 : SURVEY

Person in charge and involved members :
Nicolas Baudru will be in charge of this task. All the other permament members will also be involved in this task, together with the PhD student.

Objectives and detailled program :
The aim of this task is to build a complete survey of the numerous existing approaches for the introduction of failures and/or perturbations in standard extensions of finite state systems. The study will both present the different models that have been proposed by the community, and also the associated results and case studies which are known.

Methods, technical choices and solutions :
In a first period of time (first six months), the different members will work individually on the model they are the most aware of and the results should thus be available very fast. In a second step (six months after), we will cross our results and check that the corresponding references have all been explored.

Risks :
This task should be amenable with no particular risk.

Deliverables:
We plan to produce a report presenting this complete survey after the first year of the project.

Individual contributions :
Following individual experience, the repartition will be as follows:
- Nicolas Baudru will be mainly interested in message sequence charts
- Jérémie Chalopin will mainly be interested in distributed systems
- Séverine Fratani will be mainly interested in channel systems and stack automata
- Peter Niebert and Pierre-Alain Reynier will be mainly interested in timed systems

In addition, the six first months of the thesis of the PhD student will be devoted to this task and he will be higly implicated in it.

3.3.3 TACHE 2 / TASK 2 : MODELS EVALUATION AND PROPOSAL

Person in charge and involved members:

Séverine Fratani will be in charge of this task. All the other permanent members will be implicated in this task, together with the PhD student.

Objectives:

The objectives of this task are twofold. First, we want to have a fair evaluation of the existing systems with perturbations: lossy channel systems, clock drifts in timed automata... This evaluation will be based on theoretical properties of the model (decidability, complexity) and on relevance of the model w.r.t. modelization issues. Second, following this evaluation, we will try to propose, when necessary, extensions and/or new models of perturbations for these systems, for other systems (such as stack automata) and for combiend systems (channel automata with time).

Detailled program, methods, technical choices and solutions:

More precisely, we aim in this task at looking at the following questions:

1. **Channel Perturbations**
   Implicated members: Nicolas Baudru, Jérémie Chalopin and Séverine Fratani.

The aim is to analyze the expressive power of the different formalisms of perturbations in message passing systems. To do so, we want to consider basic distributed tasks (like consensus, election, broadcast, etc.) and understand in which models they can be solved (i.e., what kind of failures can we overcome). We already know that there is an important gap between synchronous and asynchronous systems when messages can be lost. In the synchronous setting, an interesting question is to identify a class of models where these problems can be solved that is an intermediate class between lossy channel systems and the models existing in the distributed computing literature, such as the one considered by Dobrev et al. [DKKS08,DKP08] where at each time step at least one message is delivered if enough messages have been sent. For each model, we also have to consider the underlying topology of the network. Indeed, even if in a given model, a problem cannot be solved in every network, it is possible that there exist interesting classes of graphs where the problem can be solved. For example, in the case of message passing systems where processes do not have ids, the election problem cannot always be solved (just consider an oriented ring where all processes have the same id). However, it has been shown that it can be solved if the graph is covering-minimal [BCG+96,CM07]: if for example, there strictly more than N/2 different ids in a network with N processes, then it is possible to solve the election problem.
An interesting question would be to characterize in a given model for which graphs the considered problem can be solved: the larger the class is, the more interesting the model is. Considering the topology is also interesting for verification purposes. For example, in [CS08], Chambart and Schnoebelen consider channel automata where some particular channels are lossy and they present a classification of topologies according to whether they have a decidable reachability problem.

2. **Clock Drift**
Implicated members: Pierre-Alain Reynier, Peter Niebert, Jérémie Chalopin
There are different directions we would like to investigate in this topic. Among them, it seems interesting, in a distributed framework, to allow different drifts in the network, which may lead to a different class of systems. Then, we want to compare such a model of perturbation for timed systems with the timed asynchronous model introduced by Cristian and Fetzer in [CF99]. In another direction, this model of perturbation has up to now not permitted to obtain better complexity or decidability results (if we except [ALM05]). We thus want to investigate this topic, either by an algorithmical approach (see Task 3), or by a proposal of alternatives definitions of perturbations.

3. **Innovative Perturbations Models**
Implicated members: Séverine Fratani, Pierre-Alain Reynier
A first objective is the study of the introduction of perturbations in stack automata. As far as we know, no such model has been proposed yet. Thus we want to evaluate the interest of this notion and, if this interest is proven, to propose original models of perturbations for this model. Therefore we will try to build links with another model of perturbations adapted to another class of systems. Other directions include the perspective to adapt models of perturbations from a system to others.

4. **Crossed Study**
Implicated members: Pierre-Alain Reynier, Nicolas Baudru
As we already mentionned, [DL06] proved equivalences between perturbations introduced in counter automata and loss of messages in channel automata. The objective here is to obtain similar equivalences for other models of perturbations, or slight adaptations of them. In a second step, we will study combined models, that is systems combining two standard extensions of finite state system, and try to

introduce adequate models of perturbations. For example, we want to consider a model combining a channel for message passing and dense-time variables representing clocks, as in timed systems. In such a model, we will introduce both loss of messages and imprecisions on clocks and aim at obtaining decidability results for reachability properties.

Risks:
The risks associated with this task are the usual risks associated with sicentific research, that is a wrong choice of scientific directives. This risk will be managed by scientific discussions and evaluations of progress planned in Task 0.

Deliverables:
We plan to produce two deliverables for this task. The first one, the intermediate report named Del 2.1, should roughly correspond to points 1 and 2 and be delivered after 24 months. The second one, the final report Del 2.2, should roughly correspond to point 3 and 4 and be delivered after 36 months.

3.3.4 TACHE 3 / TASK 3 : ALGORITHMIC AND DECIDABILITY ISSUES

Person in charge and involved members:
Pierre-Alain Reynier will be in charge of this task. All the other permanent members will be implicated in this task, together with the PhD student and the post-doctoral researcher.

Objectives:
In this task, our goal is to propose algorithmical solutions to various issues for existing models and for our original models. We will be interested in different kinds of problems, such as model checking, controller synthesis and realizability of distributed algorithms...

Detailled program, methods, technical choices and solutions:

1. **Model Checking**
   Implicated members: Pierre-Alain Reynier, Peter Niebert, Séverine Fratani
   The models of perturbations described before are often used for verifying the correctness of a system, even if the real system deviates a little from the trajectories of the exact model. Introductions of the perurbations in the semantics lead to a need of definition of original algorithms. This is for example the case for lossy channel systems and for clock drifts and much work remains to do in this topic. A first example we are working on is to succeed, in the analysis of perturbations in timed automata, to move from qualitative to a quantitative analysis. More precisely, exisiting algorithms allow to decide whether, for some parameter ε of deviation, the system is still correct w.r.t. the property. A quantitative approach aims at computing the supremum value for ε for which the property satisfied. This requires to have a full understanding of the effect of perturbations on the system, and of the existing qualitative algorithms.

2. **Controller Synthesis**
   Implicated members: Pierre-Alain Reynier, Peter Niebert, Nicolas Baudru
   A major challenge is the combination of the definitions of perturbations with the notion of games. A natural application is the automatic synthesis of controllers from specifications, which are by construction robust against perturbations. Intuitively, when the perturbation is quantitative, such as for timed systems, it appears that the value of perturbation should be choosen by the adversary. A first attempt for timed

systems has been presented in [CHP08], but it does not solve the problem for unspecified deviations. Indeed, it either lets the choice of the value of the (positive) deviation to the controller, or defines the maximal deviation as a fixed parameter. We aim, in this context, at solving the problem of deciding whether there exists a value ε of the perturbation together with a controller such that, for any deviation smaller than ε, the system is correctly controlled. Note that this kind of problem is very close from undecidability, as proven in [CHR02] where the authors show that the question of determining whether there exists a discretized controler is undecidable for very simple specifications.

