

Projet ANR-06-SETI-015

RIMEL (Raffinement Incrémental de Modèles événementiels)

Rapport intermédiaire semestriel Juillet 2010

Coordonnateur Dominique Méry
LORIA, Université Henri Poincaré Nancy 1

Partenaire 2 Thierry Lecomte
ClearSy

Partenaire 3 Mohamed Mosbah
LABRI, Université Bordeaux I

Juillet 2010 à 10:00 P.M.

Résumé

Ce document présente une synthèse des résultats obtenus par les partenaires du projet RIMEL au cours des six derniers mois ; il comprend un rappel des objectifs de ce projet et une analyse des tâches associées aux livrables. En particulier, une description plus détaillée a été apportée dans les rapports précédents ; les résultats obtenus sont principalement attestés par des publications, des archives de modèles B et des spécifications de logiciels en cours de développement, notamment BART qui est diffusé par la société ClearSy et VISIDIA qui est diffusé au LABRI. Notre projet avait prévu un livrable sur l'intégration des aspects probabilistes au développement incrémental prouvé, ainsi qu'un livrable concernant les outils. L'extension du projet de 6 mois nous a conduit à différer de quelques mois le livrable sur les outils tout en mentionnant que les logiciels sont disponibles sur leur site respectif. Le site RIMEL (<http://rimel.loria.fr>) est à jour au moment de l'envoi de ce document à l'ANR.

1 Introduction au projet

Le projet RIMEL (Raffinement Incrémental de Modèles événementiels) concerne principalement le raffinement de modèles événementiels et la systématisation de cette technique dans le cadre d'applications ciblées notamment la conception d'algorithmes ou systèmes répartis. La systématisation de cette technique repose sur le développement de schémas conceptuels appelés *patrons de développement* s'appuyant sur une validation par la preuve (patrons de développement prouvés). Le développement du protocole IEEE 1394 a montré les limites du raffinement sur les aspects temps réel et probabilistes et conduit à rechercher à intégrer des extensions liées au traitement des aspects probabilistes et des contraintes éventuelles de temps. Le travail est organisé selon les directions scientifiques suivantes :

1. *Théorie du raffinement* : raffinement probabiliste, raffinement avec intégration de temps, prise en compte de contrainte de fatalité.
2. *Proof-based design patterns* : méthodologie d'ingénierie système formelle
3. *Self-Healing Systems et Algorithmes Répartis*
4. *Outils et diffusion*

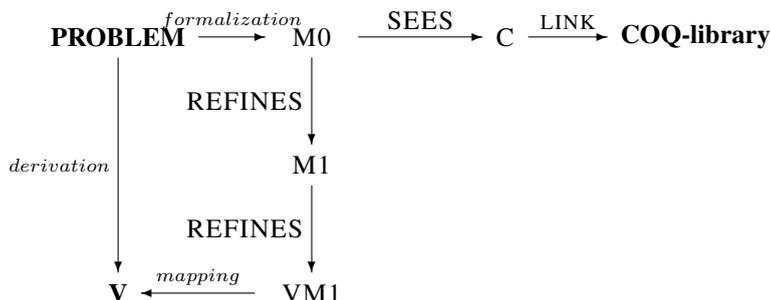
Les motivations de ce projet concernent principalement l'intégration de la preuve mathématique dans le processus de développement de systèmes informatiques, pour en justifier la confiance. Deux domaines d'applications sont exploités pour inférer et valider les apports méthodologiques du raffinement.

Le projet comprend plusieurs étapes identifiées par des livrables et correspondant à des étapes du projet.

- **Deliverable 1 Development of distributed algorithms** [1] : le projet s'appuie sur des études de cas constituées principalement de problèmes de l'algorithmique répartie et l'objectif est de les développer en utilisant la technique du raffinement. PUBLICATION À T0+12.

- **Deliverable 2 Integration of timing constraints in an incremental proof-based development** [2] : l'objectif est de mieux comprendre l'introduction d'éléments temporels dans le cadre du raffinement; certains algorithmes répartis reposent sur des hypothèses temporelles et serviront d'études de cas. PUBLICATION À T0+18.
- **Deliverable 3 Proof-based design patterns** [3] : Le développement incrémental et prouvé de systèmes répartis posent des problèmes de preuves et certains développements peuvent être rejoués ou réutilisés ; la notion de patron reste à définir et à concrétiser dans le cadre du projet. PUBLICATION À T0+18.
- **Deliverable 4 Formal system engineering** : Il s'agit de considérer non seulement des systèmes comme des algorithmes mais aussi des systèmes au sens général et de considérer le développement incrémental et prouvé dans ce cadre. PUBLICATION À T0+30.
- **Deliverable 5 Probabilistic incremental proof-based development** : Il est aussi important de considérer les systèmes où une loi de probabilité intervient de manière explicite ou implicite. PUBLICATION À T0+36.
- **Deliverable 6 Tools** : Cette tâche s'échelonne tout au long de ce projet et vise à fournir des outils pour la méthode de développement. PUBLICATION À T0+42.

