



IN PARTNERSHIP WITH:
CNRS

**Ecole normale supérieure de
Cachan**

Activity Report 2017

Project-Team MEXICO

Modeling and Exploitation of Interaction and Concurrency

IN COLLABORATION WITH: Laboratoire spécification et vérification (LSV)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Proofs and Verification

Table of contents

1. Personnel	1
2. Overall Objectives	2
2.1.1. Introduction	2
2.1.2. Concurrency	2
2.1.3. Interaction	3
2.1.4. Quantitative Features	3
2.1.5. Evolution and Perspectives	3
3. Research Program	3
3.1. Concurrency	3
3.1.1. Introduction	4
3.1.2. Diagnosis	4
3.1.2.1. Observability and Diagnosability	4
3.1.2.2. Distribution	4
3.1.3. Hybrid Systems	5
3.1.4. Contextual Nets	5
3.2. Management of Quantitative Behavior	6
3.2.1. Introduction	6
3.2.2. Probabilistic distributed Systems	6
3.2.2.1. Non-sequential probabilistic processes	6
3.2.2.2. Distributed Markov Decision Processes	7
3.2.3. Large scale probabilistic systems	7
3.2.4. Real time distributed systems	7
4. Application Domains	8
4.1. Telecommunications	8
4.2. Biological Systems	8
4.3. Autonomous Vehicles	9
5. Highlights of the Year	9
6. New Software and Platforms	10
6.1. COSMOS	10
6.2. CosyVerif	10
6.3. Mole	10
7. New Results	10
7.1. Optimal constructions for active diagnosis	10
7.2. Diagnosability of Repairable Faults	11
7.3. Diagnostic et contrôle de la dégradation des systèmes probabilistes	11
7.4. The Complexity of Diagnosability and Opacity Verification for Petri Nets	11
7.5. Probabilistic Disclosure: Maximisation vs. Minimisation	11
7.6. D-SPACES: Implementing Declarative Semantics for Spatially Structured Information	12
7.7. Unbounded product-form Petri nets	12
7.8. Statistical Model-Checking for Autonomous Vehicle Safety Validation	12
7.9. Une sémantique formelle pour les modèles Simulink	13
7.10. The Logical View on Continuous Petri Nets	13
7.11. Memoryless Determinacy of Finite Parity Games: Another Simple Proof	13
7.12. Interval iteration algorithm for MDPs and IMDPs	13
7.13. Alignment-Based Trace Clustering	14
7.14. Aligning Modeled and Observed Behavior: A Compromise Between Complexity and Quality	14
7.15. Temporal Reprogramming of Boolean Networks	14
7.16. Goal-Driven Unfolding of Petri Nets	15

7.17.	Euler's Method Applied to the Control of Switched Systems	15
7.18.	An Improved Algorithm for the Control Synthesis of Nonlinear Sampled Switched Systems	15
7.19.	Distributed Control Synthesis Using Euler's Method	15
7.20.	Control Synthesis of Nonlinear Sampled Switched Systems using Euler's Method	16
7.21.	Metastability-Aware Memory-Efficient Time-to-Digital Converter	16
7.22.	Brief Announcement: Lower Bounds for Asymptotic Consensus in Dynamic Networks	16
7.23.	Metastability Tolerant Computing	16
8.	Partnerships and Cooperations	17
8.1.	National Initiatives	17
8.2.	International Initiatives	17
8.3.	International Research Visitors	17
8.3.1.	Visits of International Scientists	17
8.3.2.	Visits to International Teams	17
9.	Dissemination	17
9.1.	Promoting Scientific Activities	17
9.1.1.	Scientific Events Organisation	17
9.1.2.	Scientific Events Selection	18
9.1.2.1.	Member of the Conference Program Committees	18
9.1.2.2.	Reviewer	18
9.1.3.	Journal	18
9.1.3.1.	Member of the Editorial Boards	18
9.1.3.2.	Reviewer - Reviewing Activities	18
9.1.4.	Invited Talks	18
9.1.5.	Scientific Expertise	19
9.1.6.	Research Administration	19
9.2.	Teaching - Supervision - Juries	19
9.2.1.	Teaching	19
9.2.2.	Supervision	19
9.2.3.	Juries	20
10.	Bibliography	20

Project-Team MEXICO

Creation of the Team: 2009 March 01, updated into Project-Team: 2011 January 01

Keywords:

Computer Science and Digital Science:

- A6.4.1. - Deterministic control
- A6.4.3. - Observability and Controlability
- A7.1. - Algorithms
- A7.2. - Logic in Computer Science
- A8.1. - Discrete mathematics, combinatorics
- A8.2. - Optimization
- A8.7. - Graph theory
- A8.8. - Network science
- A8.9. - Performance evaluation

Other Research Topics and Application Domains:

- B1.1.2. - Molecular biology
- B1.1.3. - Cellular biology
- B1.1.11. - Systems biology
- B1.1.12. - Synthetic biology
- B6.3.1. - Web
- B6.3.2. - Network protocols
- B6.3.3. - Network Management
- B7.1. - Traffic management
- B7.2.1. - Smart vehicles

1. Personnel

Research Scientists

- Stefan Haar [Team leader, Inria, Senior Researcher, HDR]
- Beatrice Berard [Univ Denis Diderot Paris, Senior Researcher, until Aug 2017]
- Laurent Fribourg [CNRS, Senior Researcher, HDR]
- Matthias Fuegger [CNRS, Researcher]

Faculty Members

- Thomas Chatain [Ecole Normale Supérieure Paris-Saclay, Associate Professor, HDR]
- Serge Haddad [Ecole Normale Supérieure Paris-Saclay, Professor, HDR]
- Claudine Picaronny [Ecole Normale Supérieure Paris-Saclay, Associate Professor]
- Stefan Schwoon [Ecole Normale Supérieure Paris-Saclay, Associate Professor, HDR]

PhD Students

- Yann Duploux [Institut de recherche technologique System X]
- Juraj Kolcak [Inria, from Mar 2017]
- Hugues Mandon [Inria]
- Adnane Saoud [CNRS]

Intern

- Aalok Thakkar [Inria, from May 2017 until Jul 2017]

Administrative Assistants

Thida Iem [Inria, until Sep 2017]

Emmanuelle Perrot [Inria, since Oct 2017]

External Collaborator

Benoît Barbot [Univ Paris-Est Marne La Vallée]

2. Overall Objectives

2.1. Scientific Objectives

2.1.1. Introduction

In the increasingly networked world, reliability of applications becomes ever more critical as the number of users of, e.g., communication systems, web services, transportation etc., grows steadily. Management of networked systems, in a very general sense of the term, therefore is a crucial task, but also a difficult one.

MEXiCo strives to take advantage of distribution by orchestrating cooperation between different agents that observe local subsystems, and interact in a localized fashion.

The need for applying formal methods in the analysis and management of complex systems has long been recognized. It is with much less unanimity that the scientific community embraces methods based on asynchronous and distributed models. Centralized and sequential modeling still prevails.

However, we observe that crucial applications have increasing numbers of users, that networks providing services grow fast both in the number of participants and the physical size and degree of spatial distribution. Moreover, traditional *isolated* and *proprietary* software products for local systems are no longer typical for emerging applications.

In contrast to traditional centralized and sequential machinery for which purely functional specifications are efficient, we have to account for applications being provided from diverse and non-coordinated sources. Their distribution (e.g. over the Web) must change the way we verify and manage them. In particular, one cannot ignore the impact of quantitative features such as delays or failure likelihoods on the functionalities of composite services in distributed systems.

We thus identify three main characteristics of complex distributed systems that constitute research challenges:

- *Concurrency* of behavior;
- *Interaction* of diverse and semi-transparent components; and
- management of *Quantitative* aspects of behavior.

2.1.2. Concurrency

The increasing size and the networked nature of communication systems, controls, distributed services, etc. confront us with an ever higher degree of parallelism between local processes. This field of application for our work includes telecommunication systems and composite web services. The challenge is to provide sound theoretical foundations and efficient algorithms for management of such systems, ranging from controller synthesis and fault diagnosis to integration and adaptation. While these tasks have received considerable attention in the *sequential* setting, managing *non-sequential* behavior requires profound modifications for existing approaches, and often the development of new approaches altogether. We see concurrency in distributed systems as an opportunity rather than a nuisance. Our goal is to *exploit* asynchronicity and distribution as an advantage. Clever use of adequate models, in particular *partial order semantics* (ranging from Mazurkiewicz traces to event structures to MSCs) actually helps in practice. In fact, the partial order vision allows us to make causal precedence relations explicit, and to perform diagnosis and test for the dependency between events. This is a conceptual advantage that interleaving-based approaches cannot match. The two key features of our work will be *(i)* the exploitation of concurrency by using asynchronous models with partial order semantics, and *(ii)* distribution of the agents performing management tasks.

2.1.3. Interaction

Systems and services exhibit non-trivial *interaction* between specialized and heterogeneous components. A coordinated interplay of several components is required; this is challenging since each of them has only a limited, partial view of the system's configuration. We refer to this problem as *distributed synthesis* or *distributed control*. An aggravating factor is that the structure of a component might be semi-transparent, which requires a form of *grey box management*.

2.1.4. Quantitative Features

Besides the logical functionalities of programs, the *quantitative* aspects of component behavior and interaction play an increasingly important role.

