AGENCE NATIONALE DE LA RECHERCHE ANR	**Compte-rendu de fin de projet**	

Projet ANR-11-INSE-004

VACSIM

Programme INS 2011

Ce document est à remplir par le coordinateur en collaboration avec les partenaires du projet. L'ensemble des partenaires doit avoir une copie de la version transmise à l'ANR.

Ce modèle doit être utilisé uniquement pour le compte-rendu de fin de projet.

A IDENTIFICATION

Acronyme du projet	VACSIM
Titre du projet	Validation de la commande des systèmes critiques par couplage simulation et méthodes d'analyse formelle
Coordinateur du projet (société/organisme)	Jean-Marc Faure – ENS de Cachan, 61 avenue du Président Wilson, 94235 Cachan Cedex
Période du projet (date de début – date de fin)	01/10/2011 31/09/2015
Site web du projet, le cas échéant	http://vacsim.inria.fr/

Rédacteur de ce rapport	
Civilité, prénom, nom	Prof. Jean-Marc Faure
Téléphone	+ 33 147 402 216
Adresse électronique	faure@lurpa.ens-cachan.fr
Date de rédaction	15/01/2016
Période faisant l'objet du rapport d'activité	01/10/2011 au 31/09/2015

Liste des partenaires présents à la fin du projet (société/organisme et responsable scientifique)	• EDF R&D, François Chériaux • Dassault Systemes, Eric Mevel • I3S, Michel Rueher • INRIA Rennes, Thierry Jéron • LaBRI, Antoine Rollet • LURPA, Jean-Marc Faure

B RESUME CONSOLIDE PUBLIC

B.1 RESUME CONSOLIDE PUBLIC EN FRANÇAIS

Améliorer la sûreté des systèmes critiques lors de la validation de leur commande

Mieux valider la commande des systèmes critiques

Un système critique est un système dont les défaillances peuvent avoir des conséquences graves sur la sécurité de l'environnement, des personnes ou des biens. Les systèmes de production d'énergie électrique, de production de produits pétroliers, de transport aérien et ferroviaire sont des exemples de tels systèmes. Ceci explique que la validation de leur commande nécessite une attention toute particulière.

Plusieurs techniques de validation progressive de la commande ont été développées en se basant sur un modèle de simulation du processus commandé puis le processus réel. Cependant, ces techniques considèrent très peu la construction du modèle de simulation (degré de finesse, complétude, …) pour son utilisation à des fins de validation de sa commande.

D'autre part, les méthodes d'analyse formelles, telles que les techniques de vérification/validation formelle et de test de conformité, qui ont produit de nombreux et importants résultats théoriques de recherche dans ce domaine, restent (très) difficiles à utiliser dans un contexte industriel (problèmes de passage à l'échelle, difficultés d'intégration dans les environnements de conception), en particulier pour ce qui concerne l'analyse de propriétés quantitatives (durées, coûts, grandeurs physiques).

Simulation et approches formelles pour la vérification et la validation

Pour contribuer à lever les deux verrous identifiés ci-dessus : construction et utilisation d'un modèle de simulation et meilleure utilisation industrielle des méthodes d'analyse formelles, les travaux du projet se sont basés sur :

- l'environnement de conception de la commande ControlBuild,
- l'environnement de simulation Dymola,
- des techniques de programmation par contraintes,
- des techniques de modélisation et d'analyse des systèmes à événements discrets, qu'ils soient temporisés ou non.

Résultats majeurs du projet

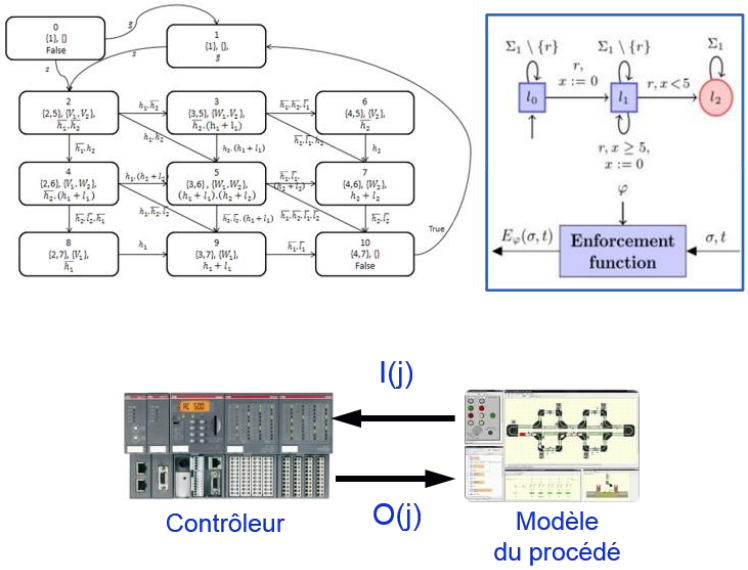
Le projet VACSIM a permis en premier lieu de proposer des techniques de réduction de la durée des tests des automates programmables industriels. Ces techniques ont été implantées dans un prototype logiciel intégré dans l'environnement ControlBuild. Des relations de conformité évitant les faux positifs et les faux négatifs lors de ces tests ont été également développées.