Chaque livrable correspond à une étape accomplie au cours du projet ; la première année a permis des échanges sur les techniques de vérification (Coq et B) et sur la modélisation des systèmes répartis (Event B). Dans la proposition initiale, les systèmes *self healing* sont visés et les études de cas ont été poursuivies dans le cadre de ce type de systèmes. La notion de stabilité est très importante notamment dans le cas des systèmes comme les réseaux dynamiques ou les systèmes de routage. Au-delà des systèmes répartis logiciels, nous sommes aussi intéressés par les systèmes répartis intégrant des aspects matériels ; le challenge de ce projet est de combiner plusieurs approches complémentaires visant des systèmes de type algorithmique et de type industriel ; ainsi, une méthodologie fondée sur le raffinement, la preuve et la représentation des systèmes répartis est au cœur de nos travaux et en constitue un des objectifs. Nous[23] illustrons un schéma utilisé pour montrer les différentes étapes et les différents éléments que nous manipulons pour développer des algorithmes répartis; ce schéma témoigne aussi des liens entre les différents langages et formalismes utilisés durant notre projet.



La mise en évidence de patrons [2–5] devrait permettre de mieux expliquer cette méthodologie de développement et la rendre opérationnelle pour des utilisateurs moins experts. Rappelons que l'intérêt des systèmes algorithmiques est d'être maîtrisés par les partenaires académiques et que ces systèmes constituent un vivier très important d'études de cas non-triviales.

Dans le semestre passé, nous avons poursuivi les études de cas sous la forme de patrons et sous la forme de réutilisation de patrons et nous nous sommes focalisé sur le dernier livrable [6] qui décrit les outils réalisés. Parmi les études de cas poursuivies et enrichies, nous avons notamment le développement d'un modèle du pacemaker en utilisant les deux patrons action/réaction (Abrial) et temps(Rehm[26]); de plus, la partie sur Bart [14] montre aussi que le raffinement automatique constituait un cadre dans lequel il est important d'ajouter des règles de raffinement si on veut que ce raffinement soit effectif et efficace. Dans le cas de Bart, il y a évidemment un savoir-faire en plus à traduire dans la plate-forme. Enfin, les travaux sur les protocoles cryptographiques[8, 10] ont mis en avant la notion de mécanisme et les moyens de composer ces mécanismes pour construire des protocoles cryptographiques.

Dans ce dernier temps du projet, les partenaires ont acquis une maturité des techniques des autres partenaires et l'intégration du modèle des calculs locaux dans Event B constitue un témoignage en ce sens.

Nous allons revoir les actions du projet et nous allons commenter les résultats obtenus dans les derniers mois mais aussi préciser ce qui reste à faire dans les tâches mentionnées.

2 Actions du projet

Dans cette section, nous faisons un bilan intermédiaire de chaque action identifiée et en cours de réalisation ou terminée. Les réunions d'avancement nous ont permis d'échanger sur les techniques, modèles et outils utilisés par les différents groupes. Nous

donnons une description des actions menées ou qui sont apparues au cours du dernier semestre.

