Les projets de recherche sur B

Henri Habrias
henri.habrias@univ-nantes.fr

> En doutant, nous nous mettons en recherche, et en cherchant, nous trouvons la vérité.
>
> Pierre Abélard, le philosophe du Pallet

1 Pojet MIST, Measurable Improvement with Specification Techniques

"The objective of this experiment is to improve the quality of design and control of safety attributes in the development of safety critical software. This will be done by introducing formal specifications into the software development process. Features of the formal specification which contribute to improvement will be identified. Comparisons of data collected will be made and quantifiable benefits defined. Procedures will be developed to document the process and quality and cost metrics will be defined to set process improvement targets.

We propose to use the Abstract Machine Notation of the B Method supported by the B Toolkit supplied by B Core (UK). The project consists of GEC-Marconi Avionics, who are the Prime User. Praxis who are the main subcontractor and B Core(UK), who are the vendor providing the B technology, training courses and consultancy.

The B Toolkit is supplied by B Core (UK), Oxford. The B system is a complete system for computer aided development. The technology consists of

— The B Method for software development, covering all tasks from high level specifications through design to detailed coding and maintenance. The method was invented by Jean Raymon Abrial.
— The B Toolkit, providing extensive support for the use of the B Method.
— The B Tool which is the common platform for the B Toolkit and provides a program based on a pattern matching and rule rewriting mechanism for the introduction, manipulation and analysis of formal objects.

The B Method is designed to provide a homogeneous language and a methodology for the formal specification, design and implementation of industrial scale software systems. The method allows the specification to be constructed and verified in an incremental way and existing specifications can be reused. It also promotes separate verification and proof by using semi hiding principles. The method uses the Abstract Machine Notation as the language for specification, design and implementation within the process.

The B Toolkit supports the method over the software development phases from specification to implementation. It comprises automatic and interactive theorem proving assistants and a set of software development tools : an abstract machine notation type checker, a specification animator and code generators integrated with the proof assistants." Projet de la Commission Européenne

"Measurable Improvement in Specification Techniques (MIST) is ESSI application experiment 10228. MIST is a 16 month project involving three companies :GEC-Marconi Avionics, who are the prime user; Praxis, who are the main subcontractor, acting as an independent reviewer; and B-Core (UK),who provide the tools used and consultancy. The main aims of MIST are to develop procedures for using formal methods with current methods on safety critical avionics software and to collect metrics to enable reasonable estimates for the use of these procedures"

Jonathan Draper, Mission Avionics Division, GEC-Marconi Avionics Ltd, *The use of the B-Method on an Avionics Example - the MIST project*, 8th Conference on : Putting into practice methods and tools for information system design, First Conference on the B method, Nov. 25-27, 1996, Nantes, Proceedings, ISBN : 2-906082-25-2, p. 303 Jonathan Draper, *Applying the B-Method to Avionics Software : An Initial Report on the MIST Project*, In : Shaw, R. (eds) Safety and Reliability of Software Based Systems. Springer, London, pp. 288-304

2 SPECTRUM, Improved competitiveness through integration and automation of complementary formal approaches in the development process

"Customer standards for the development of safety critical software strongly advocate a formal approach. Viable formal methods require industrial strength tools supporting a wide spectrum of the software development lifecycle.

SPECTRUM draws together four users partners each charged with safety-critical software development in different application domains : GEC Marconi Avionics (GMAv) in avionics systems, Dassault Electronique (DE) in terrestrial transport embedded control, Commissariat à l'Energie Atomique (CEA) in nuclear plant control, and Space Software Italia (SSI) in satellite communication control. Each user perceives requirements beyond the formal software development support currently available to them and each has a need to integrate such support into their existing working environments.

The integration and increased automation of existing commercially available support technologies is seen as a pragmatic way of meeting these user needs. Hence SPECTRUM brings together IFAD (VDM-SL Toolbox) and B-Core (B-Toolkit) as its technology providers. Such integration requires basic but tractable research focused by user requirements and the Rutherford Appleton Laboratory (RAL) fills SPECTRUM's role of coordinator and strategic researcher.

The objective of the SPECTRUM project is to assess the feasibility and derived benefits from the integration and automation of commercial VDM and B formal technologies.