- *Real-time* properties cannot be neglected even if time is not an explicit functional issue, since transmission delays, parallelism, etc, can lead to time-outs striking, and thus change even the logical course of processes. Again, this phenomenon arises in telecommunications and web services, but also in transport systems.
- In the same contexts, *probabilities* need to be taken into account, for many diverse reasons such as unpredictable functionalities, or because the outcome of a computation may be governed by race conditions.
- Last but not least, constraints on *cost* cannot be ignored, be it in terms of money or any other limited resource, such as memory space or available CPU time.

2.1.5. Evolution and Perspectives

Since the creation of *MExICo*, the weight of *quantitative* aspects in all parts of our activities has grown, be it in terms of the models considered (weighted automata and logics), be it in transforming verification or diagnosis verdict into probabilistic statements (probabilistic diagnosis, statistical model checking), or within the recently started SystemX cooperation on supervision in multi-modal transport systems. This trend is certain to continue over the next couple of years, along with the growing importance of diagnosis and control issues.

In another development, the theory and use of partial order semantics has gained momentum in the past four years, and we intend to further strengthen our efforts and contacts in this domain to further develop and apply partial-order based deduction methods.

As concerns the study of interaction, our progress has been thus far less in the domain of *distributed* approaches than in the analysis of *system composition*, such as in networks of untimed or timed automata. While continuing this line of study, we also intend to turn more strongly towards distributed *algorithms*, namely in terms of parametrized verification methods.

3. Research Program

3.1. Concurrency

Participants: Thomas Chatain, Stefan Haar, Serge Haddad, Stefan Schwoon.

Concurrency; Semantics; Automatic Control ; Diagnosis ; Verification

Concurrency: Property of systems allowing some interacting processes to be executed in parallel.

Diagnosis: The process of deducing from a partial observation of a system aspects of the internal states or events of that system; in particular, *fault diagnosis* aims at determining whether or not some non-observable fault event has occurred.

Conformance Testing: Feeding dedicated input into an implemented system *IS* and deducing, from the resulting output of *I*, whether *I* respects a formal specification *S*.

3.1.1. Introduction

It is well known that, whatever the intended form of analysis or control, a *global* view of the system state leads to overwhelming numbers of states and transitions, thus slowing down algorithms that need to explore the state space. Worse yet, it often blurs the mechanics that are at work rather than exhibiting them. Conversely, respecting concurrency relations avoids exhaustive enumeration of interleavings. It allows us to focus on ‘essential’ properties of non-sequential processes, which are expressible with causal precedence relations. These precedence relations are usually called causal (partial) orders. Concurrency is the explicit absence of such a precedence between actions that do not have to wait for one another. Both causal orders and concurrency are in fact essential elements of a specification. This is especially true when the specification is constructed in a distributed and modular way. Making these ordering relations explicit requires to leave the framework of state/interleaving based semantics. Therefore, we need to develop new dedicated algorithms for tasks such as conformance testing, fault diagnosis, or control for distributed discrete systems. Existing solutions for these problems often rely on centralized sequential models which do not scale up well.

3.1.2. Diagnosis

Participants: Stefan Haar, Serge Haddad, Stefan Schwoon.

Fault Diagnosis for discrete event systems is a crucial task in automatic control. Our focus is on *event oriented* (as opposed to *state oriented*) model-based diagnosis, asking e.g. the following questions: given a - potentially large - *alarm pattern* formed of observations,

- what are the possible *fault scenarios* in the system that *explain* the pattern ?
- Based on the observations, can we deduce whether or not a certain - invisible - fault has actually occurred ?

Model-based diagnosis starts from a discrete event model of the observed system - or rather, its relevant aspects, such as possible fault propagations, abstracting away other dimensions. From this model, an extraction or unfolding process, guided by the observation, produces recursively the explanation candidates.

In asynchronous partial-order based diagnosis with Petri nets [40], [41], [42], one unfolds the *labelled product* of a Petri net model \mathcal{N} and an observed alarm pattern \mathcal{A} , also in Petri net form. We obtain an acyclic net giving partial order representation of the behaviors compatible with the alarm pattern. A recursive online procedure filters out those runs (*configurations*) that explain *exactly* \mathcal{A} . The Petri-net based approach generalizes to dynamically evolving topologies, in dynamical systems modeled by graph grammars, see [29]

3.1.2.1. Observability and Diagnosability

Diagnosis algorithms have to operate in contexts with low observability, i.e., in systems where many events are invisible to the supervisor. Checking *observability* and *diagnosability* for the supervised systems is therefore a crucial and non-trivial task in its own right. Analysis of the relational structure of occurrence nets allows us to check whether the system exhibits sufficient visibility to allow diagnosis. Developing efficient methods for both verification of *diagnosability checking* under concurrency, and the *diagnosis* itself for distributed, composite and asynchronous systems, is an important field for *MExCo*.

3.1.2.2. Distribution

Distributed computation of unfoldings allows one to factor the unfolding of the global system into smaller *local* unfoldings, by local supervisors associated with sub-networks and communicating among each other. In [41], [31], elements of a methodology for distributed computation of unfoldings between several supervisors, underwritten by algebraic properties of the category of Petri nets have been developed. Generalizations, in particular to Graph Grammars, are still to be done.

Computing diagnosis in a distributed way is only one aspect of a much vaster topic, that of *distributed diagnosis* (see [38], [44]). In fact, it involves a more abstract and often indirect reasoning to conclude whether or not some given invisible fault has occurred. Combination of local scenarios is in general not sufficient: the global system may have behaviors that do not reveal themselves as faulty (or, dually, non-faulty) on any local supervisor's domain (compare [28], [34]). Rather, the local diagnosers have to join all *information* that is available to them locally, and then deduce collectively further information from the combination of their views. In particular, even the *absence* of fault evidence on all peers may allow to deduce fault occurrence jointly, see [46], [47]. Automating such procedures for the supervision and management of distributed and locally monitored asynchronous systems is a long-term goal to which *MExICo* hopes to contribute.

3.1.3. Hybrid Systems

Participants: Laurent Fribourg, Serge Haddad.

Hybrid systems constitute a model for cyber-physical systems which integrates continuous-time dynamics (modes) governed by differential equations, and discrete transitions which switch instantaneously from one mode to another. Thanks to their ease of programming, hybrid systems have been integrated to power electronics systems, and more generally in cyber-physical systems. In order to guarantee that such systems meet their specifications, classical methods consist in finitely abstracting the systems by discretization of the (infinite) state space, and deriving automatically the appropriate mode control from the specification using standard graph techniques. These methods face the well-known problem of “curse of dimensionality”, and cannot generally treat systems of dimension exceeding 5 or 6. Thanks to the introduction of original compositional techniques [22] as well as finer estimations of integration errors [21], we are now able to control several case studies of greater dimension. Actually, in the real world, many parameters of hybrid models are not known precisely, and require adjustments to experimental data. We plan to elaborate methods based on parameter estimation and machine learning techniques in order to define formal stability criteria and well-posed learning problems in the framework of hybrid systems with nonlinear dynamics.

3.1.4. Contextual Nets

Participant: Stefan Schwoon.

Assuring the correctness of concurrent systems is notoriously difficult due to the many unforeseeable ways in which the components may interact and the resulting state-space explosion. A well-established approach to alleviate this problem is to model concurrent systems as Petri nets and analyse their unfoldings, essentially an acyclic version of the Petri net whose simpler structure permits easier analysis [39].

However, Petri nets are inadequate to model concurrent read accesses to the same resource. Such situations often arise naturally, for instance in concurrent databases or in asynchronous circuits. The encoding tricks typically used to model these cases in Petri nets make the unfolding technique inefficient. Contextual nets, which explicitly do model concurrent read accesses, address this problem. Their accurate representation of concurrency makes contextual unfoldings up to exponentially smaller in certain situations. An abstract algorithm for contextual unfoldings was first given in [30]. In recent work, we further studied this subject from a theoretical and practical perspective, allowing us to develop concrete, efficient data structures and algorithms and a tool (Cunf) that improves upon existing state of the art. This work led to the PhD thesis of César Rodríguez in 2014 .

Contextual unfoldings deal well with two sources of state-space explosion: concurrency and shared resources. Recently, we proposed an improved data structure, called *contextual merged processes* (CMP) to deal with a third source of state-space explosion, i.e. sequences of choices. The work on CMP [48] is currently at an abstract level. In the short term, we want to put this work into practice, requiring some theoretical groundwork, as well as programming and experimentation.

Another well-known approach to verifying concurrent systems is *partial-order reduction*, exemplified by the tool SPIN. Although it is known that both partial-order reduction and unfoldings have their respective strengths and weaknesses, we are not aware of any conclusive comparison between the two techniques. Spin comes with a high-level modeling language having an explicit notion of processes, communication channels, and variables.

Indeed, the reduction techniques implemented in Spin exploit the specific properties of these features. On the other side, while there exist highly efficient tools for unfoldings, Petri nets are a relatively general low-level formalism, so these techniques do not exploit properties of higher language features. Our work on contextual unfoldings and CMPs represents a first step to make unfoldings exploit richer models. In the long run, we wish raise the unfolding technique to a suitable high-level modelling language and develop appropriate tool support.

3.2. Management of Quantitative Behavior

Participants: Thomas Chatain, Stefan Haar, Serge Haddad.

3.2.1. Introduction

Besides the logical functionalities of programs, the *quantitative* aspects of component behavior and interaction play an increasingly important role.