2.1 Action Algorithmes répartis développés incrémentalement et prouvés

Cette action a permis aux membres du projet d'échanger sur les algorithmes répartis et sur les techniques de vérification et de conception incrémentale prouvée pour les systèmes événementiels. Cette action aboutit à un livrable qui a repris les études de cas développées selon la méthode incrémentale prouvée et qui va aussi situer cette approche par rapport à l'approche suivie par le partenaire LABRI. Il est clair que le partenaire LABRI s'appuie sur une vérification *a posteriori* des algorithmes répartis et que cette vérification n'est pas encore effective sur le plan des outils de preuve ; l'assistant de preuve utilisé est Coq et une partie du travail de ce partenaire est de développer des bibliothèques de théories liées aux graphes et aux algorithmes répartis étudiés. Cependant, l'intérêt de la collaboration réside dans les échanges portant sur les algorithmes répartis et la description des principes de ces algorithmes. Ainsi, les échanges entre le partenaire LORIA et le partenaire LABRI ont permis de modéliser des algorithmes réputés non-triviaux dans un temps raisonnable. Au cours de notre exposé devant la commission d'évaluation, nous avons été interpellés sur les algorithmes de consensus et la question de les traiter a été posée par cette commission. D'une part nous avons des relations régulières avec L. Lamport sur ce type d'algorithme et d'autre part, il ne constitue pas un objectif en soi du projet initialement. Ce n'est pas le cas des algorithmes autostabilisants qui sont très complexes à vérifier et sont donc de vrais challenges pour leur conception incrémentale. Nous avons limité le livrable 1 [1] à quelques études de cas qui nous ont permis de comprendre le savoir-faire des uns et des autres au niveau des algorithmes répartis; la liste a été arrêtée en janvier 2008 mais les développements se sont poursuivis sur d'autres exmples. Si le partenaire LORIA reste plus familier avec le développement incrémental, il est assez clair que la comparaison des approches notamment avec des outils comme VISIDIA [18] est prometteuse. Les deux partenaires de cette tâche ont poursuivi le développement d'études de cas et échangent des expériences pédagogiques en lien avec les cours donnés en master à Nancy et à Bordeaux. Cet échange est important pour étudier le lien entre le plateforme RODIN et l'environnement VISIDIA. Notons que le LABRI et le LORIA ont poursuivi cet exercice de développement d'algorithmes répartis en lien avec la tâche des outils, notamment l'intégration de B et VISIDIA. Le bilan contractuel de cette action est consigné dans le livrable 1 [1].

Perspectives : Cette action a conduit au livrable [1] **Development of distributed algorithms** ; il présente une collection d'études de cas, afin de mieux comprendre les algorithmes répartis et leur conception mais aussi de dégager des patrons liés à ces algorithmes. Le travail de développement d'études de cas se poursuit en lien avec le partenaire LABRI [4, 12]. L'idée est d'échanger ces études de cas, afin de produire une description d'algorithmes répartis pour les étudiants de nos universités. Il s'agit aussi de développer des patrons ad hoc, notamment pour prendre en compte les notions de probabilités. Nous pensons aussi poursuivre les développements d'algorithmes cryptologiques [?], puisque nous avons acquis un certain succès dans cette voie; ces développements ont montré aussi les limites du prouveur. Bien que cette tâche soit soldée par un livrable [1], nous pensons poursuivre de tels développements notamment le consensus qui avait été demandé par le jury intermédiaire de l'ANR; nous allons aussi essayer de comprendre comment les probabilités pouvaient être intégrées à notre travail. De plus, le travail sur le lien entre les outils comme Event B, Coq via VISIDIA[18,23], est aussi un point s'appuyant sur ces études de cas qui favorisent les recherches en commun.

2.2 Action Intégration du temps dans le raffinement

Le temps joue un rôle fondamental dans de nombreux algorithmes répartis et nous étudions dans cette action l'introduction du temps au cours du développement incrémental. Des résultats ont été donnés et publiés [26] et nous avons publié des éléments étendant le modèle Event B avec des contraintes temps réel. Cette étude a mis en avant quelques patrons pour concevoir des modèles intégrant des aspects temps réel. Ainsi, la notion d'agenda a été mis en avant dans une telle démarche de modélisation. Nous avons aussi noté l'utilisation des patrons proposés dans cette tâche dans le projet TACOS, tout particulièrement l'équipe DEDALE de notre laboratoire; cela permet ainsi de montrer la généralité des patrons développés. De plus, les patrons sur le temps ontv été réutilisés et adaptés dans le cas de la modélisation de business process par des collègues de Newcastle du projet DEPLOY.

Perspectives : Cette action se focalise sur le temps dans les systèmes répartis mais au travers du raffinement et il convient de développer des solutions réparties en prenant soin de comprendre comment des patrons de développement peuvent aider dans cette démarche. Un livrable [2] a fait le point sur les éléments apportés et un article de revue [26]; ce document est publié en février 2010. Les résultats sur le pacemaker [20, 22] montrent que les patrons sur le temps sont utiles et sont réutilisés. Le travail de cette tâche conduit à la soutenance de la thèse de Joris Rehm en décembre 2009 [?] constituant un résultat très important.

2.3 Action Ingénierie système formelle

Cette action est aussi fondée sur le développement d'études de cas mais ces études de cas sont liées à des systèmes s'appuyant sur des éléments algorithmiques ou logiciels. Nous avons plusieurs résultats intermédiaires :

- le développement de systèmes de vote électronique et leur analyse
- l'étude du contrôle d'accès dans le cadre du raffinement[8]
- l'étude de patrons de développement[8]
- le développement de programmes séquentiels structurés [24] a mis en évidence un patron de développement qui a été introduit dans l'enseignement en master.