3. **Synthesis of distributed algorithms in perturbed models**
Implicated members: Jérémie Chalopin, Séverine Fratani, Nicolas Baudru
We are interested in finding general algorithms that enable to implement any distributed task. To do so, we will use the same approach as Yamashita and Kameda, Boldi and Vigna, and Chalopin, Godard and Métivier. We will start to study some classical distributed problems in models with perturbations. In [YK96a, BCG+96, CM07], the previously mentionned authors have studied the election problem in message passing systems where processes do not have unique ids. In these studies, they introduce combinatorial tools to express impossibility results and algorithmic tools to obtain specific distributed algorithms for the election problem. It turns out that in all these cases, these tools were powerful enough to express necessary and sufficient conditions a distributed task must fulfill to be computable in a message-passing system where processes do not have ids [YK96b,BV99,BV01,CGM08]. In all these cases, the given characterizations enable to transform a distributed decision problem (does there exist a distributed algorithm that solves this distributed task?) into a classical decision problem (do there exists computable functions that satisfy some particular properties?)
Note that in particular, using this approach, Boldi and Vigna [BV02] have been able to characterize problems that can be solved in a self-stabilizing way in synchronous message passing systems. In [CGM08], Chalopin, Godard and Métivier have characterized distributed tasks that can be computable in the asynchronous message passing model by distributed algorithms with a polynomial bit complexity (i.e., algorithms that exchange only a polynomial number of messages of polynomial size).

   We hope that the tools we will use and introduce for the study of basic distributed problems in perturbed models will also enable us to obtain more general results about what can be computed in these different models.

4. **Automata Theoretic Analysis**
Implicated members: Séverine Fratani, Peter Niebert, Pierre-Alain Reynier
When associating with a system a model of perturbations, it is possible to introduce different notions of robustness and/or robust language acceptance, for instance by requiring that a word is still accepted / rejected for any arbirarily small perturbation. It can be the case that such definitions lead to class of languages having better properties (recall the decidability property of lossy channel system). The first example on which we will work is the study of a good notion of robust acceptance for timed automata. This could be a way a class of timed languages with closed under complementation, determinization...

Risks:
The risks associated with this task are the usual risks associated with sicentific research, that is a wrong choice of scientific directives. This risk will be managed by scientific discussions and evaluations of progress planned in Task 0.

Deliverables:
We plan to produce two deliverables for this task. The first one, the intermediate report named Del 3.1, should be delivered after 24 months. The second one, the final report Del 3.2, should be delivered after 36 months.

3.3.5 TACHE 4 / TASK 4 : CASE STUDIES AND APPLICATIONS

Person in charge and involved members:
Jérémie Chalopin will be in charge of this task. Persons involved are, by order of implication, Jérémie Chalopin, Pierre-Alain Reynier, Séverine Fratani, the post-doctoral researcher and the PhD student.

Objectives:
In this tasks, our aim is twofold. First, at the beginning of the project, we will try to use case studies in existing models of perturbations/failures in order to evaluate these models. Second, at the end of the project, once eventually new models have been proposed, with corresponding algorithms and tools, we will validate our verification framework using our set of case studies.

Detailled program, methods, technical choices and solutions:

1. **Academic Case Studies**
   As explained in Task 2 (Models Evaluation and Proposals), we are interested in finding models that are expressive enough to model realistic systems. In order to evaluate these models, we want to establish a repository of problems that are representative of the different kinds of perturbations we consider. These problems can be seen as benchmarking problems that enable to give a hierarchy between the different models we consider.
   For example, in distributed computing, the consensus problem is a standard problem in order to evaluate the power of a model where faults can occur. When it is not assumed that processes have unique ids, the election problem is also a key problem to understand what kind of initial symmetries can be broken in the considered models.
   We are interested in identifying such key problems in order to evaluate the expressivity of existing and proposed models for the different kind of failures we will consider.
   This subtask is strongly related to Task 1 (Survey) and 2 (Models Evaluation and Proposals), since existing results will enable us to identify these key problems and since these case studies will help us to understand the expressivity power of the considered models. This subtask will be handled at the beginning of the project.

2. **Algorithms and Tools Evaluation**
   We are interested in using these identified problems in order to evaluate our algorithms and tools. We want to use these problems as benchmarks to compare our work with other existing algorithms and tools for both finite state and infinite state systems with perturbations.
   For example, we are interested in finding new techniques in order to be able to do model checking of classical distributed algorithms (with different levels perturbations). Heuristic algorithms may apply dedicated reduction techniques with respect to perturbations in a similar manner partial order reductions address redundancy due to interleaving: When considering distributed determinism, the set of possible executions is usually highly non deterministic and this leads to a

combinatorial explosion of the number of possible global states of the system to verify, but partial order methods can considerably reduce this redundancy in the models.
Likewise, we want to create case studies for the synthesis of robust controllers. One idea for benchmarks of this kind is to consider classical problems from control like the inverted pendulum balancing problem : An originally continuous problem is modeled in a discretized hybrid model which suffers from state explosion due to the discretization granularity. Such models are scalable in nature and naturally include the need for robust controllers since the systems are not known with absolute precision. They will represent a tough, scalable challenge to synthesis tools.

3. **Modelling Patterns**
Using the results obtained in Task 3 (Algorithmic and Decidability Issues), as well as expressiveness criteria defined using our academic case studies, we are interested in presenting a catalogue of modelization techniques. This set of modelizations can then be used to give some techniques to modelize real systems by theoretical models, depending on the properties of the system we are interested in.
Indeed, it may be difficult or impossible to have a correct modelization of a real system that preserves all its properties, and even when it is possible it may lead to highly costly algorithms and decision procedures. However, when focusing on some particular property of the model, we can have a partial modelization of the system that preserves this property and for which there exists some more efficient algorithms and decision procedures.

4. **Industrial requirements**
As we develop industrial relations, we will document actual needs as expressed by our partners. We do not expect to be able to handle industrial size case studies in the project, but this analysis will give a guideline in the conception of artificial case studies. From preliminary discussions, we know that problems related to perturbations are a very important topic to companies notably in the Pégase pole of competitivity. In the long run they may be interested by the use of formal methods in the certification process of robust controllers. Note that we have very recently realized a first attempt in this direction [CLRR08], by automatically synthesizing a controller robust to perturbations for an industrial case study provided by a company in the framework of the european research project Quasimodo.

Risks:
The case studies arising from industrial needs highly depend on the contact we have with our local partners and on their specific needs.

Delivrables:
We plan to produce three deliverables for this task. The first one, the report named Del 4.1 containing a description of the case studies, should be delivered after 12 months. The second one, the report Del 4.2 describing the evaluation of our tools and algorithms through case studues, should be delivered after 48 months. The third one, the report Del 4.3 describing our modelling patterns, should be delivered after 48 months.

3.3.6 TACHE 5 / TASK 5 : TOOLS

Person in charge and involved members:
The person in charge of this task will be Peter Niebert. Persons involved are, by order of implication, Peter Niebert, the post-doctoral researcher, the PhD student and Pierre-Alain

Reynier.

Objectives:
The global objective of this task is to develop prototype to mature implementations of the algorithms explored in Task 3. The aim is twofold, on the one hand to allow for practical assessment and evaluation of the algorithms with respect to the case studies, on the other hand to provide a platform allowing computer assisted exploration of the consequences of modeling with perturbations.