De plus, des méthodes innovantes d'analyse et de vérification/validation des systèmes temporisés ainsi que de localisation des erreurs dans des programmes ont été conçues lors du projet.

Production scientifique et brevets depuis le début du projet

Les résultats obtenus dans le projet VACSIM ont donné lieu à quatre mémoires de thèse, à une dizaine d'articles dans des revues de haut niveau et à plus de trente communications dans des conférences renommées des domaines scientifiques considérés.

Illustration



Informations factuelles

Le projet VACSIM (Validation de la commande des systèmes critiques par couplage simulation et méthodes d'analyse formelle) est un projet de recherche industrielle coordonné par le LURPA de l'ENS Cachan. Il réunit deux industriels, EDF R&D et Dassault Systèmes, et trois autres laboratoires : I3S, INRIA Rennes et LaBRI. Ce projet a débuté en octobre 2011 et a duré en tout 48 mois. Il a bénéficié d'une aide ANR d'environ 960 k€ pour un coût total d'environ 3,5 M€.

B.2 RESUME CONSOLIDE PUBLIC EN ANGLAIS

Improving dependability of critical systems when validating their control

For a better validation of critical systems control

A critical system is a system whose failures can have catastrophic consequences on safety. Examples can be found in the fields of power production, oil and chemical processes, air and railway transportation. This explains that validation of their control system requires many attentions.

Several techniques to progressively validate a control system have been developed in the past, by using a simulation model of the controlled process, then this process. Nonetheless, construction of the simulation model (fineness, completeness …) to be used for validation of the control system has not been deeply investigated.

On the other hand, formal analysis methods, such than verification and validation techniques and conformance testing, that have produced numerous and significant theoretical research results in this domain, remain (very) difficult to apply in an industrial context (scalability, tricky integration in industrial design environments), in particular when analysis of quantitative properties (durations, costs, physical quantities) is considered.

Simulation and formal approaches for V&V

To contribute to solve the following two issues: construction and use of the simulation model of the process and better industrial use of formal analysis methods, the works of the project have been based on:

- the software tool for designing control systems ControlBuild,
- the simulation environment Dymola,
- constraints programming techniques,

- several techniques for modeling and analysis of timed and non-timed discrete event systems.

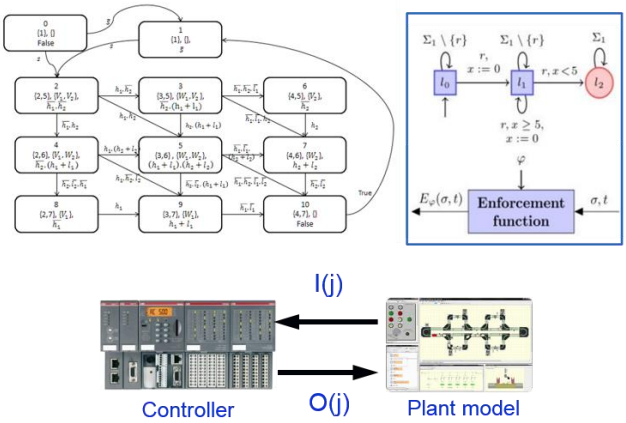
Main results of the project

Efficient techniques to lessen the duration of the tests of programmable logic controllers have been first proposed; these techniques have been implemented in a prototype software tool in the ControlBuild environment. In addition, conformance relations to avoid false positive and false negative during these tests have been developed.
Moreover, novel methods for analysis and V&V of timed systems as well as errors localization in programs have been designed during the project.

Publications

The results of the project have been published in four PhD reports, a ten articles in top-ranked journals and more than thirty communications in renowned conferences of the considered scientific domains.

