RAPPORT D'ACTIVITE et PROJET SCIENTIFIQUE

Equipe VASCO

Responsable : Yves Ledru, Professeur, Université Joseph Fourier

1 Personnel

- Chercheurs : D. Bert, J.-L. Richier
- Enseignants-Chercheurs : P. Berlioux, S. Boulmé, L. du Bousquet, R. Groz, P. Jacquet, Y. Ledru, C. Oriat, F. Ouabdesselam, I. Parissis, M.-L. Potet
- Ingénieurs : M. Delaunay, J.-C. Reynaud
- Nombre de doctorants : 10.
- Nombre d'équivalents chercheurs (NE) : 14,6.

Voir le tableau en annexe 1 pour les informations détaillées.

Table des matières

1 Personnel **1**

2 Bilan des activités de recherche 02-05 **3**
2.1 *Thématique scientifique et objectifs généraux* 3
2.1.1 Thème 1 : Construction prouvée de programmes et de systèmes : des spécifications au code 4
2.1.2 Thème 2 : Validation des logiciels par des techniques de test . 14
2.1.3 Thème 3 : Construction de modèles pour l'expression et la vérification de propriétés de sécurité 24
2.1.4 Autres activités de recherche 28
2.2 *Résultats majeurs* 30

3 Activités d'encadrement **32**
3.1 *Thèses et HDR soutenues depuis le 01/10/01* 32
3.2 *Thèses et HDR en cours* 32

4 Collaboration et valorisation **33**
4.1 *Principales relations scientifiques hors contrats* 33
4.2 *Contrats institutionnels* 34
4.3 *Contrats (co)financés par un industriel* 34
4.4 *Création d'entreprise* 34
4.5 *Brevets et licences* 34

5 Publications(01-05) **35**

6 Principales responsabilités scientifiques et administratives **48**
6.1 Responsabilités scientifiques 48
6.2 Responsabilités administratives 49

7 Perspectives de recherche 06-10 **51**
7.1 Sécurité, construction prouvée 51
7.2 Test 52
7.3 Domaines d'application 53

2 Bilan des activités de recherche 02-05

2.1 *Thématique scientifique et objectifs généraux*

L'équipe VASCO fait partie de l'axe "Logiciels" du laboratoire LSR. Ses thèmes de recherches portent sur la validation des logiciels à l'aide de modèles.

Cette validation peut intervenir à divers stades du développement, allant de la validation de code existant jusqu'à la production rigoureuse de logiciels à partir de spécifications validées. Plusieurs approches sont étudiées. Elles reposent toutes sur des modèles formels ou semi-formels fournissant des descriptions abstraites du logiciel proprement dit (fonctionnalités, sémantique) ou de certaines caractéristiques non fonctionnelles de son comportement. Le choix d'utiliser des modèles qui ont un certain niveau de formalité, est justifié par la perspective d'automatiser certaines activités de développement ou de validation.

Nos travaux portent sur les thèmes suivants:

- la production de logiciels validés par construction : en suivant une démarche rigoureuse par raffinements à partir de modèles formels (méthode B);
- la production de logiciels validés à posteriori : en engendrant des tests à partir des modèles (Lutess) ou en utilisant les modèles comme oracle des tests (Tobias, Jartege);
- l'aide à la construction des modèles : génération, animation, vérification et évaluation des modèles;
- la construction de modèles pour l'expression et la vérification de propriétés non fonctionnelles des logiciels (sécurité);
- la sémantique des modèles.

Ce rapport présente les activités de l'équipe pendant la période 2001-2005 en les organisant autour de trois thèmes :

- Construction prouvée de programmes et de systèmes : des spécifications au code
- Validation des logiciels par des techniques de test
- Construction de modèles pour l'expression et la vérification de propriétés non fonctionnelles des logiciels (sécurité)

2.1.1 Thème 1 : Construction prouvée de programmes et de systèmes : des spécifications au code

Membres permanents de l'équipe impliqués dans cette activité :

- Didier Bert (CR CNRS)
- Sylvain Boulmé (MCF INPG)
- Yves Ledru (PR UJF)
- Marie-Laure Potet (PR INPG)

Membres non permanents (doctorants, post-doctorants, ingénieurs) :

- Akram Idani (Doctorant MENRT)
- Thomas Deruyter (Doctorant CIFRE Motorola/Freescale)
- Héctor Ruíz Barradas (Doctorant Univ. Autónoma Metropolitana Azcapotzalco, Mexique)
- Nicolas Stouls (Doctorant BDI CNRS)