Detailled program, methods, technical choices and solutions:

The tool development will be based on a common platform, the POEM code base. POEM (Partial Order Environment of Marseille) has grown from a similar need for algorithm assessment and has been developed in the MoVe group under the direction of Peter Niebert since 2003. This choice has two advantages for the project : On the one hand, several participants and the PhD student candidate are already familiar with the architecture and programming of POEM, on the other hand, the plugin based architecture of POEM facilitates extension : There are plugins for input languages (currently : IF 2.0 and to some extent Promela, in the near future UppAal) and plugins for different analysis methods (currently classical model checking with extensions for timed automata and certain kinds or partial order reduction, as well as SAT based bounded model checking).

In an early stage, we will assess whether the perturbation models should be explicitely be represented by extensions to input languages, or whether it is possible to use standard input languages and have the perturbation models occurring only on the analysis level. This may depend on the type of perturbation (e.g. some channels may be lossy and other perfect). Based on this assessment, the languages will be extended and will give the framework for the formal definition of case studies.
In the main period (second and third year) of the project, algorithms emerging from Task 3 as well as certain algorithms from the literature will be implemented. It will be an important part of the post-doctoral student's work to participate in these developments in the second or third year. The PhD student will also participate in the development.

The third period (fourth year) will be used to stabilize and optimize the code.

This task has close links with Task 4 (case studies) with mutual feedback.

Risks:
Certain algorithms may not be straight forward to implement with the current internal model representation of POEM. Since POEM is locally developed, we can react to such situations by evolutionary changes to the data structures which might have implications on plugins not originally concerned by the project. Another risk concerns the workforce as development requires a high implication. As a consequence, tool development is subject to the help of the PhD student and the post-doctoral researcher.

Deliverables:
We plan to produce two deliverables for this task. The first one, the intermediate prototype named Del 5.1, should constitte a first outline of the tool that will be produced. It will present the difficulties encontered in the realization and the solutions choosen, leading to the global structure of the tool. It will be be delivered after 36 months. The second one, the final platform for experiments, named Del 5.2, should be delivered after 48 months.

3.3.7 TACHE 6 / TASK 6 : OVERALL EVALUATION

Person in charge : Pierre-Alain Reynier, involved members: *all*

Objectives:
The aim of this task is the auto assessment of the progress achieved in the project and an evaluation of prospects arising from it. It is the dual of the survey taking place in the first six months and it aims to establish a synthetic view of the project and the emerging prospectives in a comprehensive final report.

Detailled program:
The last six months of the project are concentrated on evaluation and for tasks 4 and 5 consolidation. As far as the project is concerned, there will be no investment in innovation in the tasks 1-5 in this period and the remaining period, with reduced effort is devoted to a synthetic analysis of the project. In a sense, this effort overlaps with all other tasks, except for the global perspective. In particular, we will analyse the successful and less successful aspects of our work and evaluate it in terms emerging scientific perspective and potential applications.

Methods, technical choices and solutions:
The different tasks 1 to 5 are cross reviewed by the participants less involved in them and discussed in several devoted seminars. In addition, an « Open ECSPER day » will be organised to which we will invite both scientific and industrial people external to the project and interested in the perturbations we work on. In particular we will try to attract representatives via the two relevant poles de compétitivité Pégase (Aviation) and SCS (Systèmes Communicants Sécurisés). The feedback of this open day will help in the analysis of post project opportunities.

Risks:
The general risk in management of scientific projects is accentuated in this task : some participants may lack motivation for sufficient implication in common tasks. The project management has to organise things in a way of making participation in this task attractive.

Deliverables:
ECSPER final report

3.4. CALENDRIER DES TACHES, LIVRABLES ET JALONS / PLANNING OF TASKS, DELIVERABLES AND MILESTONES

The planning of tasks, motivated in their presentation in previous subsection, is as depicted in Figure 2.

Concerning milestones, we have explained in Task 0 on coordination that we will have meetings every 6 months in order to evaluate the progress of the project. Moreover, we can note that every 12 months we have many deliverables, which will constitute an important milestone too.

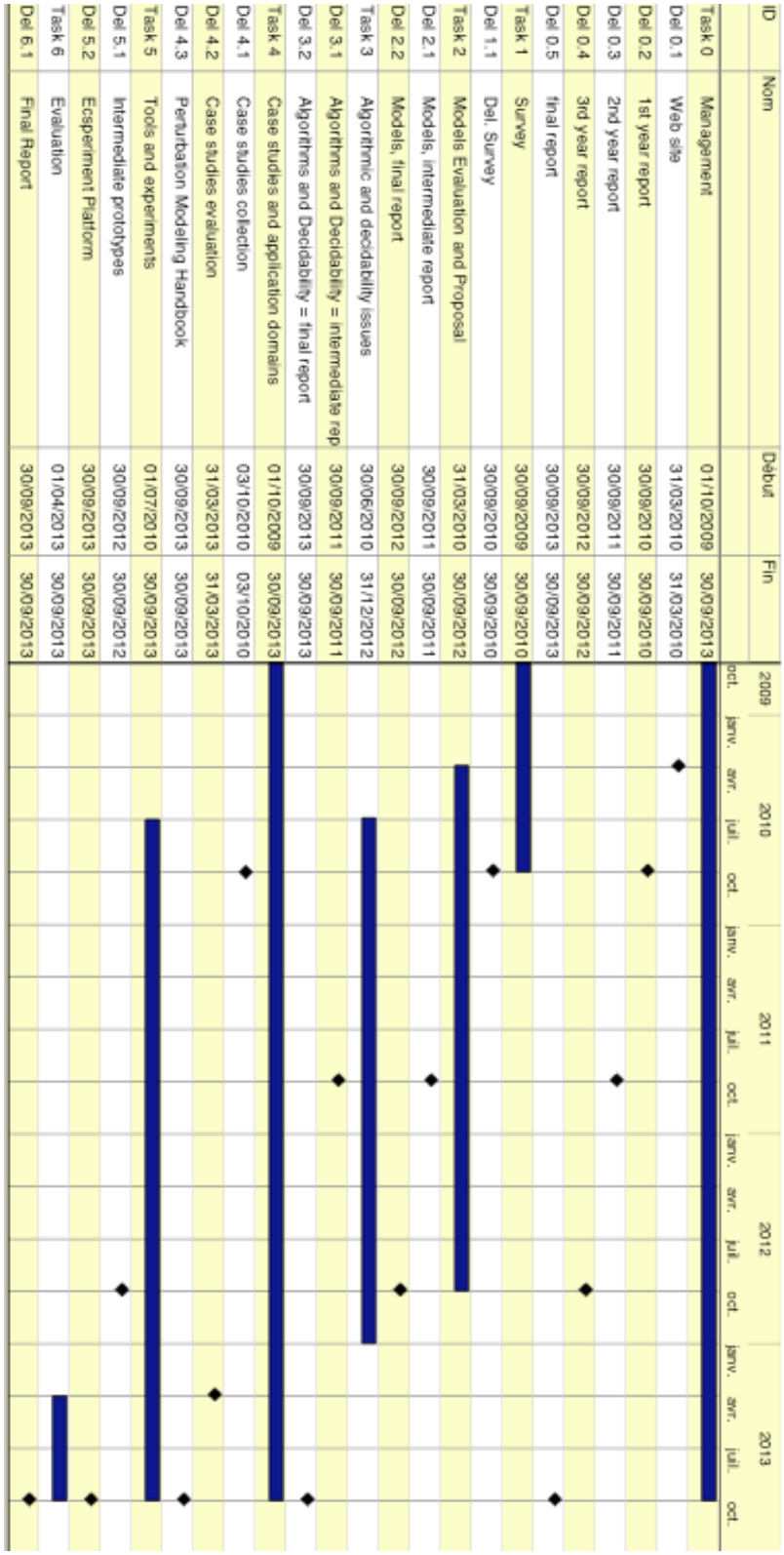

Figure 2 : Gantt diagram of the tasks.