Illustration



Facts

The VACSIM (Validating critical systems control by coupling simulation and formal analysis methods) project is an industrial research project managed by the laboratory LURPA from ENS Cachan. Two companies, EDF and Dassault Systemes, and three other labs: I3S, INRIA Rennes and LaBRI, are also involved in this project. This project started in October 2011 and lasted 48 months. It received a funding from ANR (about 960 k€) and its overall budget is around 3,5 M€.

C MEMOIRE SCIENTIFIQUE

Mémoire scientifique confidentiel : non

C.1 RESUME DU MEMOIRE

Cf. section B.1

C.2 ENJEUX ET PROBLEMATIQUE, ETAT DE L'ART

Quatre approches de validation complémentaires sont considérées dans ce projet :

- Validation par test progressif par parties
- Validation par simulation de partie opérative
- Validation de propriétés logiques à l'aide de techniques d'analyse des systèmes à événements discrets
- Validation de propriétés quantitatives à l'aide de techniques de vérification de systèmes temporisés et de programmation par contraintes.

Les travaux relatifs à la validation par test progressif par parties de systèmes logiques se basent sur les résultats obtenus lors du projet ANR TESTEC (TEst des Systèmes Temps réel Embarqués Critiques – 07 TLOG 022). Un algorithme de génération de tests et de vérifications minimales, qui utilise l'existence de sorties intermédiaires entre les sorties à tester et leurs entrées, a été en effet proposé lors de ce projet. Le temps imparti n'a cependant pas permis de prototyper ces nouveaux algorithmes et de les mettre en œuvre sur des cas industriels. Le projet VACSIM est l'occasion de vérifier le caractère réalisable et performant de ces nouvelles possibilités, qui correspondent à la levée d'un verrou technique important pour le problème de la réduction de la combinatoire du test des fonctions logiques critiques non bouclées. L'objectif final est de développer un prototype, intégré dans l'environnement ControlBuild, réalisant le test progressif par parties de systèmes logiques non-bouclés et de le mettre en œuvre sur des cas industriels.

L'objectif des travaux sur la validation par simulation de partie opérative est de proposer une méthode d'utilisation automatisée d'un simulateur de partie opérative, afin d'augmenter l'efficacité de la validation de la commande des systèmes critiques. On appelle simulateur de partie opérative un système qui, relié à la partie contrôle-commande (à l'état de spécification ou réelle), permet de réagir de manière cohérente aux sollicitations du contrôle-commande en lui fournissant des informations réalistes en entrée.

La validation de propriétés logiques à l'aide de techniques d'analyse des systèmes à événements discrets vise à étendre les résultats obtenus dans le projet TESTEC en matière de test de conformité de contrôleurs logiques et à développer de nouvelles techniques de validation basées sur l'analyse des évolutions d'un système bouclé contrôleur - simulateur de partie opérative.

La validation de propriétés quantitatives à l'aide de techniques de vérification de systèmes temporisés se divise en trois sous-tâches complémentaires, visant chacune une problématique particulière de validation : analyse quantitative des automates temporisés, validation à l'exécution (test, monitoring et enforcement), et vérification d'automates temporisés communicants.

La validation de propriétés quantitatives à l'aide de techniques de programmation par contraintes, quant à elle, comporte deux sous-tâches complémentaires, visant chacune une problématique particulière : génération et résolution des systèmes de contraintes sur les flottants et localisation des erreurs.

C.3 APPROCHE SCIENTIFIQUE ET TECHNIQUE

Les résultats décrits dans la section suivante ont été obtenus en se basant sur les compétences scientifiques des membres du consortium, en matière de modélisation et d'analyse des systèmes à événements discrets logiques et temporisés, de programmation par contraintes, de vérification formelle et test de conformité en particulier. La combinaison de ces techniques avec d'autres, telles que l'interprétation abstraite, l'identification ou la théorie des jeux, a été également investiguée.

Pour ce qui concerne les approches de test par parties et de simulation de partie opérative, les environnements de conception et simulation ControlBuild et Dymola ont été utilisés.