2.1.1.1 Présentation du thème Dans certains domaines d'application pour lesquels il existe de fortes exigences en terme de surêté de fonctionnement du logiciel, l'utilisation des techniques formelles dans l'industrie est maintenant effective comme décrit dans les rapports commandés par le NIST[1] et par l'agence fédérale allemande pour la sécurité de l'information[2]. Ces utilisations sont motivées par des besoins en vérification mais aussi pour des raisons d'efficacité et de rationalisation du processus de développement. En effet les méthodes formelles permettent d'assurer la traçabilité des exigences jusqu'au code et surtout d'utiliser des outils engendrant du code à partir de descriptions de haut niveau. Notons que les besoins ne portent généralement pas sur l'application en son entier, ni sur tous les aspects d'une application. C'est par exemple le cas de la sûreté de fonctionnement qui ne porte que sur le sous-ensemble bien isolé des fonctions critiques.

Les méthodes formelles que nous expérimentons sont essentiellement orientées "modèles" et basées sur la logique du premier ordre avec théorie des ensembles : Z et B. Nous utilisons aussi les méthodes basées sur les logiques constructives, comme Coq. Elles offrent l'avantage de pouvoir donner lieu à des études qui conduisent à des outils. Cependant, devant la difficulté d'utiliser les notations formelles comme support d'échange entre communautés différentes (informaticiens, donneurs d'ordre,

[1] D. Craigen, S.L. Gerhart et T.J. Ralston : *An International Survey of Industrial Applications of Formal Methods*, U.S. National Institute of Standards and Technology, NISTGCR 93/626, 1993

[2] R.E. Bloomfield et D. Craigen, *Formal Methods Diffusion : Past Lessons and Future Prospects*, Adelard, numéro D/167/6101/1 v2.0, 1999

spécialistes-métier), nous étudions des représentations plus accessibles, essentiellement à base de diagrammes. Dans ce domaine, nous nous appuyons sur la notation UML qui est largement répandue et qui est standardisée. L'important est que les deux types de notations soient reliées automatiquement pour assurer la cohérence des représentations. Enfin, en partenariat avec des industriels, nous étudions les techniques avancées de génération de code à partir de spécifications.

Les principales directions explorées par l'équipe VASCO dans ces domaines sont les suivantes :

- Etude des fondements et des extensions de la spécification, de la modularité et du raffinement de systèmes (section 2.1.1.2)
- Aides à la construction des modèles (section 2.1.1.3)
- Outils pour la compilation reciblable de systèmes embarqués (section 2.1.1.4)

Dans le cadre de ce quadriennal, ces travaux sont, ou ont été développés, dans les projets suivants :

- Collaboration avec STMicroelectronics : Thèse de Nicolas Stouls, BDI cofinancée CNRS-STMicroelectronics (2003-2006).
- Projet précompétitif RNTL BOM (B Optimisant la Mémoire). Partenaires : Gemplus, ClearSy, LIFC et LSR (avril 2001 - mars 2003).
- Collaboration avec Freescale (anciennement Motorola-SemiConductors) depuis octobre 2001 (Thèse CIFRE de Thomas Deruyter).
- Projet GECCOO de l'ACI sécurité informatique (Génération de Code Certifié Orienté Objet). Partenaires : équipe VASCO du LSR, équipe Logical du LRI, équipe TFC du Laboratoire d'informatique de Franche-Comté, équipe Everest de Sophia et équipe CASSIS du Loria (septembre 2003 - septembre 2006).
- Projet EDEMOI de l'ACI sécurité informatique (Elaboration d'une DEmarche et d'outils pour la Modélisation In formatique, la validation et la restructuration de réglementation de "sûreté" et la détection des biais dans les aéroports). Partenaires : ONERA/DPRS, CNAM (CEDRIC), ENST Paris, LACL (Paris12), LSR, LIFC (septembre 2003 - septembre 2006).

Par ailleurs, les membres de l'équipe VASCO animent deux groupes de travail du GDR ALP dont les thématiques correspondent à ce thème :

- Didier Bert anime le groupe B, consacré à la méthode du même nom.
- Yves Ledru et Marie-Laure Potet animent le groupe AFADL (Approches Formelles dans l'Assistance au Développement de Logiciels).