4. STRATEGIE DE VALORISATION DES RESULTATS ET MODE DE PROTECTION ET D'EXPLOITATION DES RESULTATS / DATA MANAGEMENT, DATA SHARING, INTELLECTUAL PROPERTY AND RESULTS EXPLOITATION

General valorisation policy : The Université de Provence disposes of a Valorisation Service that sets the general guidelines for the protection and valorisation of intellectual property and technology transfer. The Laboratoire d'Informatique Fondamentale additionally disposes of a Valorisation Cell, which includes Pierre-Alain Reynier and Peter Niebert. The purpose of this cell is to improve the laboratory effort in technology transfer and industrial relations.

Scientific communication : The project will disseminate the produced knowledge by presentations and publications in international workshops, conferences and journals, as usual for basic research. The budget for missions reflects the ambition in this area : We need to provide ourselves the means of international visibility. Submitted articles will be registered in the HAL data base to ensure protection of innovation claims. HAL will also serve as a reference to the produced publications in the project with an integration into the ECSPER website.

Tool development : The tools developed at MoVe and in the ECSPER project (Task 5) are of academic level. We intend to publish versions of the tools under the CeCILL open source licence, which allows at the same time to arrouse interest in the academic community (and to obtain feedback from that community) and the University to keep the ownership of the original code for other forms of valorisation in the future.

Case studies : The case studies (Task 4) will be made available on the ECSPER website, in addition, the « Perturbation modeling handbook » (deliverable 4.3) will make these case studies and the overall approach of ECSPER accessible to a public larger than the academic community. The aim is to render the potential of the approach understandable both to scientists and engineers in the related domains.

Industrial relations : By all means, this project is fundamental research and immediate industrial exploitation is not on the agenda of ECSPER. However, we have started to develop industrial relations around the project with the prospect of future direct cooperation. In fact, the orientation of ECSPER on perturbations is linked to discussions we had with participants in the *Pégase* Pole of Competivity, notably with *NovaDem* (Meyreuil), a surprising startup in drones. A principle obstacle for the civil exploitation of drones (which is currently not legally possible) is safety. The prospect of being able to deal with perturbations in the validation of product specifications is of immediate interest to this industry. Our aim is to use ECSPER to further develop these relations and to prepare a project that will include industrial partners.

Open ECSPER day : An open seminar in the last year of ECSPER (explained in Task 6), is part of the valorisation strategy : At the same time, it will allow us to evaluate the results of the project and make our work known in related regional industries.

5. ORGANISATION DU PROJET / CONSORTIUM ORGANISATION AND DESCRIPTION

5.1. DESCRIPTION, ADÉQUATION ET COMPLÉMENTARITÉ DES PARTICIPANTS / RELEVANCE AND COMPLEMENTARITY OF THE PARTNERS WITHIN THE CONSORTIUM

The different members of the project are all members of the MoVe team of LIF, in Marseille. The recent arrival of Pierre-Alain Reynier in this team has been the source of several discussions and the opportunity to exhibit the common interest of these members in the study of perturbations. Indeed, most of the participants have already worked on that topic. More generally, the subject of the project is related to the application of formal methods for the verification of systems. This is the topic of the team MoVe of the LIF (MoVe stands for Modélisation et Vérification) and thus all the participants are experts in this area of computer science.

More precisely, the members of the project have different skills which will be complementary for the realization of the project. First, several areas of the thematics of the project are present in the team. Indeed, some are experts of model checking and control, others are experts of distributed algorithmics and others are experts of language theory and synthesis. Thus a very large scope of problems will be studied in the project. Second, an important knwoledge of models is also available in the team. Members are specialists of many extensions of finite state systems that will be focused on during the project. These models range from timed and hybrid systems to infinite state systems, passing through different models for distributed systems.

We detail now more precisely the individual skills.

Nicolas Baudru is an expert from analysis of distributed systems. He is interested in notions of concurrency and looks at questions of realizability, model-checking and controller synthesis. The models he looks at are, among others, message sequence charts, Petri nets and more generally message passing systems. These different skills explain the implication of Nicolas in the tasks related to message passing systems and to distributed systems. More precisely, he will play an important role for the study of models for message passing systems (Task 2.1) and for the definition of crossed models (Task 2.4) since we aim at looking at a combination of message passing systems with dense time variables. For the algorithmic part, he will be involved in the controller synthesis task (Task 3.2) and in the synthesis of distributed algorithms (Task 3.3).

Jérémie Chalopin is specialist from distributed computing and graph theory. He will thus naturally be implicated in tasks related to distributed aspects. More precisely, he will be the leader in the topics related to the synthesis of distributed algorithms (Task 3.3). Moreover, he will also be strongly implicated in the study of perturbations in message passing systems (Task 2.1). He is also very interested in enlarging his scope and aims at looking at drifts of variables, what motivates its participation to Task 2.2. Finally, since an important part of the case studies will be devoted to the study of academical case studies from distributed computing, he will be the leader of Task 4 on case studies.

Séverine Fratani has an important experience of infinite state systems, with questions related to model checking and language theory. More precisely, she studied during her PhD systems

with stacks, regarding decidability and language theoretical aspects. Then, she worked on dynamical structures with pointers with model checking objectives. She will be thus naturally be involved in Task 2.3 related to innovative perturbations models (such as for stack automata) and in Task 3.4 on language theoretical questions. Moreover, she is very interested in developing her knowledge in message passing systems and is thus also involved in Tasks 2.1 and 3.3. Finally, she will be in charge of Task 2 on Models.

Peter Niebert is an expert from algorithmical techniques for both timed systems and distributed systems, regarding model checking and control issues. He is specialist from symbolic and partial order techniques and in the development of efficient algorithms. He is also very interested in developing experimental platforms validating these algorithms, what he is doing now with the POEM platform. This is thus very naturally that he will be involved in Task 2.2 on clock drifts in timed systems and on model checking and controller synthesis questions (Tasks 3.1 and 3.2). Finally, he will of course be the responsible of Task 5 on Tool Development, since the development will be done in the framework of the POEM platform and will be involved in applications of the tool in Task 4 on case studies.

Pierre-Alain Reynier is specialist of timed and distributed systems, and has worked a lot on perturbations for these systems. He is interested in algorithmic problems such as model checking and controller synthesis, and in language theoretical questions. He will thus be involved in the corresponding tasks, namely Tasks 3.1, 3.2 and 3.4. As a consequence, he will be responsible of Task 3 on Algorithms. He will also be involved in tasks related to timed systems such as Tasks 2.2 (clock drifts), 2.3 (innovative perturbations models) and 2.4 (Crossed study). In addition, he disposes of an experience in tool developement, after a work in the well known tool UppAal, and in an industrial case study related to the theme of controller synthesis in presence of perturbations. Then, he will be implicated in Tasks 4 and 5 on case studies and tool development respectively. Finally, as he is the responsible of the project, he is in charge of Tasks 0 and 6.

We really believe that this large scope of competences is a great opportunity to have a broad view on systems with perturbations and that individual skills are very complementary for the project. Moreover, the connexions between the research thematics of the different members appear clearly in the project, and discussions and first collaborations have shown the many possible interactions between members, as described in the project.