C.4 RESULTATS OBTENUS

Les résultats obtenus dans le domaine du test progressif par parties de systèmes logiques sont présentés dans les livrables 2 et 7 de la section D, ce dernier livrable étant un prototype logiciel dans l'environnement ControlBuild.
Globalement, ces résultats s'appuient sur une analyse plus approfondie du système de commande, afin de déterminer, pour chaque sortie, les entrées dont elle dépend comme cela était le cas précédemment, mais également les sorties intervenant dans le calcul de cette sortie, appelées sorties intermédiaires. L'utilisation de ces sorties intermédiaires autorise ainsi un test progressif par parties : la combinatoire se réduit en « masquant » les entrées des sorties intermédiaires par l'utilisation de ces sorties elles-mêmes. Les algorithmes élaborés en début de projet ont fait l'objet d'évolutions et d'optimisations au regard des expérimentations effectuées au cours du projet suite à l'implémentation de ceux-ci dans l'environnement ControlBuild. Ces travaux ont permis d'atteindre les résultats escomptés en début du projet. En effet, l'utilisation des sorties intermédiaires du système permet de réduire efficacement le nombre de vecteurs de test à jouer, tout en préservant l'exhaustivité des jeux de tests. Les cas industriels étudiés ont permis de démontrer que ce nombre de vecteurs de test évolue désormais de manière linéaire, proportionnellement au nombre d'entrées du système.

Les résultats obtenus dans le domaine de la validation par simulation de la partie opérative sont présentés dans les livrables 3 et 8 de la section D.
Le prototype logiciel faisant l'objet du livrable 8 opère sur un modèle de partie opérative sous la forme d'un assemblage de modèles pouvant être développés nativement dans l'outil et/ou provenant de logiciels capables de produire des modèles conformes au standard FMI (Functional Mock-up Interface), issu du projet ITEA2 MODELISAR. Ce prototype permet de définir les états normaux et stables de fonctionnement d'un système (par ex. les différents niveaux d'exploitation d'une centrale) ainsi que les événements pouvant survenir (évolution du système d'un état vers un autre, défauts mécaniques, défaillance du contrôle-commande, etc.). A partir de ces définitions, des scénarios sont générés de manière à positionner le système dans chacun des états définis pour introduire l'ensemble des événements en séquence. Deux cas d'étude ont été mis en place : le premier dans le domaine du transport ferroviaire, le second dans le domaine de la production électrique.

Les résultats en matière de validation de propriétés logiques à l'aide de techniques d'analyse des systèmes à événements discrets sont contenus dans les livrables 4 et 12 et dans certaines publications de la section E.
Les premiers résultats sur ce thème constituent une extension de ceux du projet TESTEC en proposant des modèles formels de spécification pour le test de conformité qui intègrent l'algorithme d'implantation de la spécification industrielle et des relations de conformité qui prennent en compte les caractéristiques technologiques des contrôleurs logiques industriels ; ces dernières permettent en particulier d'éviter des faux positifs ou négatifs et autorisent la construction en ligne de séquences de test. Par la suite, des

techniques d'analyse des évolutions du système bouclé contrôleur - partie opérative, et non plus du contrôleur isolé, ont été développées. Un critère d'arrêt de l'observation de ces évolutions a été proposé, en s'appuyant sur des résultats antérieurs en identification des systèmes à événements discrets.

Les résultats en matière de validation de propriétés quantitatives à l'aide de techniques de vérification de systèmes temporisés sont décrits dans les livrables 5, 10 et 13 et dans certaines publications de la section E.
La notion de « forgetfullness » a été tout d'abord introduite pour le calcul de l'ensemble des fréquences (proportion de temps de séjour dans des états marqués) d'automates temporisés multi-horloges. Pour ce qui concerne la validation à l'exécution de systèmes critiques, nous avons défini formellement et prouvé la correction d'une méthode d'enforcement à l'exécution de propriétés temporisées de sûreté et leur négation, les propriétés de co-sûreté, puis généralisé à toute propriété régulière (définie par des automates temporisés généraux). Ces travaux ont ensuite été étendus à des propriétés paramétrées, et appliquées à plusieurs études de cas. Un prototype logiciel validant cette approche a été développé et expérimenté dans le cas de propriétés de sûreté et co-sûreté et une extension du prototype aux propriétés régulières et paramétrées est en cours. Enfin, pour ce qui concerne la vérification d'automates temporisés communicants, les architectures de communication pour lesquelles la vérification de propriétés de sûreté est automatisable ont été caractérisées, en prenant une hypothèse d'évolution uniforme du temps dans tous les composants, ce qui implique que les horloges des composants soient parfaitement synchronisées. Nous cherchons actuellement à étendre ces résultats en relâchant cette hypothèse forte de synchronisation parfaite des horloges locales. D'autre part, nous avons élaboré des travaux permettant de prendre en compte le temps de propagation entre un testeur et une implémentation en utilisant un principe de jeu temporisé à deux joueurs.