2.1.1.2 Approches pour la spécification, la modularité et le raffinement de systèmes Une des problématiques générales de l'équipe VASCO est la spécification et la construction d'applications correctes par construction. Dans cadre nous menons depuis longtemps une activité sur la spécification et la mise en œuvre de processus formels de développement. Ces travaux ont débuté dans le cadre des spécifications algébriques, compétence initiale de l'équipe, puis nous nous sommes plutôt intéressés aux spécifications basées modèle. Nous menons actuellement en grande partie nos expérimentations avec la méthode B, qui offre un cadre suffisamment général pour pouvoir prendre en compte différents aspects d'un système et d'un développement. En effet la méthode B, initialement conçue et utilisée pour modéliser les données et les traitements, a été étendue pour prendre en compte les comportements d'un système[3]. Les directions principales que nous développons actuellement sont les suivantes :

- Développements modulaires (sous-section 2.1.1.2.1)
- Spécification et raffinement de propriétés dynamiques (sous-section 2.1.1.2.2)
- Raffinement et preuve de programmes "orientés objets" (sous-section 2.1.1.2.3)

2.1.1.2.1 Spécifications et développements modulaires Dans toute méthode, la maîtrise de la complexité nécessite de pouvoir allier à la fois le raffinement (ou son inverse l'abstraction) et la décomposition (ou son inverse la composition). Le raffinement permet de partir de modèles simples qui sont ensuite enrichis. De plus il assure une certaine traçabilité du développement. La décomposition, quant à elle, permet d'appréhender et de développer un modèle par parties. Dans le cadre des méthodes formelles ceci revient à modulariser le raisonnement, ce qui est un point délicat, en particulier lorsque les différents composants ne sont pas indépendants (partage de variables, interaction entre un système et son environnement, etc.).

La méthode B offre une notion de composant, basé sur un état interne, et qui permet d'associer des propriétés invariantes à un jeu d'opérations. Elle offre, de plus, un ensemble de primitives de structuration pour composer les spécifications ainsi que leur raffinement (le modèle B de Météor contient par exemple un millier de composants). Néanmoins certaines architectures ne sont pas valides : des propriétés sur les composants peuvent être invalidées par assemblage. Une partie de nos travaux antérieurs ont consisté à étudier les conditions permettant de composer les preuves[4] [5]. Ces conditions ont été incorporées dans l'Atelier B[6], l'outillage industriel de la méthode.

[3] J.R. Abrial, *Extending B Without Changing it*, First B conference, H. Habrias, Nantes, 1996.

[4] D. Bert, M-L. Potet et Y. Rouzaud, *A study on Components and Assembly Primitives in B*, Proc. of First B Conference, pp. 47-62, H. Habrias, Nantes, 1996

[5] M.-L. Potet et Y. Rouzaud, *Composition and Refinement in the B-method*, LNCS 1393, Springer-Verlag, Proc. of the 2nd Int. B Conference, D. Bert (ed.), 1998.

[6] *Le Langage B. Manuel de référence version 1.5*, ClearSy, Aix-en-Provence, France.

La théorie du raffinement ne prend pas en compte la modularité. Ce n'est que récemment que R. Back et M. Butler[7] ont proposé des opérateurs permettant de modéliser la composition et ont étudié les propriétés de ces opérateurs dans le calcul du raffinement. Néanmoins l'aspect mise en œuvre dans un langage est encore un problème ouvert. Nous développons donc un cadre théorique permettant de modéliser la composition des preuves [TH93]. En plus d'établir la correction des règles de composition de la méthode B, ce modèle doit permettre d'étudier l'impact de nouvelles extensions, en terme de preuves. L'article [ACL5] justifie les restrictions actuelles de la méthode B et présente leurs limitations.