5.2. QUALIFICATION DU PORTEUR DU PROJET / QUALIFICATION OF THE PRINCIPAL INVESTIGATOR

Though Pierre-Alain Reynier is a young researcher, he has already been involved in many research projects, whose sizes range from a national ACI research project to a european research project of the FP7 framework, as described on the following list :

- ACI Sécurité Informatique "CORTOS" : 2003-2006
- ANR Sécurité et Informatique "DOTS" : 2007-2010
- PAI "MOVES" (programme inter-universitaire belge) : 2007-2011
- IST FP7 Quasimodo : 2008-2010

He was highly implicated in these projects and participated to the redaction of activity reports and has thus a good knowledge of the management of projects. Moreover, he will also benefit from the experience of other members of the laboratory or even of the project, such as Denis Lugiez, Peter Niebert, who coordinated or participated in such projects.

5.3. QUALIFICATION, ROLE ET IMPLICATION DES PARTICIPANTS / CONTRIBUTION AND QUALIFICATION OF EACH PROJECT PARTICIPANT

	Nom	Prénom	Emploi actuel	Unité de rattachement et Lieu	Personne. mois	Rôle/Responsabilité dans le projet 4 lignes max
Coordinateur	REYNIER	Pierre-Alain	MCF	Université de Provence, LIF, Marseille	36 9/an 75%	Responsable des tâches 0 (Management), 3 (Algorithmes) et 6 (Evaluation). Spécialiste des systèmes temporisés. Encadrement du doctorant.
Autres membres	BAUDRU	Nicolas	MCF	Université de la Méditerranée, LIF, Marseille	24 6/an 50%	Responsable de la tâche 1 (Survey). Spécialiste des systèmes distribués comme les MSCs.
	CHALOPIN	Jérémie	CR2	CNRS, LIF, Marseille	16 4/an 33%	Responsable de la tâche 4 (Case Studies). Spécialiste des algorithmes distribués.
	FRATANI	Séverine	MCF	Université de Provence, LIF, Marseille	24 6/an 50%	Responsable de la tâche 2 (Models). Spécialiste des systèmes infinis comme les automates à piles, à pointeurs.
	NIEBERT	Peter	MCF	Université de Provence, LIF, Marseille	24 6/an 50%	Responsable de la tâche 5 (Tools). Spécialiste des systèmes temporisés, du développement de l'outil POEM.
TOTAL					124	

6. JUSTIFICATION SCIENTIFIQUE DES MOYENS DEMANDES / SCIENTIFIC JUSTIFICATION OF REQUESTED BUDGET

The submission document A presents the different elements of the budget of the project. Note that for evaluating the number of person months for each task of the project for the permanent memebers of the project, we used the total implication in terms of person months for the permament members, and the relative importance of each task in the whole project, as presented in the following table. This explains the fractions in the number of person months.

Task	Title	Relative weight
T0	Management	5%
T1	Survey	10%
T2	Models	25%
T3	Algorithms	25%
T4	Case Studies	15%

T5	Tools	15%
T6	Evaluation	5%
Total		100%

Table 2: Relative importance of the different taks.

Moreover, we used the estimations of salary proposed in the document given by the ANR to evaluate the cost for the (permanent ot not) staff for each task of the project.

Globally, including non permanent staff (52 person.months), we obtain 178 person.months for the four years of the project, which corresponds approximately to 3,7 full-time researchers per year. We use this approximation to evaluate further costs.

- *Équipement / Equipment*

None.

- *Personnel / Staff*

We ask for the realization of the project three non permanent employees: one PhD student (three years), one post-doctoral researcher (one year) and six months of allocations for master2 students internships. We detail the motivations for the three employees below.

PhD student.
The aim of the project, which is rather innovative, fits very well the perspective of a PhD thesis. There are basis to define, and the duration of the thesis allows such a relatively long development. Thus, we would like to hire a PhD student at the very beginning of the project, in order that he could work on the survey aspects, and then pursue on the different theoretical aspects of the project (models and algorithms for timed and message passing systems). We do not believe that he will be implied in all these topics, this is not realistic, but it will surely depend on his skils and aspirations. However, we will require from him to be strongly invovled in the tool development and the case studies.

More precisely, we have specified in submission document A its implication in the different tasks as follows : T1: 6 months, T2: 8 months, T3: 8 months, T4: 8 months and T5: 6 months.

Post-doctoral researcher.
As identified by the importance of the different tasks (Table 2), almost half of our work will be devoted to algorithms and tool development. Moreover these aspects will mainly be focused on during the second and third years of the project. This will thus be a period od high activity, and we would like to hire a post-doctoral researcher during this period, either on second or on third year depending on the candidates and on the advancement of the project. As explained before, the post-doctoral researcher would thus be concerned mainly by algorithms and implementation of these algorithms.

More precisely, we have specified in submission document A its implication in the different tasks as follows : T3: 6 months and T5: 6 months.

Master2 internships.

Finally, we believe that it is very important to attract to research master students as much as possible. Therefore, it is necessary to be able to provide financiary help to these students, which is evaluated to 400€ per month. There is no doubt that the project will be the opportunity to propose numerous internships for these students. We thus ask for 6 months of salaries, whih may be used for two periods of three months or aisngle one of six months, depending to the framewotk of internship.

More precisely, we have specified in submission document A the implication in the different tasks as follows : T4: 3 months and T5: 3 months.

- *Prestation de service externe / Subcontracting*

None.

- *Missions / Missions*

As for any fundamental research project, this is very important to have national and/or international relations and collaborations. Moreover, we also plan to go to international workshop and conferences to present our works and exchange with other researchers. Therefore, we need fundings for national and international travels.

Considering that a full-time researcher may have two international missions per year, or at least one plus national missions, we evalute the missions expenses to 3K€ per year and per full-time researcher. Together with the evaluation made above of of the workforce of 3,7 full-time researcher, this yields 45K€ for the full project.

In submission document A, we have distributed this amount on the different tasks.

- *Dépenses justifiées sur une procédure de facturation interne / Internal expenses*

None

- *Autres dépenses de fonctionnement / Other expenses*

First, we need personal computers for the different members of the project. We evaluate that the life-time of such a computer is of four years, and thus ask for 4 personal equipments (recall that there are in the project the equivalent of 3,7 full-time researchers per year). We evaluate the cost of such equipment to 2500€ (laptop plus external display).

In addition, we ask for a more powerful computer for experiments, whose cost is evaluated to 3K€.

These informations are summarized in table below:

Object	Quantity	Affectation	Unit cost	Total cost
Laptop Computers	4	Project members incuding PhD and post-doc students	2.5K	10K
Desktop Computer	1	Experiments	3K	3K

In submission document A, we have distributed these amounts on the tasks T1-T5.

Second, for teaching compensations, we ask, as specified in the document presenting rules of the "ANR JC" projects, an amount of 10K€ per year, yielding a sum of 40K€.

In submission document A, we have distributed these amounts on the different tasks.

Third, we have motivated in section 3.3.7 (description of Task 0) the interest of having the visit of external senior researchers for milestones meetings (every 6 months). We thus ask for 500€ for each visit, yielding an amount of 4000€. We have placed this amount in submission document A in Task 0.

Fourth, we have mentionned in the description of Task 6 on overall evaluation our objective to organize a one-day meeting on the ECSPER experience for our local industrial partners. We ask for this meeting a financiary help of 4K€, placed in line of Task 6 in document A.

7. ANNEXES

7.1. REFERENCES BIBLIOGRAPHIQUES / REFERENCES

[AB01] Eugene Asarin and Ahmed Bouajjani. Perturbed turing machines and hybrid systems. In *Proc. 16th Annual IEEE Symposium on Logic in Computer Science (LICS'01)*, pages 269–278. IEEE Computer Society, 2001.

[AD94] Rajeev Alur and David Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[AJ96a] Parosh Aziz Abdulla and Bengt Jonsson. Undecidable verification problems for programs with unreliable channels. *Information and Computation*, 130(1):71–90, 1996.