Contrary to past method proliferation, SPECTRUM seeks to integrate two complementary market offerings. This approach will be assessed through a number of user scenarios in a variety of application domains. SPECTRUM's technology results are expected to bring greater user satisfaction from an earlier use of analysis in development, reducing specification and design defects, and a greater availability of automation, such as an automated derivation of test-cases and test-harnesses from specifications. The acquired evidence of the application

of formal methods across a spectrum of safety critical subdomains and across a spectrum of user backgrounds are anticipated to encourage a more mainstream adoption of formal methods.

The project is a feasibility study. It will demonstrate potential business benefits derived from greater competitiveness through decreased delivery and maintenance costs and improved quality. GMAv is already able to report benefits in applying rigour and formality to parts of its development life-cycle, whilst the other users wish to share that experience.

SPECTRUM's users expect to improve and extend their current use of formal methods, anticipating further reductions in the overall cost of their formal development and improved customer satisfaction through improved product quality.

SPECTRUM's suppliers believe that method and tool integration will foster greater market penetration than is currently achievable individually." Programme FP4-ESPRIT 4 - Specific research and technological development programme in the field of information technologies, 1994-1998 1-01-
textbf1997, 30-091997

3 Projet BOM (B Optimisant la Mémoire)

Projet RNTL[1] " Le but était d'obtenir un traducteur du langage B vers le langage C, facilement adaptable à des contraintes mémoire (logiciels embarqués sur cartes à puce)"

Frédéric Badeau, Didier Bert, Sylvain Boulmé, Claude Métayer, Marie-Laure Potet, et al.. Adaptabilité et validation de la traduction de B vers C - Points de vue du projet BOM. Revue des Sciences et Technologies de l'Information - Série TSI : Technique et Science Informatiques, 2004, Approches Formelles pour le Développement de Logiciels, 23 (7), pp. 879-90

Marie-Laure Potet. Spécifications et développements formels : Etude des aspects compositionnels dans la méthode B. Document d'HDR, Institut National Polytechnique de Grenoble - INPG, 2002. M-L Potet, Etude du passage de paramètres de la méthode B en vue d'optimisere la mémoire, Annexe Rapport Projet RNTL BOM in pp.147-158

Frédéric Badeau, Didier Bert, Sylvain Boulmé, Christophe Métayer, Marie-Laure Potet, Nicolas Stouls et Laurent Voisin. Adaptabilité et validation de la traduction de B vers C - Points de vue du projet BOM(.bib), Technique et Science Informatiques, RSTI, série TSI, numéro 7/2004, Hermès-Lavoisier

D. Bert, S. Boulmé, M-L. Potet, A. Requet, L. Voisin. Adaptable Translator of B Specifications to Embedded C Programs. in FM 2003 : Formal Methods, LNCS 2805, pp. 94-113, Pise, Sept. 2003

Les deux projets suivants ont été financés par l'Union Européenne, CT Project ADVANCE (2011 à 2014)

1. Réseau National en Technologies Logicielles (RNTL)

Le Réseau National de recherche et d'innovation en Technologies Logicielles (RNTL) a été mis en place, fin 1999, par le ministère de la Recherche et le ministère de l'Industrie. Le RNTL a été renouvelé en 2005, dans le cadre de l'Agence Nationale de la Recherche (ANR). Il a reçu comme mission de favoriser la constitution de projets innovants de recherche et de développement coopératif entre entreprises et équipes de la recherche publique.

4 Projet Rodin, Rigorous Open Development Environment for Complex Systems

(2004 à 2007)

The Rodin Platform is an Eclipse-based IDE for Event-B that provides effective support for refinement and mathematical proof. The platform is open source, contributes to the Eclipse framework and is further extendable with plugins. `https://www.eclipse.org/downloads/`

> The Eclipse Foundation Specification Process (EFSP) provides an open and transparent framework for the development of community-driven, open source-friendly specifications

Michael J. Butler, Cliff B. Jones, Alexander Romanovsky, Elena Troubitsyna (Eds.) : *Rigorous Development of Complex Fault-Tolerant Systems* [FP6 IST-511599 RODIN project]. Lecture Notes in Computer Science 4157 Springer 2006, ISBN 3-540-48265-2

Les sites créés sur la Toile à l'occasion de ces projets ne sont pas toujours maintenus. Actuellement, il faut aller sur `https://wiki.event-b.org/index.php/Main_Page`. Mais dans la cadre des conférences ABZ (The ABZ conference is dedicated to the cross-fertilization of state-based and machine-based formal methods, like Abstract State Machines (ASM), Alloy, B, TLA, VDM and Z, that share a common conceptual foundation and are widely used in both academia and industry for the design and analysis of hardware and software systems. The conference aims for a vital exchange of knowledge and experience among the research communities around different formal methods) , a lieu un Rodin Workshop.