- *Real-time* properties cannot be neglected even if time is not an explicit functional issue, since transmission delays, parallelism, etc, can lead to time-outs striking, and thus change even the logical course of processes. Again, this phenomenon arises in telecommunications and web services, but also in transport systems.
- In the same contexts, *probabilities* need to be taken into account, for many diverse reasons such as unpredictable functionalities, or because the outcome of a computation may be governed by race conditions.
- Last but not least, constraints on *cost* cannot be ignored, be it in terms of money or any other limited resource, such as memory space or available CPU time.

Traditional mainframe systems were proprietary and (essentially) localized; therefore, impact of delays, unforeseen failures, etc. could be considered under the control of the system manager. It was therefore natural, in verification and control of systems, to focus on *functional* behavior entirely.

With the increase in size of computing system and the growing degree of compositionality and distribution, quantitative factors enter the stage:

- calling remote services and transmitting data over the web creates *delays*;
- remote or non-proprietary components are not “deterministic”, in the sense that their behavior is uncertain.

Time and *probability* are thus parameters that management of distributed systems must be able to handle; along with both, the *cost* of operations is often subject to restrictions, or its minimization is at least desired. The mathematical treatment of these features in distributed systems is an important challenge, which *MExiCo* is addressing; the following describes our activities concerning probabilistic and timed systems. Note that cost optimization is not a current activity but enters the picture in several intended activities.

3.2.2. Probabilistic distributed Systems

Participants: Stefan Haar, Serge Haddad, Claudine Picaronny.

3.2.2.1. Non-sequential probabilistic processes

Practical fault diagnosis requires to select explanations of *maximal likelihood*. For partial-order based diagnosis, this leads therefore to the question what the probability of a given partially ordered execution is. In Benveniste et al. [33], [26], we presented a model of stochastic processes, whose trajectories are partially ordered, based on local branching in Petri net unfoldings; an alternative and complementary model based on Markov fields is developed in [43], which takes a different view on the semantics and overcomes the first model’s restrictions on applicability.

Both approaches abstract away from real time progress and randomize choices in *logical* time. On the other hand, the relative speed - and thus, indirectly, the real-time behavior of the system’s local processes - are crucial factors determining the outcome of probabilistic choices, even if non-determinism is absent from the system.

In another line of research [35] we have studied the likelihood of occurrence of non-sequential runs under random durations in a stochastic Petri net setting. It remains to better understand the properties of the probability measures thus obtained, to relate them with the models in logical time, and exploit them e.g. in *diagnosis*.

3.2.2.2. *Distributed Markov Decision Processes*

Participant: Serge Haddad.

Distributed systems featuring non-deterministic and probabilistic aspects are usually hard to analyze and, more specifically, to optimize. Furthermore, high complexity theoretical lower bounds have been established for models like partially observed Markovian decision processes and distributed partially observed Markovian decision processes. We believe that these negative results are consequences of the choice of the models rather than the intrinsic complexity of problems to be solved. Thus we plan to introduce new models in which the associated optimization problems can be solved in a more efficient way. More precisely, we start by studying connection protocols weighted by costs and we look for online and offline strategies for optimizing the mean cost to achieve the protocol. We have been cooperating on this subject with the SUMO team at Inria Rennes; in the joint work [27]; there, we strive to synthesize for a given MDP a control so as to guarantee a specific stationary behavior, rather than - as is usually done - so as to maximize some reward.

3.2.3. *Large scale probabilistic systems*

Addressing large-scale probabilistic systems requires to face state explosion, due to both the discrete part and the probabilistic part of the model. In order to deal with such systems, different approaches have been proposed:

- Restricting the synchronization between the components as in queuing networks allows to express the steady-state distribution of the model by an analytical formula called a product-form [32].
- Some methods that tackle with the combinatory explosion for discrete-event systems can be generalized to stochastic systems using an appropriate theory. For instance symmetry based methods have been generalized to stochastic systems with the help of aggregation theory [37].
- At last simulation, which works as soon as a stochastic operational semantic is defined, has been adapted to perform statistical model checking. Roughly speaking, it consists to produce a confidence interval for the probability that a random path fulfills a formula of some temporal logic [49].

We want to contribute to these three axes: (1) we are looking for product-forms related to systems where synchronization are more involved (like in Petri nets), see [2]; (2) we want to adapt methods for discrete-event systems that require some theoretical developments in the stochastic framework and, (3) we plan to address some important limitations of statistical model checking like the expressiveness of the associated logic and the handling of rare events.

3.2.4. *Real time distributed systems*

Nowadays, software systems largely depend on complex timing constraints and usually consist of many interacting local components. Among them, railway crossings, traffic control units, mobile phones, computer servers, and many more safety-critical systems are subject to particular quality standards. It is therefore becoming increasingly important to look at networks of timed systems, which allow real-time systems to operate in a distributed manner.

Timed automata are a well-studied formalism to describe reactive systems that come with timing constraints. For modeling distributed real-time systems, networks of timed automata have been considered, where the local clocks of the processes usually evolve at the same rate [45] [36]. It is, however, not always adequate to assume that distributed components of a system obey a global time. Actually, there is generally no reason to assume that different timed systems in the networks refer to the same time or evolve at the same rate. Any component is rather determined by local influences such as temperature and workload.

3.2.4.1. *Implementation of Real-Time Concurrent Systems*

Participants: Thomas Chatain, Stefan Haar, Serge Haddad.

This was one of the tasks of the ANR ImpRo.

Formal models for real-time systems, like timed automata and time Petri nets, have been extensively studied and have proved their interest for the verification of real-time systems. On the other hand, the question of using these models as specifications for designing real-time systems raises some difficulties. One of those comes from the fact that the real-time constraints introduce some artifacts and because of them some syntactically correct models have a formal semantics that is clearly unrealistic. One famous situation is the case of Zeno executions, where the formal semantics allows the system to do infinitely many actions in finite time. But there are other problems, and some of them are related to the distributed nature of the system. These are the ones we address here.

One approach to implementability problems is to formalize either syntactical or behavioral requirements about what should be considered as a reasonable model, and reject other models. Another approach is to adapt the formal semantics such that only realistic behaviors are considered.

These techniques are preliminaries for dealing with the problem of implementability of models. Indeed implementing a model may be possible at the cost of some transformation, which make it suitable for the target device. By the way these transformations may be of interest for the designer who can now use high-level features in a model of a system or protocol, and rely on the transformation to make it implementable.

We aim at formalizing and automating translations that preserve both the timed semantics and the concurrent semantics. This effort is crucial for extending concurrency-oriented methods for logical time, in particular for exploiting partial order properties. In fact, validation and management - in a broad sense - of distributed systems is not realistic *in general* without understanding and control of their real-time dependent features; the link between real-time and logical-time behaviors is thus crucial for many aspects of *MExiCo*'s work.

4. Application Domains

4.1. Telecommunications

Participants: Stefan Haar, Serge Haddad.

Telecommunications

MExiCo's research is motivated by problems of system management in several domains, such as:

- In the domain of service oriented computing, it is often necessary to insert some Web service into an existing orchestrated business process, e.g. to replace another component after failures. This requires to ensure, often actively, conformance to the interaction protocol. One therefore needs to synthesize adaptators for every component in order to steer its interaction with the surrounding processes.
- Still in the domain of telecommunications, the supervision of a network tends to move from out-of-band technology, with a fixed dedicated supervision infrastructure, to in-band supervision where the supervision process uses the supervised network itself. This new setting requires to revisit the existing supervision techniques using control and diagnosis tools.

Currently, we have no active cooperation on these subjects.

4.2. Biological Systems

Participants: Thomas Chatain, Stefan Haar, Serge Haddad, Stefan Schwoon.

We have begun in 2014 to examine concurrency issues in systems biology, and are currently enlarging the scope of our research's applications in this direction. To see the context, note that in recent years, a considerable shift of biologists' interest can be observed, from the mapping of static genotypes to gene expression, i.e. the processes in which genetic information is used in producing functional products. These processes are far from being uniquely determined by the gene itself, or even jointly with static properties of the environment; rather, regulation occurs throughout the expression processes, with specific mechanisms increasing or decreasing the production of various products, and thus modulating the outcome. These regulations are central in understanding cell fate (how does the cell differentiate ? Do mutations occur ? etc), and progress there hinges on our capacity to analyse, predict, monitor and control complex and variegated processes. We have applied Petri net unfolding techniques for the efficient computation of attractors in a regulatory network; that is, to identify strongly connected reachability components that correspond to stable evolutions, e.g. of a cell that differentiates into a specific functionality (or mutation). This constitutes the starting point of a broader research with Petri net unfolding techniques in regulation. In fact, the use of ordinary Petri nets for capturing regulatory network (RN) dynamics overcomes the limitations of traditional RN models : those impose e.g. Monotonicity properties in the influence that one factor had upon another, i.e. always increasing or always decreasing, and were thus unable to cover all actual behaviours (see [75]). Rather, we follow the more refined model of boolean networks of automata, where the local states of the different factors jointly determine which state transitions are possible. For these connectors, ordinary PNs constitute a first approximation, improving greatly over the literature but leaving room for improvement in terms of introducing more refined logical connectors. Future work thus involves transcending this class of PN models. Via unfoldings, one has access – provided efficient techniques are available – to all behaviours of the model, rather than over-or under-approximations as previously. This opens the way to efficiently searching in particular for determinants of the cell fate : which attractors are reachable from a given stage, and what are the factors that decide in favor of one or the other attractor, etc. Our current research focusses on *cellular reprogramming*.