Ces travaux ont abouti à la mise en évidence de patrons de conception prouvés et ces premiers patrons sont décrits dans le livrable 3 [3]. L'idée est de clarifier la notion de patron dans le cadre du développement incrémental prouvé de systèmes. Nous considérons que ce point est assez central dans notre projet dans la mesure où il s'agit d'apporter une aide aux utilisateurs dans le développement incrémental prouvé. Dans cette action, nous avons utilisé les modèles d'attaques pour intégrer cet aspect dans le développement d'algorithmes cryptologiques et nous avons ainsi identifié un patron permettant de fusionner deux développements; cette technique [8, 10] a été utilisée dans le cas du modèle de Dolev et Yao et des algorithmes de transaction dont le Mondex avec cryptologie.

Perspectives Cette action se poursuit avec notamment les algorithmes répartis qui devraient fournir des patrons propres à leur développement. Les protocoles cryptographiques constituent des algorithmes répartis et sont intégrés au livrable 3 mais il convient d'exploiter les algorithmes plus complexes à comprendre comme ceux liés à l'autostabilisation. Un nouveau doctorant a débuté une thèse sur la modélisation d'un système complexe du Grand Challenge, le pacemaker. Ce travail[?] est déjà bien abouti mais il convient de nouer des relations avec le monde médical afin d'avoir un retour sur notre modélisation et comprendre leurs besoins.

2.4 Action Outils

Cette action vise à réaliser des outils dans le cadre du développement prouvé ; elle aura sans doute comme support principal la plateforme RODIN qui supporte la notation Event B et qui est ouverte au développement d'applications dans le cadre de l'atelier ECLIPSE. Cependant, notre partenaire industriel a fait un effort de développement de la version 4.0 de l'Atelier B et cette outil n'intègre pas la même syntaxe que celle de RODIN; nous veillerons donc à être aussi cohérent que possible avec les deux plate-formes. Deux outils sont réalisés:

- le développement d'un outil de raffinement automatique par la société ClearSy : il s'agit de BART; cet outil doit encore être validé par une société partenaire de ClearSy. Nous pourrions sans doute y intégrer certains patrons mais cela devrait être analysé prochainement.
- l'intégration de VISIDIA dans le cadre de la notation Event B et de RODIN: un ingénieur a visité le partenaire LORIA pour acquérir les compétences nécessaires en B et poursuit son travail de mise en œuvre du traducteur; cependant, cet ingénieur a quitté le LABRI et a été remplacé par un nouveau doctorant qui va visiter le LORIA pour poursuivre le développement de B2VISIDIA.

Le livrable 6 présente ces outils disponibles à partir du site de RIMEL.

Perspectives Cette action enrichira les applications disponibles sur la plate-forme RODIN notamment et VISIDIA. Il en va de même pour l'outil de raffinement automatique BART. Les travaux sur B2VISIDIA devraient se concrétiser par les travaux de deux nouveaux doctorants en septembre 2010.

3 Evolution du projet

Les activités du projet se poursuivent par des actions de dissémination et de rédaction de documents. Nous avons noté aussi que l'activité de développement et de redéveloppement est très importante et il est important de faire une place dans notre échéancier pour ces études de cas. D'une certaine mesure, le livrable 3 ne clôt pas les travaux sur les patrons mais constitue un embryon qu'il conviendra d'enrichir et de fonder sur le plan sémantique. On peut ainsi résumer la poursuite du travail comme suit:

1. Poursuivre les travaux sur les aspects temps réel notamment par la question des synchroniseurs mais aussi en lien avec le pacemaker.
2. Enrichir les patrons de développement notamment pour les algorithmes répartis
3. Etudes de cas pour les Self-Healing Systems et Algorithmes Répartis
4. Poursuivre les travaux sur le raffinement des aspects probabilistes.

5. Diffusion: cours d'algorithmique répartie
6. Démarrage de deux thèses sur le développement d'algorithmes répartis en collaboration entre LORIA et LABRI.
7. Préparation de projets