[AJ96b] Parosh Aziz Abdulla and Bengt Jonsson. Verifying programs with unreliable channels. *Information and Computation*, 127(2):91–101, 1996.

[AK95] Parosh Aziz Abdulla and Mats Kindahl. Decidability of simulation and bisimulation between lossy channel systems and finite state systems. In Lee and Smolka, editors, *Proc. CONCUR '95-6th Int. Conf. on Concurrency Theory*, volume 962 of *Lecture Notes in Computer Science*, pages 333–347. Springer Verlag, 1995.

[ALM05] Rajeev Alur, Salvatore La Torre, and P. Madhusudan. Perturbed timed automata. In *Proc. 8th Intl Workshop Hybrid Systems: Computation & Control (HSCC'05)*, volume 3414 of *LNCS*, pages 70–85. Springer, 2005.

[ASTY06] Manindra Agrawal, Frank Stephan, P. S. Thiagarajan, and Shaofa Yang. Behavioural approximations for restricted linear differential hybrid automata. In *Proc. 9th International Workshop on Computation and Control (HSCC'06)*, volume 3927 of *Lecture Notes in Computer Science*, pages 4–18. Springer, 2006.

[AT04] Manindra Agrawal and P. S. Thiagarajan. Lazy rectangular hybrid automata. In *Proc. 7th International Workshop on Computation and Control (HSCC'04)*, volume 2993 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2004.

[AT05] Manindra Agrawal and P. S. Thiagarajan. The discrete time behavior of lazy linear hybrid automata. In *Proc. 8th International Workshop on Computation and Control (HSCC'05)*, volume 3414 of *Lecture Notes in Computer Science*, pages 55–69. Springer, 2005.

[BCG+96] P. Boldi, B. Codenotti, P. Gemmell, S. Shammah, J. Simon, and S. Vigna. Symmetry breaking in anonymous networks: characterizations. In *Proc. of the 4th Israeli*

Symposium on Theory of Computing and Systems (ISTCS 1996), pages 16–26. IEEE Press, 1996.

[BD97] Michel Bidoit and Max Dauchet, editors. *TAPSOFT'97: Theory and Practice of Software Development, 7th International Joint Conference CAAP/FASE, Lille, France, April 14-18, 1997, Proceedings*, volume 1214 of *Lecture Notes in Computer Science*. Springer, 1997.

[BHH+04] Christel Baier, Boudewijn R. Haverkort, Holger Hermanns, Joost-Pieter Katoen, and Markus Siegle, editors. *Validation of Stochastic Systems - A Guide to Current Research*, volume 2925 of *Lecture Notes in Computer Science*. Springer, 2004.

[BMR06] Patricia Bouyer, Nicolas Markey, and Pierre-Alain Reynier. Robust model-checking of linear-time properties in timed automata. In *Proc. 7th Latin American Symposium on Theoretical Informatics (LATIN'06)*, volume 3887 of *Lecture Notes in Computer Science*, pages 238–249, Valdivia, Chile, 2006. Springer.

[BV99] P. Boldi and S. Vigna. Computing anonymously with arbitrary knowledge. In *Proc. of the 18th ACM Symposium on principles of distributed computing (PODC 1999)*, pages 181–188. ACM Press, 1999.

[BV01] P. Boldi and S. Vigna. An effective characterization of computability in anonymous networks. In *Proc. of Distributed Computing, 15th International Conference (DISC 2001)*, volume 2180 of *Lecture Notes in Computer Science*, pages 33–47. Springer-Verlag, 2001.

[BV02] P. Boldi and S. Vigna. Universal dynamic synchronous self-stabilization. *Distributed Computing*, 15(3):137–153, 2002.

[BZ83] Daniel Brand and Pitro Zafiropulo. On communicating finite-state machines. *J. ACM*, 30(2):323–342, 1983.

[CAMN04] Scott Cotton, Eugene Asarin, Oded Maler, and Peter Niebert. Some progress in satisfiability checking for difference logic. In *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems, Joint International Conferences on Formal Modelling and Analysis of Timed Systems, FORMATS 2004 and Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRTFT 2004, Grenoble, France*, pages 263–276, 2004.

[CF99] Flaviu Cristian and Christof Fetzer. The timed asynchronous distributed system model. *IEEE Trans. Parallel Distrib. Syst.*, 10(6):642–657, 1999.

[CFP96] Gérard Cécé, Alain Finkel, and S. Purushothaman Iyer. Unreliable channels are easier to verify than perfect channels. *Information and Computation*, 124(1):20–31, January 1996.

[CGM08] J. Chalopin, E. Godard, and Y. Métivier. Local terminations and distributed computability in anonymous networks. In *Proc. of Distributed Computing, 22nd International Symposium, DISC 2008*, volume 5218 of *Lecture Notes in Computer Science*, pages 47–62. Springer, 2008.

[CHP08] Krishnendu Chatterjee, Thomas A. Henzinger, and Vinayak S. Prabhu. Timed parity games: Complexity and robustness. In *6th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'08)*, volume 5215 of *Lecture Notes in Computer Science*, pages 124–140. Springer, 2008.

[CHR02] Franck Cassez, Thomas A. Henzinger, and Jean-François Raskin. A comparison of control problems for timed and hybrid systems. In *Proc. 5th International Workshop on Hybrid Systems: Computation and Control (HSCC'02)*, volume 2289 of *Lecture Notes in Computer Science*, pages 134–148. Springer, 2002.

[CLRR08] Franck Cassez, Kim G. Larsen, Jean-François Raskin, and Pierre-Alain Reynier. Automatic synthesis of robust and optimal controllers ? an industrial case study, 2008. Submitted to conference on Hybrid Systems Computation and Control, 2009.

[CM07] J. Chalopin and Y. Métivier. An efficient message passing election algorithm based on Mazurkiewicz's algorithm. *Fundamenta Informaticae*, 80(1–3):221–246, 2007.

[CS08] P. Chambart and Ph. Schnoebelen. Mixing lossy and perfect fifo channels. In *Proc. of Concurrency Theory, 19th International Conference, CONCUR 2008*, volume 5201 of *Lecture Notes in Computer Science*, pages 340–355. Springer, 2008.

[DDMR04] Martin De Wulf, Laurent Doyen, Nicolas Markey, and Jean-François Raskin. Robustness and implementability of timed automata. In *Proc. Joint Conference on*

Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant System (FORMATS+FTRTFT'04), volume 3253 of *Lecture Notes in Computer Science*, pages 118–133. Springer, 2004.

[DDR04] Martin De Wulf, Laurent Doyen, and Jean-François Raskin. Almost ASAP semantics: From timed models to timed implementations. In *Proc. 7th International Workshop on Hybrid Systems: Computation and Control (HSCC'04)*, volume 2993 of *Lecture Notes in Computer Science*, pages 296–310. Springer, 2004.

[DDR05a] Martin De Wulf, Laurent Doyen, and Jean-François Raskin. Almost asap semantics: from timed models to timed implementations. *Formal Aspects of Computing*, 17(3):319–341, 2005.

[DDR05b] Martin De Wulf, Martin Doyen, and Jean-François Raskin. Systematic implementation of real-time models. In *Proc. Formal Methods (FM'05)*, volume 3582 of *Lecture Notes in Computer Science*, pages 139–156. Springer, 2005.

[Dij74] E.W. Dijkstra. Self-stabilizing systems in spite of distributed control. *Commun. ACM*, 17(11):643–644, 1974.

[Dim07] Cătălin Dima. Dynamical properties of timed automata revisited. In *Proc. 5th Intl Conf, Formal Modeling and Analysis of Timed Systems (FORMATS'07)*, volume 4763 of *LNCS*, pages 130–146. Springer, 2007.