Ces travaux se poursuivent dans le cadre de l'ACI sécurité GECCOO[8]. Cette action porte sur le développement d'applications objets dans l'objectif de vérifier des propriétés de sécurité pour des applications Java cartes. L'approche adoptée dans ce projet est l'approche JML[9] qui permet d'annoter les programmes Java (invariant de classe, pré et postcondition). Une approche similaire est développée par MicroSoft Research pour le langage C# (Spec#)[10]. Ces approches ont été initialement conçues pour des vérifications à l'exécution. Dans ce projet nous nous intéressons à la vérification statique des assertions par preuve. L'équipe VASCO est en charge de proposer des mécanismes compositionnels pour les preuves d'invariant et de raffinement. Une des difficultés inhérentes à l'objet est relative à la forte modularité liée aux classes et à l'héritage qui nécessite de faire de nombreuses preuves. Ce problème se pose d'ailleurs aussi lors des vérifications à l'exécution, les solutions actuelles étant sujettes à explosion combinatoire. En effet, la notion d'invariant attaché à une classe introduit un niveau de granularité (les méthodes de la classe) pour lequel ces invariants sont requis, avant appel. Lors de la construction d'applications architecturées il faut vérifier quels invariants sont demandés, et en quels points de l'application. De même l'héritage nécessite de faire des choix sur les propriétés qui doivent être préservées et sur la façon de prendre en compte la liaison dynamique. Nous utilisons l'expérience acquise pour la méthode B, et le cadre formel qui a été développé, pour proposer une approche à ces problèmes. Notre objectif, dans ce projet et à plus long terme, est de développer un calcul du raffinement qui permette de modéliser des aspects objets (liaison tardive et pattern) tout en gardant une maîtrise de l'activité de preuve (voir section 2.1.1.2.3).

2.1.1.2.2 Spécification et raffinement de propriétés dynamiques Traditionnellement, dans la spécification de systèmes, on distingue les propriétés de *sûreté* et les propriétés de *vivacité*. Les propriétés de sûreté sont exprimées par des

[7] R.J. Back et M. Butler, *Fusion and simultaneous execution in the refinement calculus*, Acta Informatica 35:921-949, Springer-Verlag, 1998.

[8] http://geccoo.lri.fr

[9] G. Leavens, A. Baker et C. Ruby, *JML: A notation for detailed design*, Behavioral Specifications of Businesses and Systems, Kluwer Academic Publishers, 1999.

[10] M. Barnett, R. Leino et W. Schulte, *The Spec# Programming System: An Overwiew*, in Proc. of Construction and analysis of Safe, Secure and Interoperable Smart Devices, CASSIS 2004, LNCS 3362, Springer-Verlag, 2004.

invariants qui décrivent les conditions en dehors desquelles le système ne peut pas fonctionner normalement. Les propriétés de vivacité, ou dynamiques, décrivent ce que l'on attend du système lorsqu'il fonctionne. Elle sont souvent de la forme : si le système se trouve dans un certain état P, alors il atteindra fatalement un état Q attendu.

Lorsque les systèmes sont décrits par des événements de manière non déterministe, les comportements possibles peuvent être très divers. Pour assurer les propriétés de vivacité, il faut alors, le plus souvent, soit ajouter des restrictions effectives dans les comportements du système, ce qui peut être difficile ou même impossible dans le cas où l'on modélise les comportements de l'environnement, soit imposer des hypothèses d'équité.

Nous avons étudié les conditions d'équité des systèmes dont les algorithmes abstraits peuvent être spécifiés de manière non déterministe. Une approche basée sur l'ordonnancement des événements a été présentée à la conférence AFADL en 2001, dans le cas du protocole de communication SCSI-3 qui contient un algorithme de gestion de l'équité [ACT42]. Avec Héctor Ruíz Barradas (doctorant encadré par D. Bert), nous travaillons sur l'intégration en B de la méthode de spécification de l'équité élaborée dans le langage Unity. Cela donne d'une part un niveau d'abstraction plus important pour décrire des propriétés de vivacité et d'autre part une plus grande souplesse pour la preuve, grâce aux règles d'inférence de la "théorie Unity" [ACT22, AP91]. Nous avons défini quelles sont les obligations de preuve qui assurent que les propriétés de vivacité "de base" sont vraies dans les systèmes et celles qui assurent qu'une propriété de vivacité est préservée dans les raffinements. De plus, nous avons montré que les obligations de preuve du raffinement sont un guide méthodologique pour conduire le raffinement de systèmes complexes [ACT56, ACL11].

Actuellement, nous avons élaboré un modèle mathématique de la relation d'atteignabilité dans les systèmes. Elle permet de prouver des propriétés dynamiques à l'aide de la notion de point fixe, plutôt que par un raisonnement opérationnel sur les traces d'événements. Nous avons montré des résultats intéressants qui indiquent, en particulier, comment raffiner des systèmes avec équité par des systèmes sans équité [ACT41].

Les perspectives de ce travail sont d'étendre le formalisme aux propriétés d'équité forte. Nous souhaitons aussi appliquer notre méthodologie à la spécification de propriétés dynamiques dans le projet EDEMOI, pour la vérification de la sécurité des aéroports. Enfin, nous pensons l'appliquer à la vérification par raffinement d'algorithmes distribués.