4.3. Autonomous Vehicles

The validation of safety properties is a crucial concern for the design of computer guided systems, in particular for automated transport systems. Our approach consists in analyzing the interactions of a randomized environment (roads, cross-sections, etc.) with a vehicle controller. This requires to :

- define the relevant case studies;
- extend our tool COSMOS to handle general hybrid systems;
- conduct experimentations and analyze their results.

In [SIA2017], we have shown that this approach scales pretty well but with a controller written in C. The next step will be to combine Simulink models with Petri nets since Simulink is widely used for specifying hybrid systems in industry. In order to do so, we need to define an operational semantic for Simulink and to design an elegant way for specifying the interface between nets and Simulink models. Then we will implement the solution in Cosmos.

5. Highlights of the Year

5.1. Highlights of the Year

See the 'New results' section.

6. New Software and Platforms

6.1. COSMOS

FUNCTIONAL DESCRIPTION: COSMOS is a statistical model checker for the Hybrid Automata Stochastic Logic (HASL). HASL employs Linear Hybrid Automata (LHA), a generalization of Deterministic Timed Automata (DTA), to describe accepting execution paths of a Discrete Event Stochastic Process (DESP), a class of stochastic models which includes, but is not limited to, Markov chains. As a result HASL verification turns out to be a unifying framework where sophisticated temporal reasoning is naturally blended with elaborate reward-based analysis. COSMOS takes as input a DESP (described in terms of a Generalized Stochastic Petri Net), an LHA and an expression Z representing the quantity to be estimated. It returns a confidence interval estimation of Z , recently, it has been equipped with functionalities for rare event analysis. COSMOS is written in C++

- Participants: Benoît Barbot, Hilal Djafri, Marie Dufлот-Kremer, Paolo Ballarini and Serge Haddad
- Contact: Hilal Djafri
- URL: <http://www.lsv.ens-cachan.fr/~barbot/cosmos/>

6.2. CosyVerif

FUNCTIONAL DESCRIPTION: CosyVerif is a platform dedicated to the formal specification and verification of dynamic systems. It allows to specify systems using several formalisms (such as automata and Petri nets), and to run verification tools on these models.

- Participants: Alban Linard, Fabrice Kordon, Laure Petrucci and Serge Haddad
- Partners: LIP6 - LSV - LIPN (Laboratoire d'Informatique de l'Université Paris Nord)
- Contact: Serge Haddad
- URL: <http://www.cosyverif.org/>

6.3. Mole

FUNCTIONAL DESCRIPTION: Mole computes, given a safe Petri net, a finite prefix of its unfolding. It is designed to be compatible with other tools, such as PEP and the Model-Checking Kit, which are using the resulting unfolding for reachability checking and other analyses. The tool Mole arose out of earlier work on Petri nets.

- Participant: Stefan Schwon
- Contact: Stefan Schwon
- URL: <http://www.lsv.ens-cachan.fr/~schwonn/tools/mole/>

7. New Results

7.1. Optimal constructions for active diagnosis

Published in [4].

Diagnosis is the task of detecting fault occurrences in a partially observed system. Depending on the possible observations, a discrete-event system may be diagnosable or not. Active diagnosis aims at controlling the system to render it diagnosable. Past research has proposed solutions for this problem, but their complexity remains to be improved. Here, we solve the decision and synthesis problems for active diagnosability, proving that (1) our procedures are optimal with respect to computational complexity, and (2) the memory required for our diagnoser is minimal. We then study the delay between a fault occurrence and its detection by the diagnoser. We construct a memory-optimal diagnoser whose delay is at most twice the minimal delay, whereas the memory required to achieve optimal delay may be highly greater. We also provide a solution for parametrized active diagnosis, where we automatically construct the most permissive controller respecting a given delay.

7.2. Diagnosability of Repairable Faults

Published in [3].

The diagnosis problem for discrete event systems consists in deciding whether some fault event occurred or not in the system, given partial observations on the run of that system. Diagnosability checks whether a correct diagnosis can be issued in bounded time after a fault, for all faulty runs of that system. This problem appeared two decades ago and numerous facets of it have been explored, mostly for permanent faults. It is known for example that diagnosability of a system can be checked in polynomial time, while the construction of a diagnoser is exponential. The present paper examines the case of transient faults, that can appear and be repaired. Diagnosability in this setting means that the occurrence of a fault should always be detected in bounded time, but also before the fault is repaired, in order to prepare for the detection of the next fault or to take corrective measures while they are needed. Checking this notion of diagnosability is proved to be PSPACE-complete. It is also shown that faults can be reliably counted provided the system is diagnosable for faults and for repairs.

7.3. Diagnostic et contrôle de la dégradation des systèmes probabilistes

Published in [18].

Le diagnostic actif est opéré par un contrôleur en vue de rendre un système diagnosticable. Afin d'éviter que le contrôleur ne dégrade trop fortement le système, on lui affecte généralement un second objectif en termes de qualité de service. Dans le cadre des systèmes probabilistes, une spécification possible consiste à assurer une probabilité positive qu'une exécution infinie soit correcte, ce qu'on appelle le diagnostic actif sûr. Nous introduisons ici deux spécifications alternatives. La gamma-correction du système affecte à une exécution une valeur de correction dépendant d'un facteur de décote gamma et le contrôleur doit assurer une valeur moyenne supérieure à un seuil fixé. La alpha-dégradation requiert qu'asymptotiquement, à chaque unité de temps une proportion supérieure à alpha des exécutions jusqu'alors correctes le demeure. D'un point de vue sémantique, nous explicitons des liens significatifs entre les différentes notions. Algorithmiquement, nous établissons la frontière entre décidabilité et indécidabilité des problèmes et dans le cas positif nous exhibons la complexité précise ainsi qu'une synthèse, potentiellement à mémoire infinie.

7.4. The Complexity of Diagnosability and Opacity Verification for Petri Nets

Published in [7].

Diagnosability and opacity are two well-studied problems in discrete-event systems. We revisit these two problems with respect to expressiveness and complexity issues. We first relate different notions of diagnosability and opacity. We consider in particular fairness issues and extend the definition of Germanos et al. [ACM TECS, 2015] of weakly fair diagnosability for safe Petri nets to general Petri nets and to opacity questions. Second, we provide a global picture of complexity results for the verification of diagnosability and opacity. We show that diagnosability is NL-complete for finite state systems, PSPACE-complete for safe Petri nets (even with fairness), and EXSPACE-complete for general Petri nets without fairness, while non diagnosability is inter-reducible with reachability when fault events are not weakly fair. Opacity is ESPACE-complete for safe Petri nets (even with fairness) and undecidable for general Petri nets already without fairness.

7.5. Probabilistic Disclosure: Maximisation vs. Minimisation

Published in [8].

We consider opacity questions where an observation function provides to an external attacker a view of the states along executions and secret executions are those visiting some state from a fixed subset. Disclosure occurs when the observer can deduce from a finite observation that the execution is secret, the ε -disclosure variant corresponding to the execution being secret with probability greater than $1 - \varepsilon$. In a probabilistic and non deterministic setting, where an internal agent can choose between actions, there are two points of view, depending on the status of this agent: the successive choices can either help the attacker trying to disclose the

secret, if the system has been corrupted, or they can prevent disclosure as much as possible if these choices are part of the system design. In the former situation, corresponding to a worst case, the disclosure value is the supremum over the strategies of the probability to disclose the secret (maximisation), whereas in the latter case, the disclosure is the infimum (minimisation). We address quantitative problems (comparing the optimal value with a threshold) and qualitative ones (when the threshold is zero or one) related to both forms of disclosure for a fixed or finite horizon. For all problems, we characterise their decidability status and their complexity. We discover a surprising asymmetry: on the one hand optimal strategies may be chosen among deterministic ones in maximisation problems, while it is not the case for minimisation. On the other hand, for the questions addressed here, more minimisation problems than maximisation ones are decidable.

7.6. D-SPACES: Implementing Declarative Semantics for Spatially Structured Information

Published in [13].

We introduce in this paper D-SPACES, an implementation of constraint systems with space and extrusion operators. Constraint systems are algebraic models that allow for a semantic language-like representation of information in systems where the concept of space is a primary structural feature. We give this information mainly an epistemic interpretation and consider various agents as entities acting upon it. D-SPACES is coded as a c++11 library providing implementations for constraint systems, space functions and extrusion functions. The interfaces to access each implementation are minimal and thoroughly documented. D-SPACES also provides property-checking methods as well as an implementation of a specific type of constraint systems (a boolean algebra). This last implementation serves as an entry point for quick access and proof of concept when using these models. Furthermore, we offer an illustrative example in the form of a small social network where users post their beliefs and utter their opinions.

7.7. Unbounded product-form Petri nets

Published in [14].

Computing steady-state distributions in infinite-state stochastic systems is in general a very difficult task. Product-form Petri nets are those Petri nets for which the steady-state distribution can be described as a natural product corresponding, up to a normalising constant, to an exponentiation of the markings. However, even though some classes of nets are known to have a product-form distribution, computing the normalising constant can be hard. The class of (closed) Π^3 -nets has been proposed in an earlier work, for which it is shown that one can compute the steady-state distribution efficiently. However these nets are bounded. In this paper, we generalise queuing Markovian networks and closed Π^3 -nets to obtain the class of open Π^3 -nets, that generate infinite-state systems. We show interesting properties of these nets: (1) we prove that liveness can be decided in polynomial time, and that reachability in live Π^3 -nets can be decided in polynomial time; (2) we show that we can decide ergodicity of such nets in polynomial time as well; (3) we provide a pseudo-polynomial time algorithm to compute the normalising constant.