References

- [1] Projet ANR-RIMEL. Développement d'algorithmes répartis. Livrable RIMEL, LORIA, Janvier/Février 2008.
- [2] Projet ANR-RIMEL. Intégration de contraintes temps-réel au sein d'un processus de développement incrémental basé sur la preuve. Livrable RIMEL, LORIA, Juillet 2008.
- [3] Projet ANR-RIMEL. Proof-based design patterns. Livrable RIMEL, LORIA, Juillet 2008.
- [4] Projet ANR-RIMEL. Formal system engineering. Livrable RIMEL, LORIA, Juillet 2009.
- [5] Projet ANR-RIMEL. Probabilistic incremental proof-based development. Livrable RIMEL, LORIA, Décembre 2009.
- [6] Projet ANR-RIMEL. Tools. Livrable RIMEL, LORIA, Juin 2010.
- [7] N. Benaïssa and D. Méry. Cryptologic protocols analysis using Event B. In Alexander Marchuk, editor, *Seventh International Andrei Ershov Memorial Conference PERSPECTIVES OF SYSTEM INFORMATICS*, volume 5947. Springer, 15-19 June 2010.
- [8] Nazim Benaïssa. *La composition des protocoles de sécurité avec la méthode B événementielle*. PhD thesis, Université Henri Poincaré Nancy 1, May 2010.
- [9] Nazim Benaïssa and Dominique Méry. Cryptographic protocols analysis in event b. In *PSI 2009*, Russie Novosibirsk, 2009-11-11. Springer.
- [10] Nazim Benaïssa and Dominique Méry. Proof-based design of security protocols. In Farid Ablayev and Ernst W. Mayr, editors, *Computer Science- Theory and Applications 5th International Computer Science Symposium in Russia, CSR 2010*, number 6072, RUSSIE, KAZAN, 2010.
- [11] Dominique Cansell and Dominique Méry. Designing old and new distributed algorithms by replaying an incremental proof-based development. In Jean-Raymond Abrial and Uwe Glässer, editors, *Rigorous Methods for Software Construction and Analysis - Papers Dedicated to Egon Börger on the Occasion of His 60th Birthday*, number 5115, 2010.
- [12] Pierre Castéran and Vincent Filou. Tâches, types et tactiques pour les systèmes de calculs locaux. In *Journées Francophones des Langages Applicatifs*, pages 83–110, La Ciotat, Janvier 2010. Studia Informatica, Hermann Informatique.
- [13] J. Chalopin and Y. Métivier. On the power of synchronizations between two adjacent vertices. *Distributed computing*, 2010.
- [14] ClearSy. BART. <http://www.clearsy.com>, 2008.
- [15] A. El Hibaoui, Y. Métivier, J.-M. Robson, N. Saheb-Djahromi, and A. Zemmari. Analysis of a randomized dynamic timetable handshake algorithm. *Pure Mathematics and Applications (PuMA)*, 19(2-3):159–169, 2010.
- [16] A. El Hibaoui, J. M. Robson, N. Saheb-Djahromi, and A. Zemmari. Uniform election in trees and polyominoes. *Discrete Appl. Math.*, 158(9):981–987, 2010.
- [17] H. Hadj Kacem, M. Mosbah, N. Ouled Abdallah, and A. Zemmari. Broadcast in wireless mobile sensor networks with population protocols and extension with the rendezvous model. In *10th International Conference on New Technologies of Distributed Systems (NOTERE 2010)*, Tozeur, Tunisie, 31 mai - 2 juin 2010.
- [18] Laboratoire LABRI. Visidia, 2008 and 2010. <http://www.labri.fr/projet/visidia/>.
- [19] Laboratoire LABRI. B2visidia, 2010. <http://www.labri.fr/projet/visidia/>.
- [20] Dominique Méry and Neeraj Kumar Singh. Functional behavior of a cardiac pacing system (in Press). *International Journal of Discrete Event Control Systems*, 1, 2010.

- [21] Dominique Méry and Neeraj Kumar Singh. Real-time animation for formal specification. In *Complex Systems Design & Management (CSDM), Paris*, page (to appear), 2010.
- [22] Dominique Méry and Neeraj Kumar Singh. Technical Report on Formal Development of Two-Electrode Cardiac Pacing System. (<http://hal.archives-ouvertes.fr/inria-00465061/en/>), LORIA, 2010.
- [23] D. Méry, M. Mosbah, and M. Tounsi. Integrating local computation models by refinement. In *Symbolic Computation in Software Science (SCSS 2010)*, RISC, 2010.
- [24] Dominique Méry. Refinement-based guidelines for constructing algorithms. In Jean-Raymond Abrial, Michael Butler, Rajeev Joshi, Elena Troubitsyna, and Jim C. P. Woodcock, editors, *Refinement Based Methods for the Construction of Dependable Systems*, number 09381 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2010. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.
- [25] Dominique Méry, Mohammed Mosbah, and Dominique Méry. Proving Distributed Algorithms by Combining Refinement and Local Computations. In *AVOCS 2010 10th International Workshop on Automated Verification of Critical Systems*, 2010.
- [26] Joris Rehm. Proved development of the real-time properties of the ieee 1394 root contention protocol with the event-b method. *International Journal on Software Tools for Technology Transfer (STTT)*, 12, fevrier 2010.