2.1.1.2.3 Calcul du raffinement en Coq et application à la preuve de programmes objets Le calcul du raffinement est une logique dérivée de la logique de Hoare, qui permet de construire incrémentalement une implémentation à partir d'une spécification abstraite, en vérifiant aussi de manière incrémentale la conservation des propriétés de la spécification abstraite. Comme la logique de Hoare,

le calcul du raffinement est fondé sur la logique du premier ordre et la théorie des ensembles. Elle s'intéresse à des programmes purement impératifs.

Nous travaillons sur une reformulation du calcul du raffinement dans le calcul des constructions inductives. Cette reformulation permet d'incorporer simplement au calcul des aspects qui lui manquent, mais sont bien compris en théorie des types: types inductifs, récursion structurelle et preuves par induction, pattern-matching et ordre supérieur. A terme, nous pensons pouvoir définir une logique qui combine harmonieusement ces aspects "purement fonctionnels" avec les aspects "non-purs" qu'on sait traiter en calcul du raffinement: effets de bord, traitement des exceptions, non-déterminisme.

D'un point de vue technique, la définition de ce calcul utilise les monades pour représenter les aspects non fonctionnels en Coq et le fait que le calcul de plus faible précondition (wp-calculus) est une sémantique par continuation: il peut être représenté en Coq comme une fonction d'ordre supérieur qui calcule des propositions.

Par ailleurs, la définition de ce calcul est "constructive": elle induit naturellement une implémentation en Coq (travail en cours). Cette implémentation doit fournir un prouveur interactif pour ce calcul. Ce prouveur écrit en Coq sera bien sûr complètement compatible avec Coq. De plus, les règles du calcul du raffinement seront en fait des théorèmes Coq (et donc prouvés formellement). Par rapport au prouveur de B (un prouveur pour le calcul du raffinement classique), le prouveur Coq aura l'avantage de donner un contrôle plus fin (interactif) sur la génération des obligations de preuve issues du wp-calculus. Ce contrôle semble en fait indispensable en présence d'ordre supérieur.

Pour finir, nous discutons de l'application de cette logique à la preuve de programmes OO. Dans les langages OO, les objets sont des valeurs du langage qui transportent des méthodes. Le code correspondant à ces méthodes n'est pas connu statiquement, mais seulement à l'exécution. Ce mécanisme est appelé "liaison dynamique". En logique de Hoare ou dans le calcul du raffinement classique, il est difficile de spécifier et prouver des propriétés sur des programmes paramétrés par d'autres programmes, car les programmes ne sont pas des valeurs de la logique. Par contre, le calcul du raffinement d'ordre supérieur permet de raisonner sur de tels programmes (dits d'ordre supérieur). Par exemple, l'opérateur "while" n'est pas une construction primitive dans cette logique. Mais il est dérivé en combinant récursion structurelle de Coq et non-déterminisme.

Sur ce travail de longue haleine, on peut voir le rapport de recherche, dont la version courante est en ligne à l'adresse ci-dessous[11].

2.1.1.3 Aide à la construction des modèles

[11] Sylvain Boulmé, *Specifying and reasoning in Coq with high-order impure programs using specifications a la Dijkstra and refinement.*
http://www-lsr.imag.fr/Les.Personnes/Sylvain.Boulme/horefinement.

2.1.1.3.1 Outils pour l'analyse du comportement des systèmes Un premier volet des travaux que nous menons dans l'équipe consiste à développer des outils permettant d'assister le processus de spécification et de raffinement. L'objectif visé est de pouvoir construire des spécifications en manipulant conjointement des systèmes de transitions symboliques pour modéliser explicitement les comportements. Lors des développements par raffinement et B événementiel, les outils doivent permettre de raisonner sur le raffinement des transitions de manière hiérarchique.

L'outil **GénéSyst**[12] développé dans l'équipe permet de visualiser le comportement de modèles B sous forme de systèmes de transitions symboliques[13] [14]. L'originalité de la construction proposée par GénéSyst est d'exhiber finement les conditions attachées aux transitions sous forme d'une condition de déclenchabilité et d'atteignabilité. Cette construction est basée sur le calcul de plus faible précondition et utilise la boîte à outils BoB, développée dans l'équipe, qui implémente différents calculs formels sur les spécifications. L'outil GénéSyst a déjà été utilisé dans différents contextes : ACI GECCOO [ACT31] et sur des exemples fournis par la société ClearSy. Il a été présenté à la session outil d'AFADL'04. Cet outil est en cours d'extension pour prendre en compte le raffinement et la modularité [ACT57] sous forme de systèmes de transitions hiérarchisés.