5 Projet DEPLOY, (Industrial deployment of system engineering methods providing high dependability and productivity)

2008 à 2012 ICT 214158 DEPLOY

6 Une plate-forme mécanisée et basée sur la preuve pour la vérification d'obligations de preuve B – BWare

INS - Ingénierie Numérique & Sécurité

" Le projet BWare est un projet de recherche industrielle qui a pour objectif de produire un environnement mécanisé pour prendre en charge la vérification automatique d'obligations de preuve provenant du développement d'applications industrielles utilisant la méthode B et exigeant de fortes garanties de confiance. Il concerne donc l'axe thématique 1 (« Ingénierie du logiciel et du matériel ») et l'axe thématique 2 (« Ingénierie Numérique & Sécurité ») de l'appel à projets « Ingénierie Numérique & Sécurité ».

La méthodologie utilisée par ce projet consistera à construire une plate-forme générique de vérification reposant sur différents outils de démonstration,

tels que des outils de démonstration au premier ordre et des solveurs SMT (« Satisfiability Modulo Theories »). La variété de ces outils de démonstration a pour objectif de permettre de démontrer automatiquement un large panel d'obligations de preuve avec notre plate-forme. La majeure partie des outils de vérification utilisés dans BWare a déjà été utilisé dans des expérimentations, qui ont consisté à vérifier des obligations de preuve ou des règles de preuve provenant d'applications industrielles. Cela devrait donc constituer un facteur décisif pour réduire les risques du projet, qui peut alors se concentrer sur la conception de plusieurs extensions pour les outils de vérification afin de traiter un plus grand nombre d'obligations de preuve.

Au-delà de l'aspect multi-outils de notre méthodologie, l'originalité du projet BWare réside également dans l'obligation pour les outils de vérification de produire des objets preuves, qui sont à vérifier indépendemment. Ce « backend » devrait nous permettre non seulement d'accroître la confiance dans les preuves produites, mais aussi de fournir de l'interopérabilité entre outils de démonstration. Le succès de BWare sera assuré par une large collection d'obligations de preuve fournie par certains des partenaires industriels de ce projet, qui développent soit des outils implantant la méthode B ou des applications impliquant l'utilisation de la méthode B.

Ce projet combine quatre types différents d'expertise : production d'obligations de preuve pour la méthode B ; traduction de la théorie des ensembles vers la logique du premier ordre ; démonstration automatique ; production et vérification de preuves. Le consortium de BWare associe des entités académiques (CEDRIC, LRI et Inria) et des partenaires industriels (Mitsubishi Electric R&D Centre Europe, ClearSy et OCamlPro). Cela assurera un excellent niveau d'expertise pour les aspects scientifiques, ainsi que pour leur exploitation pour le développement de logiciels exigeant de fortes garanties de confiance.

L'organisation du projet consiste en plusieurs parties. Parmi ces parties, il y a une étude théorique concernant la génération d'obligations de preuve, ainsi que la formalisation de plusieurs modèles pour la théorie des ensembles sous-jacente à la méthode B. Cette partie servira à une autre partie concernant la conception d'une plate-forme de vérification, qui réunira plusieurs outils, et des extensions de ces outils seront considérées et développées. Cette plate-forme sera intégrée à l'outil d'un partenaire industriel (l'Atelier B de ClearSy) pour une évaluation sur des applications industrielles et une comparaison avec d'autres outils de vérification similaires. Une activité de preuve interactive sera également conduite de manière à combiner de façon optimale les outils de démonstration automatique, et des optimisations des outils de vérification seront aussi étudiées.