7.8. Statistical Model-Checking for Autonomous Vehicle Safety Validation

Published in [20].

We present an application of statistical model-checking to the verification of an autonomous vehicle controller. Our goal is to check safety properties in various traffic situations. More specifically, we focus on a traffic jam situation.

The controller is specified by a C++ program. Using sensors, it registers positions and velocities of nearby vehicles and modifies the position and velocity of the controlled vehicle to avoid collisions. We model the environment using a stochastic high level Petri net, where random behaviors of other vehicles can be described. We use HASL, a quantitative variant of linear temporal logic, to express the desired properties. A large family of performance indicators can be specified in HASL and we target in particular the expectation of travelled distance or the collision probability.

We evaluate the properties of this model using COSMOS1. This simulation tool implements numerous statistical techniques such as sequential hypothesis testing and most confidence range computation methods. Its efficiency allowed us to conduct several experiments with success.

7.9. Une sémantique formelle pour les modèles Simulink

Published in [19].

De nombreux projets industriels, notamment dans la construction automobile, font appel à la suite d'outils Simulink pour la conception et la validation de composants critiques représentant des systèmes hybrides c'est-à-dire combinant des aspects discrets et continus. Cependant les formalismes associés ne disposent pas d'une sémantique formelle ce qui peut diminuer la confiance des ingénieurs vis-à-vis des résultats produits. Nous proposons ici une telle sémantique en procédant en deux étapes. Nous développons d'abord une sémantique exacte mais non exécutable. Puis nous l'enrichissons d'une sémantique opérationnelle approchée avec pour objectif une quantification de l'erreur issue de cette approximation.

7.10. The Logical View on Continuous Petri Nets

Published in [5].

Continuous Petri nets are a relaxation of classical discrete Petri nets in which transitions can be fired a fractional number of times, and consequently places may contain a fractional number of tokens. Such continuous Petri nets are an appealing object to study since they over approximate the set of reachable configurations of their discrete counterparts, and their reachability problem is known to be decidable in polynomial time. The starting point of this paper is to show that the reachability relation for continuous Petri nets is definable by a sentence of linear size in the existential theory of the rationals with addition and order. Using this characterization, we obtain decidability and complexity results for a number of classical decision problems for continuous Petri nets. In particular, we settle the open problem about the precise complexity of reachability set inclusion. Finally, we show how continuous Petri nets can be incorporated inside the classical backward coverability algorithm for discrete Petri nets as a pruning heuristic in order to tackle the symbolic state explosion problem. The cornerstone of the approach we present is that our logical characterization enables us to leverage the power of modern SMT-solvers in order to yield a highly performant and robust decision procedure for coverability in Petri nets. We demonstrate the applicability of our approach on a set of standard benchmarks from the literature.

7.11. Memoryless Determinacy of Finite Parity Games: Another Simple Proof

Published in [24].

Memoryless determinacy of (infinite) parity games is an important result with numerous applications. It was first independently established by Emerson and Jutla [1] and Mostowski [2] but their proofs involve elaborate developments. The elegant and simpler proof of Zielonka [3] still requires a nested induction on the finite number of priorities and on ordinals for sets of vertices. There are other proofs for finite games like the one of Bjørklund, Sandberg and Vorobyov [4] that relies on relating infinite and finite duration games. We present here another simple proof that finite parity games are determined with memoryless strategies using induction on the number of relevant states. The closest proof that relies on induction over non absorbing states is the one of Graedel [5]. However instead of focusing on a single appropriate vertex for induction as we do here, he considers two reduced games per vertex, for all the vertices of the game. The idea of reasoning about a single state has been inspired to me by the analysis of finite stochastic priority games by Karelövic and Zielonka [6].

7.12. Interval iteration algorithm for MDPs and IMDPs

Markov Decision Processes (MDP) are a widely used model including both non-deterministic and probabilistic choices. Minimal and maximal probabilities to reach a target set of states, with respect to a policy resolving non-determinism, may be computed by several methods including value iteration. This algorithm, easy to

implement and efficient in terms of space complexity, iteratively computes the probabilities of paths of increasing length. However, it raises three issues: (1) defining a stopping criterion ensuring a bound on the approximation, (2) analysing the rate of convergence, and (3) specifying an additional procedure to obtain the exact values once a sufficient number of iterations has been performed. The first two issues are still open and, for the third one, an upper bound on the number of iterations has been proposed. Based on a graph analysis and transformation of MDPs, we address these problems. First we introduce an interval iteration algorithm, for which the stopping criterion is straightforward. Then we exhibit its convergence rate. Finally we significantly improve the upper bound on the number of iterations required to get the exact values. We extend our approach to also deal with Interval Markov Decision Processes (IMDP) that can be seen as symbolic representations of MDPs.

7.13. Alignment-Based Trace Clustering

Published in [9].

A novel method to cluster event log traces is presented in this paper. In contrast to the approaches in the literature, the clustering approach of this paper assumes an additional input: a process model that describes the current process. The core idea of the algorithm is to use model traces as centroids of the clusters detected, computed from a generalization of the notion of alignment. This way, model explanations of observed behavior are the driving force to compute the clusters, instead of current model agnostic approaches, e.g., which group log traces merely on their vector-space similarity. We believe alignment-based trace clustering provides results more useful for stakeholders. Moreover, in case of log incompleteness, noisy logs or concept drift, they can be more robust for dealing with highly deviating traces. The technique of this paper can be combined with any clustering technique to provide model explanations to the clusters computed. The proposed technique relies on encoding the individual alignment problems into the (pseudo-)Boolean domain, and has been implemented in our tool DarkSider that uses an open-source solver.

7.14. Aligning Modeled and Observed Behavior: A Compromise Between Complexity and Quality

Published in [17].

Certifying that a process model is aligned with the real process executions is perhaps the most desired feature a process model may have: aligned process models are crucial for organizations, since strategic decisions can be made easier on models instead of on plain data. In spite of its importance, the current algorithmic support for computing alignments is limited: either techniques that explicitly explore the model behavior (which may be worst-case exponential with respect to the model size), or heuristic approaches that cannot guarantee a solution, are the only alternatives. In this paper we propose a solution that sits right in the middle in the complexity spectrum of alignment techniques; it can always guarantee a solution, whose quality depends on the exploration depth used and local decisions taken at each step. We use linear algebraic techniques in combination with an iterative search which focuses on progressing towards a solution. The experiments show a clear reduction in the time required for reaching a solution, without sacrificing significantly the quality of the alignment obtained.

7.15. Temporal Reprogramming of Boolean Networks

Published in [15].

Cellular reprogramming, a technique that opens huge opportunities in modern and regenerative medicine, heavily relies on identifying key genes to perturb. Most of computational methods focus on finding mutations to apply to the initial state in order to control which attractor the cell will reach. However, it has been shown, and is proved in this article, that waiting between the perturbations and using the transient dynamics of the system allow new reprogramming strategies. To identify these temporal perturbations, we consider a qualitative model of regulatory networks, and rely on Petri nets to model their dynamics and the putative perturbations.

Our method establishes a complete characterization of temporal perturbations, whether permanent (mutations) or only temporary, to achieve the existential or inevitable reachability of an arbitrary state of the system. We apply a prototype implementation on small models from the literature and show that we are able to derive temporal perturbations to achieve trans-differentiation.

7.16. Goal-Driven Unfolding of Petri Nets

Published in [10].

Unfoldings provide an efficient way to avoid the state-space explosion due to interleavings of concurrent transitions when exploring the runs of a Petri net. The theory of adequate orders allows one to define finite prefixes of unfoldings which contain all the reachable markings. In this paper we are interested in reachability of a single given marking, called the goal. We propose an algorithm for computing a finite prefix of the unfolding of a 1-safe Petri net that preserves all minimal configurations reaching this goal. Our algorithm combines the unfolding technique with on-the-fly model reduction by static analysis aiming at avoiding the exploration of branches which are not needed for reaching the goal. We present some experimental results.

7.17. Euler's Method Applied to the Control of Switched Systems

Hybrid systems are a powerful formalism for modeling and reasoning about cyber-physical systems. They mix the continuous and discrete natures of the evolution of computerized systems. Switched systems are a special kind of hybrid systems, with restricted discrete behaviours: those systems only have finitely many different modes of (continuous) evolution, with isolated switches between modes. Such systems provide a good balance between expressiveness and controllability, and are thus in widespread use in large branches of industry such as power electronics and automotive control. The control law for a switched system defines the way of selecting the modes during the run of the system. Controllability is the problem of (automatically) synthesizing a control law in order to satisfy a desired property, such as safety (maintaining the variables within a given zone) or stabilisation (confinement of the variables in a close neighborhood around an objective point). In order to compute the control of a switched system, we need to compute the solutions of the differential equations governing the modes. Euler's method is the most basic technique for approximating such solutions. We present here an estimation of the Euler's method local error, using the notion of "one-sided Lipschitz constant" for modes. This yields a general control synthesis approach which can encompass several features such as bounded disturbance and compositionality.

7.18. An Improved Algorithm for the Control Synthesis of Nonlinear Sampled Switched Systems

Published in [6].