Le raffinement est un outil très puissant qui permet de décrire les systèmes suivant différents degrés de granularité. La prise en compte des aspects comportementaux rend ce processus complexe à mettre en œuvre. Nous cherchons à proposer une approche par schémas de raffinement, qui devrait permettre de faciliter le processus de raffinement par inférence de certaines propriétés invariantes. Cette approche a déjà été explorée dans le cadre de deux travaux de DEA[15] [16] et est étendue dans la thèse de Nicolas Stouls (dirigée par M.-L. Potet et S. Boulmé), en lien avec la vérification de propriétés de sécurité. Des démonstrations ont eu lieu à la conférence ZB2005.

2.1.1.3.2 Méthodes et outils pour l'analyse des réglementations Le projet EDEMOI de l'ACI Sécurité Informatique aborde la spécification formelle de la sûreté[17] dans la zone passagers d'un aéroport. Aujourd'hui, on constate que les réglementations, écrites en langue naturelle, comportent des imprécisions qui

[12] http://www-lsr.imag.fr/Les.Personnes/Nicolas.Stouls/

[13] D. Bert et F. Cave, *Construction of Finite Labelled Transition Systems from B Abstract Systems*, in Proc. of Integrated Formal Methods, IFM 2000, LNCS 1945, Springer-Verlag, 2000.

[14] N. Stouls, *Génération de systèmes de transitions étiquetées à partir de spécifications B événementiel*, rapport de DEA, Université Joseph Fourier, Grenoble, juin 2003.

[15] J. Lebray, *Modélisation de Systèmes en B : Proposition de guides méthodologiques pour la décomposition d'événements*, rapport de DEA, INPG, Grenoble, 2000.

[16] J. Nahoum, *Outils d'assistance à la construction de systèmes dans la méthode B*, rapport de DEA, INPG, Grenoble, 2001.

[17] Dans le transport aérien, la *sûreté* concerne la prévention contre les attaques terroristes et les interventions illicites. La *sécurité* concerne la prévention et l'évitement des accidents techniques, pannes, collisions, etc.

peuvent mener deux inspecteurs à des conclusions différentes sur la conformité d'un aéroport à ces réglementations. En outre, le caractère informel de ces documents ne facilite pas leur maintenance car il est difficile de mesurer l'impact de nouvelles mesures en interaction avec l'existant.

Le projet EDEMOI regroupe des membres de six équipes de recherche (CEDRIC/ CNAM, ENST Paris, LACL (Paris 12), LIFC (Besançon), LSR et ONERA/Centre de Toulouse). En outre, au cours du projet, nous avons établi des contacts avec les autorités de certification de l'ECAC (au niveau européen) et de l'ICAO (au niveau mondial). Le projet a pour objectif de modéliser des réglementations éditées par l'ECAC et l'ICAO, en UML puis en B ou en Z, afin de mieux les comprendre, de les structurer et de les valider [COM67]. Le projet se base sur des compétences de l'équipe VASCO autour de la méthode B et d'outils comme RoZ (voir plus loin) qui permettent de faire ce lien entre le diagramme de classes d'UML et une spécification formelle.

Un autre type d'outil est cependant souhaitable pour permettre le passage inverse d'une spécification formelle vers une représentation graphique. Tel est l'objectif de la thèse préparée par Akram Idani (dirigée par Y. Ledru et D. Bert). Partant d'une spécification B, Akram Idani propose de construire deux types de représentations: diagramme de classes et diagramme Etats/Transitions. De tels outils permettent la remontée d'informations vers des experts du domaine qui ne maîtrisent pas nécessairement les techniques formelles. Il contribue ainsi à la validation des spécifications formelles.

La construction d'un diagramme de classes à partir d'une spécification B s'appuie sur des techniques de formation de concepts, empruntées à l'ingénierie inverse. En [ACT28], nous avons montré que cette technique originale améliorait significativement l'état de l'art. Un outil a été réalisé pour automatiser l'approche et a fait l'objet d'une publication à ICFEM'05 [ACT34].