Les résultats en matière de validation de propriétés quantitatives à l'aide de techniques de programmation par contraintes sont exposés dans les livrables 6, 11 et 14 et dans des publications de la section E.
En premier lieu, des techniques de simplification de modèles issues de la bio-informatique et pouvant être transposées au model-checking des systèmes informatiques ont été mises en évidence. Une stratégie de model-checking borné de programmes contenant des flottants a été également développée et appliquée à un cas d'étude fourni par Dassault Systèmes. Enfin, un état de l'art de la localisation d'erreurs à partir d'un contre-exemple a été effectué et a permis d'envisager des solutions issues de la programmation par contraintes (calcul d'ensembles insatisfaisables irréductibles notamment) pouvant répondre en partie à ce problème. Des logiciels «preuves de concept» ont également été développés : RAICP, basé sur l'interprétation abstraite et la programmation par contraintes pour une approximation fine des résultats d'un programme et la détection de fausses alarmes, et LocFaults, basé sur les techniques de programmation par contraintes sur les entiers pour l'aide à la localisation d'erreurs dans un programme impératif.

C.5 EXPLOITATION DES RESULTATS

L'exploitation industrielle des résultats dont le TRL est le plus élevé (test par parties et validation par simulation de la partie opérative) est en cours d'évaluation. En particulier, EDF étudie à ce jour l'utilisation industrielle des résultats sur le test par parties dans le cadre de la réalisation et de la modification de systèmes de contrôle-commande, pour plusieurs paliers en nucléaire notamment.

Les résultats plus académiques seront exploités dans le cadre de travaux de recherche futurs propres à chaque partenaire ou de projet coopératif (Projet Blanc ANR COVERIF par exemple).

C.6 DISCUSSION ET CONCLUSIONS

Les objectifs initiaux du projet sont très majoritairement atteints. Des activités d'industrialisation de certains résultats sont d'ores et déjà en cours. Pour les autres résultats, plusieurs pistes de recherche prometteuses ont été clairement identifiées afin d'en améliorer la portée.

C.7 REFERENCES

Cf. section E.2

D LISTE DES LIVRABLES

Date de livraison	N°	Titre	Nature (rapport, logiciel, prototype, données, …)	Partenaires (souligner le responsable)	Commentaires
Février 2013	1	Accord de consortium	Contrat	LURPA	
Septembre 2012	2	Algorithmes de génération et d'exécution du test des systèmes logiques, séquentiels et temporisés non-bouclés	Rapport	EDF	
Septembre 2012	3	Spécification et validation, sur études de cas, d'une méthode d'utilisation des simulateurs de parties opératives :	Rapport	EDF	
Juin 2013	4	Construction de modèles formels de contrôleurs logiques pour le test de conformité	Rapport	LURPA	
Avril 2013	5	Analyse quantitative des modèles temporisés	Rapport	LaBRI	
Juin 2013	6	Apport de la bio-informatique à la vérification des systèmes complexes	Rapport	I3S	
Décembre 2013	7	Algorithme de test progressif par parties de systèmes logiques non-bouclés dans l'environnement ControlBuild	Logiciel	Dassault Systemes	
Mars 2014	8	Utilisation automatisée du simulateur ControlBuild V	Logiciel	Dassault Systemes	
Abandonné	9	Validation par identification	Rapport	LURPA	Rapport fusionné avec le livrable 12
Avril 2014	10	Techniques de validation à l'exécution pour des systèmes réactifs critiques	Rapport	INRIA	
Septembre 2013	11	Vérification de propriétés quantitatives par résolution de systèmes de contraintes sur les flottants	Rapport	I3S	
Avril 2015	12	Validation fonctionnelle de contrôleurs logiques : contribution au test de conformité et à l'analyse en boucle fermée	Rapport	LURPA	
Avril 2015	13	Décidabilité et complexité du model-checking	Rapport	LaBRI	
Avril 2015	14	Système d'aide à la localisation des erreurs	Rapport	I3S	
Décembre 2015	15	Rapport de fin de projet	Rapport	LURPA	

E IMPACT DU PROJET

E.1 INDICATEURS D'IMPACT

Nombre de publications et de communications (à détailler en E.2)

		Publications multipartenaires	Publications monopartenaires
International	**Revues à comité de lecture**	2	6
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)	3	24
France	**Revues à comité de lecture**		1
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)		4

Autres valorisations scientifiques (à détailler en E.3)