La dissémination des résultats sera assurée par un site web, des publications, l'organisation de séminaires (et éventuellement des workshops), et un accès libre à la plate-forme de vérification. La diversité des membres du consortium aidera à promouvoir assez largement les résultats de ce projet dans différentes communautés, telles que les académiques, les acteurs industriels, les développeurs et les utilisateurs." Coordinateur : David DELAHAYE (Centre d'Étude et De Recherche en Informatique et Communications (CEDRIC)) **August 2012** - 48 Mois

7 Augmenter les outils de raisonnement sur le langage B par des techniques SAT et SMT – BLaSST

"Le projet BLaSST vise à établir un pont entre des techniques combinatoires et symboliques en déduction automatique en vue de résoudre des obligations de preuves issues de modèles B. Les travaux contribuent à avancer l'état de l'art en déduction automatique, notamment les techniques SAT et SMT, et à rendre ces techniques plus largement disponibles pour la vérification de logiciels. Plus concrètement, des encodages, d'optimisations des techniques de résolution ainsi que la construction de modèles et la suggestion de lemmes seront considérés. En recombinant ces avancées, l'impact scientifique attendu est (i) un taux d'automatisation élevé grâce à des techniques de raisonnement en logique de l'ordre supérieur ainsi qu'à des techniques d'instanciation énumérative pour des domaines finis et (ii) des retours utiles en cas de conditions de vérification qui ne peuvent être démontrées correctes. L'efficacité des méthodes issues du projet sera quantifiée en les appliquant à des collections de problèmes fournies par le partenaire industriel. L'impact dans l'industrie sera une productivité accrue des ingénieurs de vérification. Les collections de problèmes et les outils de résolution seront mis à disposition publiquement, avec des licences open-source permissives." Coordinateur : Stephan Merz (Centre de Recherche Inria Nancy - Grand Est) **February 2022** - 48 Mois

8 Méthode outillée de modélisation formelle des exigences pour des systèmes complexes critiques – FORMOSE

"Le projet Formose est un projet de recherche industrielle dont l'objectif est de produire une méthode formelle d'ingénierie des exigences (IE) orientée modèles pour des systèmes complexes critiques, supportée par un outil libre. C'est un projet de 48 mois auquel participent 2 partenaires académiques (LACL – porteur du projet –, Institut Mines-Telecom) et deux partenaires industriels (THALES, ClearSy). L'IE est un processus critique dans la conception de logiciels et de systèmes. Une part importante des coûts de développement logiciel ou système est d'ailleurs imputable à la compréhension du domaine et des exigences. Cependant, les pratiques industrielles actuelles ne sont pas assez efficaces. Elles consistent principalement en processus « maison », retour d'expérience et outils de gestion des exigences (macros dans des outils de traitement de texte, outils de « traçabilité » et base de données d'exigences). Même si ces dernières années de nombreux projets de recherche ont produit des avancées notables et ont atteint un niveau de maturité suffisant, des études récentes ont montré que des problèmes persistent. Le projet Formose vise à résoudre plusieurs défis soulevés par ces problèmes, en particulier les plus cruciaux pour les systèmes complexes critiques. Ils concernent la nécessité de prendre en compte la grande complexité de ces systèmes, d'une meilleure intégration de l'IE avec les techniques de vérification et de validation pour assurer une meilleure qualité des exigences, et plus généralement d'un guide méthodologique et d'un support outillé pour accom-