A novel algorithm for the control synthesis for nonlinear switched systems is presented in this paper. Based on an existing procedure of state-space bisection and made available for nonlinear systems with the help of guaranteed integration, the algorithm has been improved to be able to consider longer patterns of modes with a better pruning approach. Moreover, the use of guaranteed integration also permits to take bounded perturbations and varying parameters into account. It is particularly interesting for safety critical applications, such as in aeronautical, military or medical fields. The whole approach is entirely guaranteed and the induced controllers are correct-by-design. Some experimentations are performed to show the important gain of the new algorithm.

7.19. Distributed Control Synthesis Using Euler's Method

Published in [22].

In a previous work, we explained how Euler’s method for computing approximate solutions of systems of ordinary differential equations can be used to synthesize safety controllers for sampled switched systems. We continue here this line of research by showing how Euler’s method can also be used for synthesizing safety controllers in a distributed manner. The global system is seen as an interconnection of two (or more) sub-systems where, for each component, the sub-state corresponding to the other component is seen as an “input”; the method exploits (a variant of) the notions of incremental input-to-state stability (δ -ISS) and ISS Lyapunov function. We illustrate this distributed control synthesis method on a building ventilation example.

7.20. Control Synthesis of Nonlinear Sampled Switched Systems using Euler’s Method

Published in [21].

In this paper, we propose a symbolic control synthesis method for nonlinear sampled switched systems whose vector fields are one-sided Lipschitz. The main idea is to use an approximate model obtained from the forward Euler method to build a guaranteed control. The benefit of this method is that the error introduced by symbolic modeling is bounded by choosing suitable time and space discretizations. The method is implemented in the interpreted language Octave. Several examples of the literature are performed and the results are compared with results obtained with a previous method based on the Runge-Kutta integration method.

7.21. Metastability-Aware Memory-Efficient Time-to-Digital Converter

Published in [11].

We propose a novel method for transforming delay-line time-to-digital converters (TDCs) into TDCs that output Gray code without relying on synchronizers. We formally prove that the inevitable metastable memory upsets (Marino, TC’81) do not induce an additional time resolution error. Our modified design provides suitable inputs to the recent metastability-containing sorting networks by Lenzen and Medina (ASYNC’16) and Bund et al. (DATE’17). In contrast, employing existing TDCs would require using thermometer code at the TDC output (followed by conversion to Gray code) or resolving metastability inside the TDC. The former is too restrictive w.r.t. the dynamic range of the TDCs, while the latter loses the advantage of enabling (accordingly much faster) computation without having to first resolve metastability.

Our all-digital designs are also of interest in their own right: they support high sample rates and large measuring ranges at nearly optimal bit-width of the output, yet maintain the original delay-line’s time resolution. No previous approach unifies all these properties in a single device.

7.22. Brief Announcement: Lower Bounds for Asymptotic Consensus in Dynamic Networks

Published in [12].

7.23. Metastability Tolerant Computing

Published in [16].

Synchronization using flip-flop chains imposes a latency of a few clock cycles when transferring data and control signals between clock domains. We propose a design scheme that avoids this latency by performing synchronization as part of state/data computations while guaranteeing that metastability is contained and its effects tolerated (with an acceptable failure probability). We present a theoretical framework for modeling synchronous state machines in the presence of metastability and use it to prove properties that guarantee some form of reliability. Specifically, we show that the inevitable state/data corruption resulting from propagating metastable states can be confined to a subset of computations. Applications that can tolerate certain failures can exploit this property to leverage low-latency and quasi-reliable operation simultaneously. We demonstrate the approach by designing a Network-on-Chip router with zero-latency asynchronous ports and show via simulation that it outperforms a variant with two flip-flop synchronizers at a negligible cost in packet transfer reliability.

8. Partnerships and Cooperations

8.1. National Initiatives

- Thomas Chatain, Stefan Haar , Serge Haddad and Stefan Schwoon are participating in the ANR Project **ALGORECELL**.
- Matthias Függer participates in the ANR project FREDDA.

8.2. International Initiatives

8.2.1. Inria Associate Teams Not Involved in an Inria International Labs

8.2.1.1. LifeForm

Title: Life Sciences need formal Methods !

International Partner (Institution - Laboratory - Researcher):

Newcastle University (United Kingdom) - School of Computing Science - Victor Khomenko

Start year: 2016

See also: <http://projects.lsv.ens-cachan.fr/LifeForm/>

This project extends an existing cooperation between the MEXICO team and Newcastle University on partial-order based formal methods for concurrent systems. We enlarge the partnership to bioinformatics and synthetic biology. The proposal addresses challenges concerning formal specification, verification, monitoring and control of synthetic biological systems, with use cases conducted in the Center for Synthetic Biology and the Bioeconomy (CSBB) in Newcastle. A main challenge is to create a solid modelling framework based on Petri-net type models that allow for causality analysis and rapid state space exploration for verification, monitoring and control purposes; a potential extension to be investigated concerns the study of attractors and cell reprogramming in Systems Biology.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Joost-Pieter Katoen, Aachen, spent two weeks with MEXICO.

8.3.1.1. Internships

Aalok Thakkar, 2nd year student from CMI (India), did a two-month research internship on 'Semantics of Mutation Dynamics' under the supervision of Stefan Haar, from May 2nd to July 21st, 2017.

8.3.2. Visits to International Teams

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Matthias Függer is general co-chair of *ASYNC 2018*

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Laurent Fribourg was a PC member of:
 - 7th International Conference on New Computational Methods for Inverse Problems, Cachan, 2017
 - The 27th International Symposium on Logic-based Program Synthesis and Transformation, Namur, Belgium, 2017
 - Seventh Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, Seoul, 2017.
- Matthias Függer was a member of the PC of **DDECS'17**.
- Stefan Haar was a member of the PCs of the conferences MSR 2017 and **ACSD 2017** and of the workshop **ATAED 2017**.
- Serge Haddad was a PC member of the *International Workshop on Petri Nets and Software Engineering* (PNSE) 2017 at Zaragoza, Spain, and of the *11th International Conference on Verification and Evaluation of Computer and Communication Systems* (VECOS) 2017 at Montreal, Québec, Canada. He was also a member of the scientific committee of *Ecole d'été temps-réel* (ETR 2017).

9.1.2.2. Reviewer

- Matthias Függer was a reviewer for ICALP, DISC, FMCAD, ICDCN, and OPODIS.
- Stefan Haar was a reviewer for FOSSACS.
- Stefan Schwoon was a reviewer for the following conferences taking place in 2017: STACS, TACAS, ESOP, ATVA, and FSTTCS.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Stefan Haar is associate editor of the *Journal of Discrete Event Dynamic Systems: Theory and Applications*.

9.1.3.2. Reviewer - Reviewing Activities

- Thomas Chatain was a reviewer for Acta Informatica, Artificial Intelligence and Journal of Discrete Event Dynamic Systems.
- Matthias Függer was a reviewer for MFCS.
- Stefan Haar was a reviewer for MSCS and IEEE Transactions on Automatic Control.
- Stefan Schwoon was a reviewer for Fundamenta Informaticae, International Journal on Software Tools for Technology Transfer, and the Journal of Discrete Event Dynamic Systems.

9.1.4. Invited Talks

- Laurent Fribourg gave the following invited talk: "Euler's Method Applied to the Control of Switched Systems", at 15th International Conference on Formal Modelling and Analysis of Timed Systems, Berlin, 2017
- Matthias Függer gave invited talks at the Theory of Hardware seminar in Vienna in February, the Noon seminar at Max-Planck Institute for Informatics in April, and the Distributed Computing Seminar at Labri in November.
- Serge Haddad gave the following invited talks:
 - at Centre Fédéré en Vérification, Bruxelles, Belgique on February 24, 2017, entitled *From Continuous Petri nets to Petri nets and Back*;
 - at LACL, Créteil on February 27, 2017, entitled *Probabilistic Disclosure: Maximisation vs. Minimisation*

- at the MSR 2017 conference, Marseille, France, on November 16, 2017, entitled *Réseaux de Petri discrets et continus : apports réciproques*.
- Claudine Picaronny gave an invited talk on 'Vérification probabiliste, numérique ou statistique', on the 21th of april 2017 at Alea 17, CIRM Marseille, France

9.1.5. Scientific Expertise

- Serge Haddad was expert for the evaluation of the researcher premiums at University Pierre et Marie Curie

9.1.6. Research Administration

- Laurent Fribourg is a member of
 - Comité Direction of Department Sciences et technologies de l'information et de la communication of Université Paris-Saclay,
 - Bureau of Domaine d'Intérêt Majeur émergent du Réseau Francilien en Sciences Informatiques
- Stefan Haar is the president of Inria's *GTRI-COST* committee for international relations, and the head of the **SciLex** (Software Reliability and Security) axis of the **LABEX DIGICOSME**, and ipso facto a member of *DIGICOSME*'s executive committee and scientific commission.
- Serge Haddad was the president of the HCERES evaluation committee of the laboratory LIAS, Poitiers.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Stefan Haar taught one half of L3 level class on Formal Languages at ENS Paris-Saclay (15 h CM, 22.5 EQTD).
- Serge Haddad is professor at ENS Paris-Saclay. Claudine Picaronny, Thomas Chatain, and Stefan Schwoon are associate professors of the same university.
- Serge Haddad is the head of the Computer Science Department, and Stefan Schwoon is in charge of the L3 formation.
- Claudine Picaronny is a co-director of the ENS Paris-Saclay's Mathematics department and a member of the juries of the 'agrégation interne de Mathématiques' and of the second 'concours de Mathématiques' of ENS Paris-Saclay; she is also the coordinator of the mathematics/computer science examination of E3A, parts MP and MC.
- Matthias Függer is teaching "Initiation à la recherche" at ENS Paris-Saclay.