	Nombre, années et commentaires (valorisations avérées ou probables)
Brevets internationaux obtenus	
Brevet internationaux en cours d'obtention	
Brevets nationaux obtenus	
Brevet nationaux en cours d'obtention	
Licences d'exploitation (obtention / cession)	
Créations d'entreprises ou essaimage	
Nouveaux projets collaboratifs	Projet Blanc ANR COVERIF "Vers une combinaison de l'interprétation abstraite et de la programmation par contraintes pour la vérification de propriétés critiques pour des programmes embarqués avec des calculs en virgule flottante", Partenaires : LIX, DI-ENS, I3S, LINA, retenu en 2015
Colloques scientifiques	
Autres (préciser)	Les résultats relatifs au test progressif par parties font l'objet d'une fourniture spécifique sous la forme d'un utilitaire rattaché à l'environnement de développement ControlBuild de Dassault Systèmes. EDF étudie à ce jour l'utilisation industrielle de cette nouvelle fonction de V&V dans le cadre de la réalisation et de la modification de systèmes de contrôle-commande, pour plusieurs paliers en nucléaire notamment. De plus, ces résultats ont suscité un intérêt clair de la part d'un constructeur nord-américain de matériel ferroviaire.

E.2 LISTE DES PUBLICATIONS ET COMMUNICATIONS

Liste des publications multipartenaires (résultant d'un travail mené en commun)		
International	**Revues à comité de lecture**	1. Constraint-Based BMC: A Backjumping Strategy. Hélène Collavizza, Le Vinh Nguyen, Olivier Ponsini, Michel Rueher, Antoine Rollet. International Journal on Software Tools for Technology Transfer (STTT Journal, 2012), 16(1), pp.103-121, 2014 2. Runtime enforcement of timed properties revisited. S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand, A. Rollet and O. Nguena-Timo. Formal Methods in System Design (FMSD) 45(3): 381-422 (2014)
	Ouvrages ou chapitres d'ouvrage	
	Communications (conférence)	1. Runtime enforcement of timed properties. S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand, A. Rollet, and O. Nguena Timo. RV12: International conference on Runtime Verification, Istanbul, Turkey, 10 2012, volume 7687 of Lecture Notes in Computer Science, 15p. Springer-Verlag. 2. Reachability of Communicating Timed Processes. L. Clemente, F. Herbreteau, A. Stainer, and G. Sutre. 16th Int. Conf. Foundations of Software Science and Computation Structures (FOSSACS'13), Rome, Italy, Mar. 2013, Lecture Notes in Computer Science, Springer, 2013 3. Enforcement of (Timed) Properties with Uncontrollable Events. M. Renard, Y. Falcone, A. Rollet, S. Pinisetty, T. Jéron, H. Marchand. 12th International Colloquium on Theoretical Aspects of Computing ICTAC 2015, Cali, Colombia

Liste des publications monopartenaires (impliquant un seul partenaire)		
International	**Revues à comité de lecture**	1. Reachability Analysis of Communicating Pushdown Systems. A. Heussner, J. Leroux, A. Muscholl, and G. Sutre. Logical Methods in Computer Science, 8(3:23):1-20, 2012. 2. Off-line test selection with test purposes for non-deterministic timed automata. N. Bertrand, T. Jéron, A. Stainer and M. Krichen. Logical methods in Computer Science 8(4), 2012 3. Efficient Emptiness Check for Timed Büchi Automata. F. Herbreteau, B. Srivathsan and I. Walukiewicz. Formal Methods in System Design, 40(2), pp. 122-146, Springer, 2012 4. Coarse Abstractions Make Zeno Behaviors Difficult to Detect. F. Herbreteau and B. Srivathsan. Logical Methods in Computer Science 9(1), 2013 5. Identifying suspicious values in programs with floating-point numbers Olivier Ponsini, Claude Michel and Michel Rueher. Automated Software Engineering (http://link.springer.com/article/10.1007/s10515-014-0154-2), May 2014, hal-00860681 6. Runtime Enforcement of Regular Timed Properties by Suppressing and Delaying Events. Y. Falcone, T. Jéron, H. Marchand, S. Pinisetty. To appear in Science of Computer Programming
	Ouvrages ou chapitres d'ouvrage	1. Symbolic methods in testing. T. Jéron, B. Wolff (eds.). Dagstuhl Reports (3)1, January 2013.
	Communications (conférence)	1. Better abstractions for timed automata. F. Herbreteau, B. Srivathsan and I. Walukiewicz. Proc. 27th ACM/IEEE Symp. on Logic in Computer Science (LICS), 2012 2. Safety Verification of Communicating One-Counter Machines. A. Heussner, T. Le Gall, and G. Sutre. Proc. IARCS Ann. Conf. Found. of Software Technology and Theor. Comp. Sci. (FSTTCS'12), Hyderabad, India, Dec. 2012, volume 18 of