pagner le processus de construction de modèles des exigences. Les principaux résultats du projet seront les suivants. Tout d'abord, nous définirons un langage de modélisation des exigences intégrant les concepts de base de langages existants comme KAOS ou Tropos/i*, tout en ajoutant de nouveaux concepts pour tenir compte des caractéristiques propres des systèmes complexes critiques : leur architecture abstraite sera considérée en permettant la modélisation des exigences à plusieurs niveaux d'abstraction tout en assurant leur cohérence ; le langage permettra de spécifier les exigences non fonctionnelles de sûreté et de performance mais aussi les exigences induites par l'existence de différents modes opératoires et de reconfigurations. Le langage sera multi vues (langage naturel, notations graphiques et formelles), pour être compréhensible par toutes les parties prenantes. Pour l'aspect vérification, nous utiliserons des méthodes formelles complémentaires existantes, supportées par des outils efficaces : la méthode B et le model-checker temporisé UPPAAL. Puis nous définirons un processus personnalisable pour guider les ingénieurs dans leurs différentes activités de construction d'un modèle des exigences. Nous utiliserons la plate-forme OpenFlexo pour supporter la mise en oeuvre de ce processus. Elle intègrera les outils ad hoc développés dans le projet et les outils de vérification existants. Elle sera capable d'envoyer des obligations de preuve aux prouveurs, de recevoir la réponse de ces prouveurs et de les interpréter pour les présenter aux utilisateurs en utilisant les représentations adéquates. Enfin, pour s'assurer de la pertinence des résultats, la méthode et les outils seront évaluées tout au long du projet sur les études de cas fournies par les partenaires industriels. De plus, les ingénieurs de THALES et ClearSy seront des utilisateurs actifs de la méthode et des outils pour donner des retours réels sur leur utilisabilité. Clearsy assurera l'exploitation et la maintenance des outils de vérification existants. Elle sera capable d'envoyer des obligations de preuve aux prouveurs, de recevoir la réponse de ces prouveurs et de les interpréter pour les présenter aux utilisateurs en utilisant les représentations adéquates. Enfin, pour s'assurer de la pertinence des résultats, la méthode et les outils seront évaluées tout au long du projet sur les études de cas fournies par les partenaires industriels. De plus, les ingénieurs de THALES et ClearSy seront des utilisateurs actifs de la méthode et des outils pour donner des retours réels sur leur utilisabilité. Clearsy assurera l'exploitation et la maintenance des outils après la fin du projet et THALES développera la version industrielle des outils. La dissémination des résultats sera assurée par un site web, des publications dans des revues et conférences internationales et nationales, ainsi que la disponibilité gratuite de la plate-forme. Nous envisageons également de communiquer avec la communauté industrielle du domaine des systèmes complexes critiques." Coordinatrice : Régine Laleau (Université Paris-Est Créteil Val de Marne - Laboratoire d'Algorithmique, Complexité et Logique) **September 2014** - 48 Mois

9 CE25 - Sciences et génie du logiciel - Réseaux de communication multi-usages, infrastructures de hautes performances, Assistants de preuve basés sur la théorie des ensembles interopérables et sûrs – ICSPA

"Les méthodes formelles déductives visent à améliorer la qualité des logiciels à l'aide d'outils qui sont construits sur des fondements mathématiques solides, tels que la théorie des ensembles. Ces outils permettent à leur utilisateur de démontrer des propriétés de correction d'un programme par rapport à ses spécifications. La confiance dans ces preuves est donc un enjeu crucial, alors même que l'implémentation des prouveurs est complexe et parfois entachée d'erreurs.

L'objectif d'ICSPA est de renforcer la confiance dans les preuves mécanisées qui sont au coeur des formalismes B, Event-B et TLA+ de spécification fondées sur la théorie des ensembles. Ces environnements de développement sûr sont utilisés dans de nombreux projets industriels, là où la correction logicielle est un besoin critique. Notre projet a aussi pour objectif l'établissement d'un cadre de partage, afin que ces trois systèmes puissent s'échanger leurs preuves et leurs théories, ce qui rendra interopérable les outils respectifs, Atelier B, Rodin et TLAPS.

Notre stratégie pour cela est de vérifier, de manière formelle et indépendante, les preuves produites par ces outils avec Dedukti, un vérificateur de preuves suffisamment simple pour être facilement expertisable, voire ré-implémentable. Par sa structure versatile Dedukti offrira une base commune qui ouvrira la possibilité aux développeurs de B, Event-B et TLA+ de partager et de réutiliser entre les systèmes leurs résultats et formalisations. Cette approche est inspirée de Logipedia, une petite bibliothèque de résultats mathématiques qui peuvent être exportés vers, et vérifiés par, un large spectre de cadres logiques, entre autres Coq et HOL.

Pour atteindre nos objectifs, nous exprimerons les théories des ensembles qui sous-tendent les trois langages de spécifications en Dedukti, puis nous exporterons leurs traces de preuves, afin de les revérifier indépendamment avec Dedukti. Ce mécanisme formera le noyau d'une fonctionnalité plus ambitieuse d'export de modèles complets, utilisés en pratique pour le développement de logiciel pour les systèmes critiques, en mettant un accent particulier sur les Systèmes de transition d'états étiquetés (LTS). Toutes ces données permettront la mise au point de traductions entre les trois systèmes au niveau de Dedukti, et de procédures d'import dans les trois outils Atelier B, Rodin et TLAPS. Un outil pourra alors utiliser ce qui aura été défini ou prouvé dans un autre.