9.2.2. Supervision

Theses in progress:

Hugues Mandon, ENS Paris-Saclay since October 2016, on *computational models and algorithms for the prediction of Cell Reprogramming Strategies*, co-supervised by Stefan Haar and L. Paulevé (LRI)

Juraj Kolčák, ENS Paris-Saclay since March 2017, on *Unfoldings and Abstract Interpretation for Parametric Biological Regulatory Networks*, co-supervised by Stefan Haar and L. Paulevé (LRI).

Adnane Saoud, Université Paris-Saclay since 2016, jointly supervised by Laurent Fribourg and Antoine Girard (Centrale-Supelec).

Engel Lefauchaux, ENS Paris-Saclay since 2015, *Controlling information in probabilistic systems*, jointly supervised by Nathalie Bertrand (SUMO team) and Serge Haddad

Yann Duploux, IRT SystemX since 2015, *Application of formal methods to the development of embedded systems for autonomous vehicles*, supervised by Béatrice Bérard and Serge Haddad.

Robert Najvirt (TU Wien, Austrian FWF SIC project), realistic delay models with applications in high-speed and low-power circuits, co-supervised by Matthias Függer and Andreas Steininger.

Martin Perner (TU Wien, Austrian FWF SIC project), clock generation on-chip and formalisms suitable to prove correct VLSI circuits, co-supervised by Matthias Függer and Ulrich Schmid.

Juergen Maier (TU Wien, Austrian FWF SIC project), on realistic delay models with applications in high-speed and low-power circuits, with focus on noise and high-order models, co-supervised by Matthias Függer and with Ulrich Schmid.

9.2.3. Juries

- Laurent Fribourg was a member of the Jury of Irini-Eleftheria Mens's PhD Thesis on "Learning regular languages over large alphabets", defended at University of Grenoble, October 2017.
- Stefan Haar was a reviewer of the thesis by Guillaume Madelaine on 'Simplifications Exactes et Structurelles de Réseaux de Réactions Biologiques', defended on February 28 at Lille University, France.
- Serge Haddad was:
 - reviewer in the jury of Bruno Karelavic on *Quantitative Analysis of Stochastic Systems – Priority Games and Populations of Markov Chains* on July 7 2017, University Paris 7
 - president of the jury of Nicolas David on *Réseaux de Petri à Paramètres Discrets* on October 20 University Nantes
 - reviewer in the jury of Thomas Geffroy on *Vers des outils efficaces pour la vérification de systèmes concurrents* on December 12 2017, University Bordeaux
- Claudine Picaronny was Member of the jury of Pierre Carlier's Thesis on 'Verification of Stochastic Timed Automata', on the 8th of december 2017, Mons, Belgium

10. Bibliography

Major publications by the team in recent years

- [1] B. BARBOT, S. HADDAD, C. PICARONNY. *Coupling and Importance Sampling for Statistical Model Checking*, in "Proceedings of the 18th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'12)", Tallinn, Estonia, C. FLANAGAN, B. KÖNIG (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7214, pp. 331-346, <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHP-tacas12.pdf>
- [2] S. HADDAD, J. MAIRESSE, H.-T. NGUYEN. *Synthesis and Analysis of Product-form Petri Nets*, in "Fundamenta Informaticae", 2013, vol. 122, n^o 1-2, pp. 147-172, <https://hal.archives-ouvertes.fr/hal-00925774>

Publications of the year

Articles in International Peer-Reviewed Journals

- [3] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "Discrete Event Dynamic Systems", June 2017, <https://hal.inria.fr/hal-01646911>
- [4] S. HAAR, S. HADDAD, T. MELLITI, S. SCHWOON. *Optimal constructions for active diagnosis*, in "Journal of Computer and System Sciences", February 2017, vol. 83, n^o 1, pp. 101-120 [DOI : 10.1016/J.JCSS.2016.04.007], <https://hal.archives-ouvertes.fr/hal-01408047>

- [5] S. HADDAD, M. BLONDIN, C. HAASE, A. FINKEL. *The Logical View on Continuous Petri Nets*, in "ACM Transactions on Computational Logic", 2017, vol. 18, n^o 3, <https://hal.inria.fr/hal-01652793>
- [6] A. LE COËNT, J. ALEXANDRE DIT SANDRETTO, A. CHAPOUTOT, L. FRIBOURG. *An Improved Algorithm for the Control Synthesis of Nonlinear Sampled Switched Systems*, in "Formal Methods in System Design", November 2017, forthcoming [DOI : 10.1007/s10703-017-0305-8], <https://hal.archives-ouvertes.fr/hal-01399337>

International Conferences with Proceedings

- [7] B. BÉRARD, S. HAAR, S. SCHMITZ, S. SCHWOON. *The Complexity of Diagnosability and Opacity Verification for Petri Nets*, in "Petri nets 2017", Zaragoza, Spain, W. VAN DER AALST, E. BEST (editors), Lecture Notes in Computer Science, Springer, 2017, <https://hal.inria.fr/hal-01484476>
- [8] B. BÉRARD, S. HADDAD, E. LEFAUCHEUX. *Probabilistic Disclosure: Maximisation vs. Minimisation*, in "FSTTCS 2017", Kanpur, India, December 2017 [DOI : 10.4230/LIPIcs.FSTTCS.2017], <https://hal.inria.fr/hal-01618955>
- [9] T. CHATAIN, J. CARMONA, B. F. VAN DONGEN. *Alignment-Based Trace Clustering*, in "ER 2017 - 36th International Conference on Conceptual Modeling", Valencia, Spain, ER 2017: Conceptual Modeling, Springer, November 2017, vol. 10650, pp. 295-308 [DOI : 10.1007/978-3-319-69904-2_24], <https://hal.inria.fr/hal-01664235>
- [10] T. CHATAIN, L. PAULEVÉ. *Goal-Driven Unfolding of Petri Nets*, in "28th International Conference on Concurrency Theory (CONCUR 2017)", Berlin, Germany, September 2017 [DOI : 10.4230/LIPIcs.CONCUR.2017.14], <https://hal.archives-ouvertes.fr/hal-01392203>
- [11] M. FÜGGER, A. KINALI, C. LENZEN, T. POLZER. *Metastability-Aware Memory-Efficient Time-to-Digital Converters*, in "IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)", San Diego, United States, May 2017, <https://hal.archives-ouvertes.fr/hal-01652787>
- [12] M. FÜGGER, T. NOWAK, M. SCHWARZ. *Brief Announcement: Lower Bounds for Asymptotic Consensus in Dynamic Networks*, in "31st International Symposium on Distributed Computing (DISC)", Wien, Austria, October 2017, vol. Proceedings of the 31st International Symposium on Distributed Computing (DISC 2017), <https://hal.archives-ouvertes.fr/hal-01652851>
- [13] S. HAAR, S. PERCHY, F. VALENCIA. *D-SPACES: Implementing Declarative Semantics for Spatially Structured Information*, in "11th International Conference on Semantic Computing", San Diego, California, United States, IEEE ICSC 2017, IEEE, January 2017, vol. 11, <https://hal.inria.fr/hal-01328189>
- [14] V. JUGÉ, P. BOUYER, S. HADDAD. *Unbounded product-form Petri nets*, in "28th International Conference on Concurrency Theory (CONCUR 2017)", Berlin, Germany, 28th International Conference on Concurrency Theory (CONCUR 2017), September 2017, <https://arxiv.org/abs/1708.05847> - 31 pages [DOI : 10.4230/LIPIcs.CONCUR.2017.31], <https://hal.archives-ouvertes.fr/hal-01615257>
- [15] H. MANDON, S. HAAR, L. PAULEVÉ. *Temporal Reprogramming of Boolean Networks*, in "CMSB 2017 - 15th conference on Computational Methods for Systems Biology", Darmstadt, Germany, J. FERET, H. KOEPL (editors), Lecture Notes in Computer Science, Springer International Publishing, September 2017, vol. 10545, pp. 179 - 195 [DOI : 10.1007/978-3-319-67471-1_11], <https://hal.archives-ouvertes.fr/hal-01589251>

[16] G. TARAWNEH, M. FÜGGER, C. LENZEN. *Metastability Tolerant Computing*, in "ASYNC17 - 23rd IEEE International Symposium on Asynchronous Circuits and Systems", San Diego, United States, May 2017, <https://hal.archives-ouvertes.fr/hal-01652772>

[17] B. F. VAN DONGEN, J. CARMONA, T. CHATAIN, F. TAYMOURI. *Aligning Modeled and Observed Behavior: A Compromise Between Complexity and Quality*, in "CAiSE 2017 - 29th International Conference on Advanced Information Systems Engineering", Essen, Germany, CAiSE 2017: Advanced Information Systems Engineering, Springer, June 2017, vol. 10253, pp. 94-109 [DOI : 10.1007/978-3-319-59536-8_7], <https://hal.inria.fr/hal-01664240>

National Conferences with Proceedings

[18] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnostic et contrôle de la dégradation des systèmes probabilistes*, in "MSR 2017 - Modélisation des Systèmes Réactifs", Marseille, France, November 2017, <https://hal.inria.fr/hal-01618922>