		LIPIcs, pages 224-235. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012. 3. McScM: A General Framework for the Verification of Communicating Machines. A. Heussner, T. Le Gall, and G. Sutre. Proc. 18th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS'12), Tallinn, Estonia, Mar.-Apr. 2012, volume 7214 of Lecture Notes in Computer Science, pages 478-484. Springer, 2012. Note: Tool paper. 4. Safety Verification of Communicating One-Counter Machines. A. Heussner, T. Le Gall, and G. Sutre. In Proc. IARCS Ann. Conf. Found. of Software Technology and Theor. Comp. Sci. (FSTTCS'12), Hyderabad, India, Dec. 2012, volume 18 of LIPIcs, pages 224-235. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012 5. Frequencies in Forgetful Timed Automata. Amélie Stainer. 10th International Conference on Formal Modeling and Analysis of Timed Systems (Formats'12), London, UK, September 2012. Springer. 6. Lazy abstractions for timed automata. Computer Aided Verification. F. Herbreteau, B. Srivathsan, I. Walukiewicz. 25th International Conference CAV 2013, Saint Petersburg, Russia, 2013 7. Remote testing of timed specifications. A. David, M. Mikucionis, K. G. Larsen, O. Nguena-Timo and A. Rollet. In 25th IFIP International Conference on Testing Software and Systems ICTSS'13, Nov 13-15, 2013 Istanbul, Turkey, volume 8254 of Lecture Notes in Computer Science, p. 65-81, Springer-Verlag 8. Enforcing I/O sequences for PLC validation purposes. Anaïs Guignard, Jean-Marc Faure. 18th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA 2013), Cagliari (Italy), Paper n°89, 6 pages, September 2013 9. Algorithms For Error Localization On Numeric Constraints. Michel Rueher Seminar at NII (National Institute of Informatics, Tokyo), 6 November 2013 (conference invitée) 10. Generating Test Cases inside Suspicious Intervals for Floating-Point Number Program. Hélène Collavizza, Claude Michel, Olivier Ponsini and Michel Rueher. 6th Workshop on Constraints in Software Testing, Verification and Analysis (CSTVA'14) 11. Runtime Enforcement of Regular Timed Properties. S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand. In Software Verification and Testing, track of the Symposium on Applied Computing ACM-SAC 2014, Pages 1279-1286, Gyeongju, Korea, March 2014. 12. A conformance relation for model-based testing of PLC. Anaïs Guignard, Jean-Marc Faure. 12th IFAC - IEEE International Workshop on Discrete Event Systems (WODES), Cachan (France), pp. 412-419, 14-16 May 2014 13. Runtime Enforcement of Parametric Timed Properties with Practical Applications. S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand. In IFAC - IEEE International Workshop on Discrete Event Systems, Cachan, France, May 2014. 14. Model-based Conformance Test Generation for Timed Systems. T. Jéron. Invited talk. In IFAC - IEEE International Workshop on Discrete Event Systems, Cachan, France, May 2014 15. Generating Test Cases inside Suspicious Intervals for Floating-Point Number Program Hélène Collavizza, Claude Michel, Olivier Ponsini and Michel Rueher. Proc. of the 6th Int. Workshop on Constraints in Software Testing, Verification, and Analysis 16. Validation of logic controllers from events observation in a closed-loop system. A. Guignard, J-M. Faure. Emerging Technologies and Factory Automation (ETFA'14), 19th IEEE International conference on, Barcelona(Spain), 16-19 September, 2014 17. On Suspicious Intervals for Floating-Point Number