Cette architecture sera étayée par des fonctionnalités de reconstruction de preuve, fournies par des prouveurs automatiques qui permettront la complétion automatique des traces de preuves reçues en entrée, souvent incomplètes car de niveau d'abstraction relativement élevé. La reconstruction sera assistée par des points d'ancrage supplémentaires qui résulteront d'une mise en correspondance horizontale entre les outils des définitions et concepts.

Cette méthodologie sera testée et évaluée sur un large corpus d'obligations de preuve fournies par notre partenaire industriel. De plus, des cas d'étude démontrant l'interopérabilité seront mis en oeuvre. Enfin, outre la dissémination

académique et éducative, Atelier B intégrera l'import et l'export de preuves, la complétion automatique de celles-ci, ainsi que leur vérification, et exploitera les résultats d'ICSPA à une échelle industrielle." Coordinatrice : Catherine Dubois (Télécom SudParis) **December 2021** - 48 Mois

10 Déduction Certifiée – DECERT

"Les niveaux les plus élevés des standards de développement logiciel, comme le niveau EAL7des Critères Communs pour la certification de systèmes et des composants critiques, exigent l'utilisation de techniques formelles fondées sur des sémantiques mathématiques strictes. Ces techniques sont mécanisées par le biais d'outils déductifs qui permettent de démontrer des propriétés portant sur les logiciels. Notre vision à long terme est de contribuer à rendre l'utilisation de tels outils économiquement viable et, autant que possible, de rendre l'utilisation de méthodes formelles invisible aux développeurs et aux utilisateurs de systèmes. Afin que cette vision puisse se réaliser sur une échelle plus étendue, des composants automatisés et performants doivent interagir et forger un environnement de confiance pour le développement et/ou le déploiement de systèmes. L'objectif du projet DECERT est de concevoir une architecture pour des procédures de décision coopérant entre elles, avec une attention particulière portée à des fragments de l'arithmétique (arithmétiques bornée et non-bornée, sur les entiers et les réels, ...) et à leur combinaison avec d'autres théories concernant les structures de données (listes, tableaux, ensembles, ...). Pour garantir une confiance globale dans cette combinaison d'outils, les procédures de décision seront soit prouvées correctes à l'intérieur d'un assistant de preuve, soit produiront des certificats de résultat qui permettront à des outils extérieurs de vérifier la validité de leurs réponses. Nous définirons un format normlisé pour des témoins de preuves adapté aux procédures de décisions et leurs combinaisons. Ces témoins de preuve devront être produits sans trop de surcoût par les procédures de décisions et certifiés de manière efficace par les noyaux des assistants de preuve. Nous proposons d'utiliser ces procédures dans plusieurs scénarii d'application provenant à la fois du milieu académique et industriel et qui demandent des garanties élevées de confiance. En développement prouvé de systèmes, des modèles de haut niveau sont généralement écrits dans des langages expressifs de modélisation tels la logique d'ordre supérieure, B ou TLA+ et dont les problèmes de vérification ne peuvent être entièrement automatisés. Dans ce contexte, des procédures de décision automatiques doivent interagir avec des assistants de preuve comme Coq ou Isabelle, sans que les assurances fortes de correction associées à l'utilisation de ceux-ci soient compromises. Le deuxième scénario d'application que nous étudierons concerne l'utilisation de code téléchargé sur des plates-formes non dignes de confiance à travers le paradigme du code porteur de preuve (PCC : Proof Carrying Code). Afin de s'assurer que le code soit conforme à une politique de sûreté précise, il est assorti d'une preuve qui peut être généré par un outil de déduction automatique et qui est certifiée correcte sur le site hôte par un vérificateur de confiance. Dans les deux scénarii, la confiance repose sur un environnement de confiance fondé sur des certificats sous la forme de traces de preuve. En résumé, le projet se concentre sur les trois problèmes suivants : 1. Développer et implémenter des nouvelles et efficaces procédures de décision coopératives, en particulier pour des fragments de

l'arithmétique. 2. Développer et standardiser une interface de sortie basée sur des certificats et des objets de preuve. 3. Intégrer les points 1 et 2 dans des assistants de preuve sceptiques, dans une architecture pour le code porteur de preuve et dans des outils de vérification tels que l'outil Rodin pour B et l'outil Frama-C du CEA pour la vérification de programmes C." Coordonnateur : Thomas JENSEN Début et durée du projet scientifique : - 36 Mois

11 Enrichissement de EventB et de RODIN : EventB-Rodin-Plus – EBRP-EventB-Rodin-Plus

"Le développement de systèmes complexes à logiciel prépondérant nécessite la conception de modèles de systèmes correspondant à différentes vues de ce système dans différents domaines d'analyse. La conception de ces modèles nécessite des connaissances spécifiques issues de plusieurs disciplines scientifiques. Par exemple, dans le cas de systèmes autonomes, la modélisation de comportements et d'interactions de systèmes requiert des concepts issus de la théorie du contrôle tels que des équations différentielles, des protocoles de communication ou d'allocation de ressources, des règles pour le contrôle d'accès etc.