[19] B. BÉRARD, Y. DUPLOUY, S. HADDAD. *Une sémantique formelle pour les modèles Simulink*, in "École d'été Temps Réel 2017", Paris, France, August 2017, <https://hal.archives-ouvertes.fr/hal-01578297>

Conferences without Proceedings

[20] B. BARBOT, B. BÉRARD, Y. DUPLOUY, S. HADDAD. *Statistical Model-Checking for Autonomous Vehicle Safety Validation*, in "SIA Simulation Numérique", Montigny-le-Bretonneux, France, Société des Ingénieurs de l'Automobile, March 2017, <https://hal.archives-ouvertes.fr/hal-01491064>

[21] A. LE COËNT, F. DE VUYST, L. CHAMOIN, L. FRIBOURG. *Guaranteed control synthesis of nonlinear switched systems using Euler method*, in "3rd International Workshop on Symbolic and Numerical Methods for Reachability Analysis", Uppsala, Sweden, April 2017, <https://hal.archives-ouvertes.fr/hal-01583164>

Scientific Books (or Scientific Book chapters)

[22] A. LE COËNT, J. ALEXANDRE DIT SANDRETTO, A. CHAPOUTOT, L. FRIBOURG, F. DE VUYST, L. CHAMOIN. *Distributed control synthesis using Euler's method*, in "International Workshop on Reachability Problems", August 2017 [DOI : 10.1007/978-3-319-67089-8_9], <https://hal.archives-ouvertes.fr/hal-01593225>

Other Publications

[23] L. FRIBOURG. *Euler's method applied to the control of switched systems*, December 2017, working paper or preprint, <https://hal.archives-ouvertes.fr/hal-01670089>

[24] S. HADDAD. *Memoryless Determinacy of Finite Parity Games: Another Simple Proof*, June 2017, working paper or preprint, <https://hal.inria.fr/hal-01541508>

[25] A. LE COËNT, L. FRIBOURG, J. VACHER. *Control Synthesis for Stochastic Switched Systems using the Tamed Euler Method*, December 2017, working paper or preprint, <https://hal.archives-ouvertes.fr/hal-01670579>

References in notes

- [26] S. ABBES, A. BENVENISTE, S. HAAR. *A Petri net model for distributed estimation*, in "Proc. MTNS 2004, Sixteenth International Symposium on Mathematical Theory of Networks and Systems, Louvain (Belgium), ISBN 90-5682-517-8", 2004
- [27] S. AKSHAY, N. BERTRAND, S. HADDAD, L. HELOUET. *The steady-state control problem for Markov decision processes*, in "Qest 2013", Buenos Aires, Argentina, K. R. JOSHI, M. SIEGLE, M. STOELINGA, P. R. D'ARGENIO (editors), Springer, September 2013, vol. 8054, pp. 290-304, <https://hal.inria.fr/hal-00879355>
- [28] R. ALUR, K. ETESSAMI, M. YANNAKAKIS. *Realizability and Verification of MSC Graphs*, in "Theor. Comput. Sci.", 2005, vol. 331, n^o 1, pp. 97–114
- [29] P. BALDAN, TH. CHATAIN, S. HAAR, B. KÖNIG. *Unfolding-based Diagnosis of Systems with an Evolving Topology*, in "Information and Computation", October 2010, vol. 208, n^o 10, pp. 1169-1192, <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCHK-icomp10.pdf>
- [30] P. BALDAN, A. CORRADINI, B. KÖNIG, S. SCHWOON. *McMillan's complete prefix for contextual nets*, in "Transactions on Petri Nets and Other Models of Concurrency", November 2008, vol. 1, pp. 199–220, Volume 5100 of Lecture Notes in Computer Science
- [31] P. BALDAN, S. HAAR, B. KOENIG. *Distributed Unfolding of Petri Nets*, in "Proc.FOSSACS 2006", LNCS, Springer, 2006, vol. 3921, pp. 126-141, Extended version: Technical Report CS-2006-1. Department of Computer Science, University Ca' Foscari of Venice
- [32] F. BASKETT, K. M. CHANDY, R. R. MUNTZ, F. G. PALACIOS. *Open, Closed, and Mixed Networks of Queues with Different Classes of Customers*, in "J. ACM", April 1975, vol. 22, pp. 248–260, <http://doi.acm.org/10.1145/321879.321887>
- [33] A. BENVENISTE, É. FABRE, S. HAAR. *Markov Nets: Probabilistic Models for distributed and concurrent Systems*, in "IEEE Transactions on Automatic Control", 2003, vol. 48 (11), pp. 1936-1950, Extended version: IRISA Research Report 1538
- [34] P. BHATEJA, P. GASTIN, M. MUKUND, K. NARAYAN KUMAR. *Local testing of message sequence charts is difficult*, in "Proceedings of the 16th International Symposium on Fundamentals of Computation Theory (FCT'07)", Budapest, Hungary, E. CSUHAJ-VARJÚ, Z. ÉSIK (editors), Lecture Notes in Computer Science, Springer, August 2007, vol. 4639, pp. 76-87 [DOI : 10.1007/978-3-540-74240-1_8], <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BGMN-fct07.pdf>
- [35] A. BOUILLARD, S. HAAR, S. ROSARIO. *Critical paths in the Partial Order Unfolding of a Stochastic Petri Net*, in "Proceedings of the 7th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'09)", Budapest, Hungary, J. OUAKNINE, F. VAANDRAGER (editors), Lecture Notes in Computer Science, Springer, September 2009, vol. 5813, pp. 43-57 [DOI : 10.1007/978-3-642-04368-0_6], <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHR-formats09.pdf>
- [36] P. BOUYER, S. HADDAD, P.-A. REYNIER. *Timed Unfoldings for Networks of Timed Automata*, in "Proceedings of the 4th International Symposium on Automated Technology for Verification and Analysis (ATVA'06)", Beijing, ROC, S. GRAF, W. ZHANG (editors), Lecture Notes in Computer Science, Springer, October 2006, vol. 4218, pp. 292-306, <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHR-atva06.pdf>

- [37] G. CHIOLA, C. DUTHELLET, G. FRANCESCHINIS, S. HADDAD. *Stochastic Well-Formed Colored Nets and Symmetric Modeling Applications*, in "IEEE Transactions on Computers", November 1993, vol. 42, n^o 11, pp. 1343-1360, <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/CDFH-toc93.ps>
- [38] R. DEBOUK, D. TENEKETZIS. *Coordinated decentralized protocols for failure diagnosis of discrete-event systems*, in "Journal of Discrete Event Dynamical Systems: Theory and Application", 2000, vol. 10, pp. 33-86
- [39] J. ESPARZA, K. HELJANKO. *Unfoldings - A Partial-Order Approach to Model Checking*, EATCS Monographs in Theoretical Computer Science, Springer, 2008
- [40] É. FABRE, A. BENVENISTE, C. JARD, S. HAAR. *Diagnosis of Asynchronous Discrete Event Systems, a Net Unfolding Approach*, in "IEEE Trans. Aut. Control", 2003, vol. 48 (5), pp. 714-727
- [41] É. FABRE, A. BENVENISTE, C. JARD, S. HAAR. *Distributed monitoring of concurrent and asynchronous systems*, in "Discrete Event Dynamic Systems: theory and application", 2005, vol. 15 (1), pp. 33-84, Preliminary version: Proc. CONCUR 2003, LNCS 2761, pp.1-28, Springer
- [42] S. HAAR, A. BENVENISTE, É. FABRE, C. JARD. *Partial Order Diagnosability Of Discrete Event Systems Using Petri Net Unfoldings*, in "42nd IEEE Conference on Decision and Control (CDC)", 2003
- [43] S. HAAR. *Probabilistic Cluster Unfoldings*, in "Fundamenta Informaticae", 2003, vol. 53 (3-4), pp. 281-314
- [44] S. LAFORTUNE, Y. WANG, T.-S. YOO. *Diagnostic Décentralisé Des Systèmes A Événements Discrets*, in "Journal Européen des Systèmes Automatisés (RS-JESA)", August 2005, vol. 99, n^o 99, pp. 95-110
- [45] K. G. LARSEN, P. PETTERSSON, W. YI. *Compositional and symbolic model-checking of real-time systems*, in "Proc. of RTSS 1995", IEEE Computer Society, 1995, pp. 76-89
- [46] L. RICKER, K. RUDIE. *Know Means No: Incorporating Knowledge into Discrete-Event Control Systems*, in "IEEE Transactions on Automatic Control", September 2000, vol. 45, n^o 9, pp. 1656-1668
- [47] L. RICKER, K. RUDIE. *Knowledge Is a Terrible Thing to Waste: Using Inference in Discrete-Event Control Problems*, in "IEEE Transactions on Automatic Control", MarchSeptember 2007, vol. 52, n^o 3, pp. 428-441
- [48] C. RODRÍGUEZ, S. SCHWOON, V. KHOMENKO. *Contextual Merged Processes*, in "34th International Conference on Applications and Theory of Petri Nets (ICATPN'13)", Italy, Lecture Notes in Computer Science, Springer, 2013, vol. 7927, pp. 29-48 [DOI : 10.1007/978-3-642-38697-8_3], <https://hal.archives-ouvertes.fr/hal-00926202>
- [49] H. L. S. YOUNES, R. G. SIMMONS. *Statistical probabilistic model checking with a focus on time-bounded properties*, in "Inf. Comput.", September 2006, vol. 204, pp. 1368-1409 [DOI : 10.1016/J.IC.2006.05.002], <http://dl.acm.org/citation.cfm?id=1182767.1182770>