[DK06] Conrado Daws and Piotr Kordy. Symbolic robustness analysis of timed automata. In *Proc. 4th Intl Conf. Formal Modeling and Analysis of Timed Systems (FORMATS'06)*, volume 4202 of *LNCS*, pages 143–155. Springer, 2006.

[DKKS08] S. Dobrev, R. Kralovic, R. Královic, and N. Santoro. On fractional dynamic faults with thresholds. *Theor. Comput. Sci.*, 399(1–2):101–117, 2008.

[DKP08] S. Dobrev, R. Kralovic, and D. Pardubská. Leader election in extremely unreliable rings and complete networks. In *Proc. of the 12th International Conference on Principles of Distributed Systems (OPODIS 2008)*, Lecture Notes in Computer Science. Springer-Verlag, 2008.

[DL06] Stéphane Demri and Ranko Lazić. LTL with the freeze quantifier and register automata. In *Proc. of the 21st Annual IEEE Symposium on Logic in Computer Science (LICS'06)*, pages 17–26, Seattle, Washington, USA, 2006. IEEE Computer Society Press.

[Fin94] Alain Finkel. Decidability of the termination problem for completely specified protocols. *Distributed Computing*, 7(3):129–135, 1994.

[FLP85] M. J. Fischer, N. A. Lynch, and M. Paterson. Impossibility of distributed consensus with one faulty process. *J. ACM*, 32(2):374–382, 1985.

[Frä99] Martin Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In *Proc. 13th Int. Workshop on Computer Science Logic (CSL' 99)*, volume 1683 of *Lecture Notes in Computer Science*, pages 126–140. Springer, 1999.

[GHJ97] Vineet Gupta, Thomas A. Henzinger, and Radha Jagadeesan. Robust timed automata. In *Proc. Intl Workshop Hybrid and Real-Time Systems (HART'97)*, volume 1201 of *LNCS*, pages 331–345. Springer, 1997.

[HR00] Thomas A. Henzinger and Jean-François Raskin. Robust undecidability of timed and hybrid systems. In *Proc. 3rd International Workshop on Hybrid Systems: Computation and Control (HSCC'00)*, volume 1790 of *Lecture Notes in Computer Science*, pages 145–159. Springer, 2000.

[IN97] S. Purushothaman Iyer and Murali Narasimha. Probabilistic lossy channel systems. In Bidoit and Dauchet [BD97], pages 667–681.

[KNQV06] Marcos E. Kurbán, Peter Niebert, Hongyang Qu, and Walter Vogler. Stronger reduction criteria for Local First Search. In *Theoretical Aspects of Computing - ICTAC 2006, Third International Colloquium*, pages 108–122, 2006.

[LNZ05] Denis Lugiez, Peter Niebert, and Sarah Zennou. A partial order semantics approach to the clock explosion problem of timed automata. *Theor. Comput. Sci.*, 345(1):27–59, 2005.

[MS02] Benoît Masson and Ph. Schnoebelen. On verifying fair lossy channel systems. In *MFCS '02: Proceedings of the 27th International Symposium on Mathematical Foundations of Computer Science*, pages 543–555, London, UK, 2002. Springer-Verlag.

[NQ06] Peter Niebert and Hongyang Qu. The implementation of mazurkiewicz traces in POEM. In *Automated Technology for Verification and Analysis, 4th International Symposium, ATVA 2006, Beijing, China, October 23-26*, pages 508–522, 2006.

[OW03] Joël Ouaknine and James B. Worrell. Revisiting digitization, robustness and decidability for timed automata. In *Proc. 18th Annual Symposium on Logic in Computer Science (LICS'03)*. IEEE Computer Society Press, 2003.

[PP07] A. Pelc and D. Peleg. Feasibility and complexity of broadcasting with random transmission failures. *Theor. Comput. Sci.*, 370(1–3):279–292, 2007.

[Pur98] Anuj Puri. Dynamical properties of timed automata. In *Proc. 5th International Symposium on Formal techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'98)*, volume 1486 of *Lecture Notes in Computer Science*, pages 210–227. Springer, 1998.

[Sch04] Ph. Schnoebelen. The verification of probabilistic lossy channel systems. In Baier et al. [BHH+04], pages 445–466.

[SF07] Mani Swaminathan and Martin Fränzle. A symbolic decision procedure for robust safety of timed systems. In *Proc. 14th Intl Symp. Temporal Representation and Reasoning (TIME'07)*, page 192. IEEE Comp. Soc. Press, 2007.

[SFK08] Mani Swaminathan, Martin Fränzle, and Joost-Pieter Katoen. The surprising robustness of (closed) timed automata against clock-drift. In *Proc. Fifth IFIP International Conference On Theoretical Computer Science (TCS'08)*, volume 273 of *IFIP*, pages 537–553. Springer, 2008.

[YK96a] M. Yamashita and T. Kameda. Computing on anonymous networks: Part I - characterizing the solvable cases. *IEEE Transactions on parallel and distributed systems*, 7(1):69–89, 1996.

[YK96b] M. Yamashita and T. Kameda. Computing functions on asynchronous anonymous networks. *Math. Systems Theory*, 29(4):331–356, 1996.

7.2. BIOGRAPHIES / CV, RESUME

Pierre-Alain Reynier
28 years old
Maître de conférences à l'Université de Provence (Assistant Professor)

Cursus :

Since 09/2008 : Maître de conférences, Université de Provence. Member of the MoVe team of the LIF, UMR 6166.
2007/2008 : Post-doctoral student at ULB in the team " Méthodes Formelles et Vérification" of professor Raskin
2004/2007 : PhD in Computer Science at LSV, CNRS & ENS de Cachan.
Advisors : Patricia Bouyer et François Laroussinie.
Subject : Vérification de systèmes temporisés et distribués : modèles, algorithmes et implémentabilité.
2003/2004 : DEA Algorithmique (master degree), mention TB, rank 2/35.
2002/2003 : Agrégation de mathématiques, rang 47/330.
2001/2005 : Student of the ENS de Cachan, departements of mathematics and computer science.

Research Interests :

- Formal methods, verification, model-checking
- (Timed) Automata, (timed) Petri nets

- Concurrency, robustessness

Projects membership:
- ACI Sécurité Informatique "CORTOS", 2003-2006
- ANR Sécurité et Informatique "DOTS", 2007-2010
- PAI "MoVES", 2007-2011
- European FP7 Quasimodo : 2008-2010

Publications :

1. P. Bouyer, S. Haddad, and P.-A. Reynier. Timed Petri nets and timed automata : On the discriminating power of Zeno sequences. *Information and Computation*, 206(1) :73–107, 2008.

2. P. Bouyer, N. Markey, and P.-A. Reynier. Robust analysis of timed automata via channel machines. In *Proc. 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'08)*, vol. 4962 of *Lecture Notes in Computer Science*, pp. 157-171. Springer, 2008.

3. P. Bouyer, S. Haddad, and P.-A. Reynier. Timed unfoldings for networks of timed automata. In *Proc. 4th International Symposium on Automated Technology for Verification and Analysis (ATVA'06)*, vol. 4218 of *Lecture Notes in Computer Science*, pp. 292–306. Springer, 2006.

4. P. Bouyer, S. Haddad, and P.-A. Reynier. Timed Petri nets and timed automata : On the discriminating power of Zeno sequences. In *Proc. 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II*, vol. 4052 of *Lecture Notes in Computer Science*, pp. 420–431. Springer, 2006.