Les méthodes formelles à base d'état explicite ont prouvé leur efficacité pour développer de tels systèmes . Une des méthodes, ayant obtenu de nombreux succès dans son utilisation, est la méthode Event-B et son environnement de développement RODIN. Ils sont au cœur de la proposition du projet EBRP. Actuellement, Event-B et RODIN offrent : - un langage de modélisation, équipé d'une sémantique formelle fondée sur la théorie des ensembles et la logique du premier ordre, permettant de concevoir des modèles à états explicites et d'exprimer des propriétés de systèmes, en particulier la sûreté ; - une opération de raffinement, explicitement définie, pour modéliser des mécanismes de décomposition/composition permettant de définir des développements incrémentaux, en plusieurs étapes de raffinement, partant d'un modèle abstrait initial pour aboutir à un modèle concret du système en cours de conception ; - un système de preuve pour prouver les obligations de preuve engendrées à partir des modèles.

Bien qu'Event-B et sa plate-forme RODIN mettent en œuvre le développement de systèmes nécessitant la formalisation de concepts de domaines d'ingénierie (ex. réels, protocoles de communication, classes, calculs de processus, allocation de ressources, contrôle d'accès) absents du noyau d'Event-B, cette formalisation requiert des modèles définis à partir des concepts du noyau d'Evenyt-B (théorie des ensembles, logique des prédicats, arithmétique sur les entiers). Cette chaîne de modélisation est complexe et la réutilisation de modèles et de preuves peut devenir fastidieuse.

L'objectif scientifique de EBRP est de permettre le développement de modèles de systèmes avec Event-B référençant explicitement, dans des théories de domaine, des concepts vus comme des objets de première classe. Il peut être atteint en étendant Event-B et RODIN par des théories de domaine (et des mécanismes d'import/export) formalisant ces différents concepts.

Pour atteindre cet objectif, EBRP promeut l'idée de définir un cadre formel pour étendre Event-B et RODIN avec des théories de domaine (ainsi que des mécanismes d'import/export) qui formalisent différents concepts de domaine. En plus, la consistance de cette extension devra être justifiée. Ce cadre d'ex-

tension défini devra permettre la définition/ l'instanciation/ l'import/ l'export/ l'extension de théories par l'introduction de type de données génériques associés à des opérateurs, des axiomes et des théorèmes. De plus, ce cadre ne doit pas être ad hoc à une théorie particulière, il doit être générique. Enfin, il doit offrir la possibilité de s'assurer de la correction de l'utilisation de ces théories, en particulier leur consistance lorsque plusieurs théories sont utilisées conjointement, ainsi que la correction des preuves réalisées.

EBRP est organisé autour de 4 tâches techniques traitant de la définition de théories de domaine, leur utilisation par des modèles formels, leur utilisation pour des preuves (automatiques) et la validation de l'approche sur des études de cas complexes et variées en thèmes (continu/discret).

Le consortium EBRP est composé d'experts de la méthode Event-B en France et en Europe. L'inventeur des méthodes B et Event-B, Jean-Raymond Abrial a accepté de se joindre à ce consortium" Coordinateur : Yamine Ait Ameur (Institut de Recherche en Informatique de Toulouse)

14/01/2020 – 48 mois

12 Projet CASES/Clearsy, calculateur Souverain sûr et sécurisé

"Le projet CASES vise à construire un calculateur générique sûr et sécuritaire souverain, permettant de contrôler et commander des infrastructures critiques au plus haut niveau d'intégrité. Il combine l'état de l'art en matière de calculateur et de logiciel, en ayant recourt de manière raisonnée aux méthodes formelles."

2022, durée du projet 24 mois dans le cadre de la Stratégie nationale cyber