		Programs. Hélène Collavizza, Claude Michel, Olivier Ponsini, Michel Rueher, Mohammed Said Belaid. Dagstuhl Seminar 14351: Decision Procedures and Abstract Interpretation (conference invitée) 18. Acceleration of Affine Hybrid Transformations. B. Boigelot, F. Herbreteau and I. Mainz. Proc. 12th Int. Symp. on Automated Technology for Verification and Analysis (ATVA), 2014 19. Decidable Topologies for Communicating Automata with FIFO and Bag Channels. L. Clemente, F. Herbreteau, and G. Sutre. In Proc. 25th Int. Conf. Concurrency Theory (CONCUR'14), Rome, Italy, Sep. 2014, volume 8704 of Lecture Notes in Computer Science, pages 281-296. Springer, 2014 20. A new flow-driven and constraint-based error localization approach Mohammed Bekkouche, Hélène Collavizza, Michel Rueher. ACM SAC'15, SVT track, Apr 2015, Salamanca, Spain 21. TiPEX: a tool chain for Timed Property Enforcement during eXecution. S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand. In RV 2015, 15th International Conference on Runtime Verification, Vienna, Austria, September 2015 22. Improving search order for reachability testing in timed automata. F. Herbreteau and T.T. Tran. Proc. 13th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), 2015 23. Constraint-Based Error Localization. Mohammed Bekkouche, Hélène Collavizza, Michel Rueher.ICS 2015: INFORMS Computing Society Conference, January 2015 (conference invitée) 24. Quelques apports de la programmation par contraintes pour la vérification de programmes. Michel Rueher. Colloque sur l'Optimisation et les Systèmes d'Information COSI'2015, 1 au 3 Juin 2015, Oran, Algérie (conférence invitée)
France	**Revues à comité de lecture**	1. Formal models for conformance test of programmable logic controllers. Anaïs Guignard, Jean-Marc Faure. Journal Européen des Systèmes Automatisés (JESA), 2014
	Ouvrages ou chapitres d'ouvrage	1.
	Communications (conférence)	1. Génération d'une machine de Mealy à partir de spécifications algébriques à des fins de test de conformité. A. Guignard, J.-M. Roussel, J.-M. Faure. Conférence Internationale Francophone d'Automatique, pp.907-912, Grenoble, 4-6 juillet 2012 (http://hal.archives-ouvertes.fr/hal-00719363) 2. Un nouvel algorithme de consistance locale sur les nombres flottants. Said Mohammed Belaid, Claude Michel and Michel Rueher. Proc. of JFPC 2012 , pp. 211-219 3. Construction de modèles formels de contrôleurs logiques pour le test de conformité. A. Guignard, J.-M. Faure. 5èmes Journées Doctorales du GdR MACS, Strasbourg, 11-12 juillet 2013 4. Une approche CSP pour l'aide à la localisation d'erreurs. Mohammed Bekkouche, Hélène Collavizza, Michel Rueher. JFPC 2014.

E.3 LISTE DES ELEMENTS DE VALORISATION

Les résultats relatifs au test progressif par parties font l'objet d'une fourniture spécifique sous la forme d'un utilitaire rattaché à l'environnement de développement ControlBuild de Dassault Systèmes. EDF étudie à ce jour l'utilisation industrielle de cette nouvelle fonction de V&V dans le cadre de la réalisation et de la modification de systèmes de contrôle-commande, pour plusieurs paliers en nucléaire notamment.

E.4 BILAN ET SUIVI DES PERSONNELS RECRUTES EN CDD (HORS STAGIAIRES)

Identification				Avant le recrutement sur le projet			Recrutement sur le projet				Après le projet				
Nom et prénom	Sexe H/F	Adresse email (1)	Date des dernières nouvelles	Dernier diplôme obtenu au moment du recrutement	Lieu d'études (France, UE, hors UE)	Expérience prof. Antérieure, y compris post-docs (ans)	Partenaire ayant embauché la personne	Poste dans le projet (2)	Durée missions (mois) (3)	Date de fin de mission sur le projet	Devenir professionnel (4)	Type d'employeur (5)	Type d'emploi (6)	Lien au projet ANR (7)	Valorisation expérience (8)
Anaïs Guignard	F	anais.guignard@lurpa.ens-cachan.fr	Décembre 2015	Master recherche Ingénierie des Systèmes Complexes	France	0	ENS Cachan	Doctorant	41	28/02/2015	Ingénieur en CDI	PME	Ingénieur	non	oui
Olivier Ponsini	H	ponsini@i3s.unice.fr		Doctorat en Informatique	France	5	I3S	Ingénieur de recherche	24	31/12/2014	Ingénieur en CDI	PME	Ingénieur	non	oui
Srinivas Pinisetty	H	Srinivas.Pinisetty@inria.fr	Novembre 2015	Master	Pays-Bas	0	Inria	Doctorant	36	27/02/2015	Post-doc étranger	Enseignement et recherche publique	chercheur	non	oui
Nguena-Timo Omer	H	nguena@labri.fr	Mars 2015	Doctorat	France	8	LaBRI	Post-doc	11	01/09/2013	Post-doc étranger	EPIC de recherche	chercheur	non	oui
Clemente Lorenzo	H	lorenzo.clemente@labri.fr	Décembre 2013	Doctorat	Italie	3	LaBRI	Post-doc	12	18/11/2013	Post-doc étranger	Enseignement et recherche publique	chercheur	non	oui