5. P. Bouyer, N. Markey, and P.-A. Reynier. Robust model-checking of linear-time properties in timed automata. In *Proc. 7th Latin American Symposium on Theoretical Informatics (LATIN'06)*, vol. 3887 of *Lecture Notes in Computer Science*, pp. 238–249. Springer, 2006.

Nicolas Baudru
28 years old
Maître de conférences à l'Université de la Méditerranée (Assistant Professor)

Cursus :
Since 09/2006: Maître de conférences, Université de la Méditerranée. Member of the MoVe team of the LIF, UMR 6166.
2005/2006 : ATER at Université de Provence
2002/2005 : Phd thesis in Computer science at LIF, CNRS & Université de Provence.
Adivsor : Rémi Morin
Subject : Syntèse d'automates synchrones et communicants.
2000/2002 : Master in Computer Science at Univeristé de Provence.

Research Interests :
- Formal methods, verification, realizability, model-checking
- Concurrency, partial order, traces, message sequence charts
- Concurrent automata, message passing systems

Participation à des projets :
- ANR SOAPDC

Publications :

1. Nicolas Baudru, Rémi Morin: Synthesis of Safe Message-Passing Systems. FSTTCS 2007: 277-289
2. Nicolas Baudru, Rémi Morin: Unfolding Synthesis of Asynchronous Automata. CSR 2006: 46-57
3. Nicolas Baudru, Rémi Morin: The Synthesis Problem of Netcharts. ICATPN 2006: 84-104
4. Nicolas Baudru, Rémi Morin: The Pros and Cons of Netcharts. CONCUR 2004: 99-114
5. Nicolas Baudru, Rémi Morin: Safe Implementability of Regular Message Sequence Chart Specifications. SNPD 2003: 210-217

Jérémie Chalopin
28 years old
Chargé de Recherches CNRS (Full time reasearcher)

Cursus :
Since 10/2007: Chargé de Recherches CNRS. Member of the research group MoVe at LIF, UMR 6166.
2003/2006 : PhD at LaBRI, Université Bordeaux 1,
Advisor: Yves Métivier.
Title : Algorithmique distribuée, calculs locaux et homomorphismes de graphes (Distributed Computing, local computations and graph homomorphisms)
2002/2003 : DEA Algorithmique (Master Degree), Université Paris 6, mention TB
2000/2002 : Licence and Maitrise d'Informatique (Bachelor Degree), ENS Lyon

Research Interests:

- Distributed Computing
- Graph Theory

Projects membership:

- ANR RIMEL, 2007-2009
- ANR SHAMAN, 2009-2012

Publications:
5 articles in international journals and 15 publications in international conferences proceedings. The most representative are the following:

1. J. Chalopin. Election and rendez-vous with incomparable labels. *Theoretical Computer Science*, 399(1–2):54–70, 2008
2. J. Chalopin, E. Godard et Y. Métivier. Local terminations and distributed computability in anonymous networks. In *Proc. of Distributed Computing, 22nd International Conference (DISC'08), LNCS* 5218, pp. 47-62, 2008
3. J. Chalopin et Y. Métivier. An efficient message passing election algorithm based on Mazurkiewicz's algorithm. *Fundamenta Informaticae*, 80(1–3):221–246, 2007
4. J. Chalopin, D. Gonçalves et P. Ochem. Planar graphs are in 1-string. In *Proc. of the*

18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'07), 2007, pp. 609-617, 2007

5. J. Chalopin, S. Das et N. Santoro. Groupings and pairings in anonymous networks. In *Proc. of Distributed Computing, 20th International Conference (DISC'06), LNCS 4167*, pp. 105–119, 2006

Séverine Fratani
32 years old
Maître de conférences à l'Université de Provence (Assistant professor)

Parcours :
Depuis 09/2007 : Maître de conférences, Université de Provence. Membre de l'équipe MoVe du LIF, UMR 6166.
2006/2007 : Post-doctorante au Laboratoire d'Informatique Algorithmique : Fondements et Applications (LIAFA UMR 7089 - CNRS). Equipe Modélisation et Vérification (MoVe). Stage effecté dans le cadre du projet RNTL Averiles
2005/2006 : ATER à l'université de Bordeaux, UFR Mathématiques et Informatique
2002/2005 : Thèse de doctorat au LaBRI (UMR 5800 CNRS).
Directeurs : Géraud Sénizergues et Frédérique Carrère.
Sujet : Automates à piles de piles... de piles.

Participation à des projets :
- Projet RNTL Games
- Projet RNTL Averiles

Publications majeures :

1. A. Bouajjani, S. Fratani, S. Qadeer. Bounded Context Switch Analysis of Multithreaded Programs with Dynamic Linked Structures. In Proc. Intern. Conf. on Computer Aided Verification (CAV'07).

2. S. Fratani, G. Sénizergues. Iterated pushdown automata and sequences of rational numbers. In Annals of Pure and Applied logic, Volume 141, Number 3, September 2006, p. 363-411.

3. Iterated pushdown automata and sequences of rational numbers. Second St. Petersburg Days of Logics and Computability. 2003, Saint-Petersbourg, Russie.

4. The theory of successor extended with several predicates. 11th Mons Days of Theoretical Computer Science. 2006, Rennes, France.

Peter Niebert
42 years
Maître de conférences à l'Université de Provence (Assistant Professor)

Scientific affiliations :
Since 01/09/2000 : Maître de conférences, Université de Provence, member of the MoVe group of LIF, UMR 6166.
1998/2000 : Post-doctorant à VERIMAG (Grenoble) dans l'équipe de Oded Mahler
1998 : Doctoral thesis in Hildesheim, Germany, supervisor : Ursula Goltz.

1992 : "Diplom-Informatiker" in Erlangen, Germany

Research topics :
Model-Checking and related algorithms, in particular with an accent on "partial orders", efficient implementation (POEM platform). Timed automata, and hybrid systems. Algorithms involving distributed observations. Temporal logics for distributed systems.

Project experience :
Participation in european projects : as postdoc near the project leader Oded Mahler of the IST project VHS (Verification of Hybrid Systems).
In Marseille, site coordinator of LIF participating in IST project AMETIST (Advanced Methods for Timed Systems).
Participant of ANR project SOAPDC.

Recent major publications :

1. Peter Niebert, Doron Peled, and Amir Pnueli. Discriminative model checking. In Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, NJ, USA, July 7-14, pages 504–516, 2008.
2. Peter Niebert and Hongyang Qu. The implementation of Mazurkiewicz traces in POEM. In Automated Technology for Verification and Analysis, 4th International Symposium, ATVA 2006, pages 508–522, 2006.
3. Marcos E. Kurban, Peter Niebert, Hongyang Qu, and Walter Vogler. Stronger reduction criteria for Local First Search. In Theoretical Aspects of Computing - ICTAC 2006, pages 108–122, 2006.
4. Peter Niebert and Doron Peled. Efficient model checking for LTL with partial order snapshots. In Tools and Algorithms for the Construction and Analysis of Systems, 12th International Conference, TACAS 2006, pages 272–286, 2006.
5. Denis Lugiez, Peter Niebert, and Sarah Zennou. A partial order semantics approach to the clock explosion problem of timed automata. Theor. Comput. Sci., 345(1):27–59, 2005.

7.3. IMPLICATION DES PERSONNES DANS D'AUTRES CONTRATS / INVOLVEMENT OF PROJECT PARTICPANTS TO OTHER GRANTS, CONTRACTS, ETC...

Part.	Nom de la personne participant au projet	Personne . mois	Intitulé de l'appel à projets Source de financement Montant attribué	Titre du projet	Nom du coordinateur	Date début & Date fin
N°	Jérémie Chalopin	5/an	ANR Verso 818 464€	SHAMAN	Sébastien Tixeuil	01/2009 01/2012