La construction d'un diagramme Etats/Transitions s'appuie sur des outils d'animation de spécifications B. Partant de traces d'exécution, des fonctions d'abstraction sont définies pour produire un automate dont les états sont caractérisés par des assertions. Ce travail fait suite au DEA d'Akram Idani, en coopération avec la société KeesDA (startup grenobloise spécialisée dans la conception de systèmes électroniques). Il a fait l'objet d'une publication acceptée dans la revue Information and Software Technology [ACL10]. Un outil de support a été développé par Ansem Ben Cheikh dans le cadre de son stage d'élève ingénieur de l'Ecole Polytechnique de Tunis qui permet de jouer des scénarios à partir des spécifications.

2.1.1.3.3 Intégration d'UML et Z dans RoZ De 1996 à 2000, nous avons travaillé avec Sophie Dupuy (thèse soutenue en 2000, dirigée par Y. Ledru et M. Chabre-Peccoud) à l'intégration d'annotations formelles dans des diagrammes semi-formels (OMT puis UML). Cette recherche s'est poursuivie dans le cadre de deux DEAs, et dans le cadre du projet EDEMOI. Cette intégration permet d'exploiter les outils associés aux techniques formelles pour établir des spécifications précises et

non-ambiguës, et montrer leur cohérence.

Pour le concepteur de systèmes d'information, elle permet des spécifications plus complètes et plus précises. En effet, les diagrammes semi-formels ne peuvent exprimer toutes les propriétés du système d'information; celles-ci sont donc souvent exprimées en français en marge de ces diagrammes. Nos propositions permettent d'exprimer de nombreuses contraintes dans un langage formel, donc précis et susceptible d'être exploité par des outils. En outre, elles fournissent un guide méthodologique pour l'identification et l'expression de ces contraintes.

Nous avons développé un environnement prototype : **RoZ**[18], qui s'interface avec des outils performants actuellement disponibles pour UML et Z. Cet environnement traduit une spécification UML annotée en Z, en une spécification Z. Il permet ensuite d'analyser finement cette spécification en utilisant un démonstrateur semi-automatique Z-EVES[19]. Des travaux menés en 2005 permettent d'animer les spécifications Z produites par RoZ avec l'outil Jaza[20].

Cette recherche a donné lieu à plusieurs publications [COM63, ACT44, ACT49, COM74, ACT30]. Elle a fait également l'objet d'une présentation invitée en mars 2003 à une journée QSL organisée à Nancy sur le thème de l'intégration d'UML et des méthodes formelles [COM65]. Nous avons réalisé des démonstrations de notre prototype à l'occasion des conférences FME2001, FME2002 et ZUM2002.

2.1.1.4 Outils pour la compilation reciblable de systèmes embarqués

Les technologies actuelles permettent d'intégrer sur une seule puce des systèmes embarqués de plus en plus complexes (freinage ABS, décodeurs TV, ...). Cette complexité n'a pu être atteinte qu'en ayant recours à des processeurs programmables, capables de répondre aux exigences de performance et de flexibilité. La programmation, initialement faite en assembleur, utilise maintenant des langages de plus haut niveau (principalement le langage C), afin de pouvoir maîtriser la taille et la complexité des applications. Ceci nécessite de développer de nouveaux outils permettant de maîtriser finement le code produit. De plus ces outils se doivent d'être reciblables : ils doivent pouvoir être paramétrés par les processeurs cibles, ayant des architectures différentes. Nos travaux portent principalement sur l'adaptabilité des processus de traduction/compilation, en fonction des caractéristiques des architectures visées.

Dans le cas de la méthode B, le problème de la traduction revient à la fois à définir un langage B0 (le langage de programmation associé à la méthode B) efficace et suffisamment expressif ainsi qu'un processus maîtrisable et adaptable de sa traduction vers un langage de programmation. Cette problématique a été traitée dans le projet RNTL BOM[21] (B Optimisant la Mémoire, 2001-2003). Notre équipe

[18] http://www-lsr.imag.fr/Les.Groupes/PFL/RoZ/index.html

[19] URL: http://www.ora.on.ca/z-eves/

[20] Mark Utting, Université de Waikato en Nouvelle Zélande,
URL: http://www.cs.waikato.ac.nz/~marku/jaza/

[21] http://lifc.univ-fcomte/~tatibouet/WEBBOM

était, en particulier, en charge de valider certains aspects de la chaîne de traduction (modularité et gestion des noms, optimisations des passages de paramètres et conditions d'expansion en ligne [ACL5], correction de la traduction ...). Ce projet a produit un outil permettant de traduire du B0 à partir de règles de traduction adaptées aux contraintes de l'architecture. Cet outil a été expérimenté dans le cadre du projet sur une application de taille conséquente (un sous-ensemble de la JCVM) [ACT47, ACT24]. Il est utilisé depuis lors par la société ClearSy. Nous continuons à développer nos travaux sur ce thème [ACL7] en étudiant comment valider les règles de traduction et en proposant une approche permettant d'exploiter les preuves issues d'un développement B pour produire du code annoté (Proof Carrying Code).

Dans le cadre du DEA[22] et de la thèse CIFRE de Thomas Deruyter (dirigée par M.-L. Potet et J.-C. Fernandez), nous nous intéressons au reciblage de la chaîne de compilation DSP de la société Freescale (anciennement Motorola-Semiconductors). L'objectif de ce travail de thèse est d'une part de développer un outil permettant de modéliser les architectures cible et les règles de traduction et d'autre part de proposer des procédures de vérification relatives au caractère irrégulier des DSP. En effet, dans ce type d'architecture, les instructions introduisent des contraintes fortes sur le placement des opérandes. Ceci rend le processus de compilation complexe et difficile à mettre au point. Les procédures de vérification que nous avons proposées ont pour objectif de calculer les contraintes de placement décrites dans les modèles d'architecture, de vérifier leur respect lors du processus de traduction et d'évaluer le jeu de règles de traduction (complétude et atteignabilité)[23]. Pour le respect des contraintes de placement par le compilateur, la solution qui a été retenue est de vérifier à l'exécution la correction du résultat produit par le sélecteur d'instructions. En effet, la preuve *a priori* de la correction du sélecteur n'est pas envisageable, en raison de sa complexité. La solution adoptée a nécessité de développer un modèle formel de l'exécution du compilateur, relativement à l'affectation de ressources aux variables du programme (placement en mémoire et en registres). Les outils sont en cours de développement et d'expérimentation sur une architecture Motorola (StarCore 140). Les travaux théoriques actuels portent sur la modélisation des contraintes de parallélisation et les problèmes de complétude et d'atteignabilité

[22] T. Deruyter, *Modèle générique de description de machine, pour la compilation DSP*, rapport de DEA, Université Joseph Fourier, Grenoble, 2002.

[23] T. Deruyter, J-C. Fernandez, M-L Potet et P. Brand, *Retargeatable DSP Compilers: a Formal Approach to Deal with Irregular Placement Constraints*, rapport, laboratoire LSR, janvier 2005.

2.1.2 Thème 2 : Validation des logiciels par des techniques de test

Membres permanents de l'équipe impliqués dans cette activité

- Michel Delaunay (IR CNRS)
- Lydie du Bousquet (MCF UJF)
- Roland Groz (PR INPG)
- Yves Ledru (PR UJF)
- Catherine Oriat (MCF INPG)
- Farid Ouabdesselam (PR UJF)
- Ioannis Parissis (MCF UJF)
- Jean-Luc Richier (CR CNRS)

Membres non permanents (doctorants, post-doctorants, ingénieurs)

- Pierre Bontron (Ingénieur sur contrats, ATER, Doctorant)
- Vianney Darmaillacq (Doctorant MENRT)
- Laurence Estrabaut (Ingénieur sur contrats)
- Karim Griche (Ingénieur sur contrats, ATER, Doctorant)
- Audrey Kermarec (Doctorante Bourse France Télécom R&D)
- Abdeslam Lakehal (Ingénieur sur contrats, ATER, Doctorant)
- Laya Madani (Doctorante bourse Syrie)
- Olivier Maury (Doctorant MENRT)
- Beznik Seljimi (ingénieur sur contrats, Doctorant)
- Jérôme Vassy (Ingénieur sur contrats, Doctorant)

Professeur invité

- Alexandre Petrenko (CRIM, Montréal, invité en avril-juin 2004)

2.1.2.1 Présentation du thème Ce thème s'intéresse à l'utilisation de techniques de test pour la validation des logiciels. Les travaux relatifs à ce thème peuvent être regroupés dans trois sous-thèmes :

- L'utilisation de spécifications comme point de départ du processus de génération des tests. Les spécifications sont vues ici comme des modèles comportementaux associés soit au logiciel lui-même (spécification fonctionnelle, spécification de propriétés non fonctionnelles) soit à son environnement (utilisateur, environnement physique). Ces activités concernent principalement l'outil Lutess, qui exploite des modèles synchrones, pour la génération de cas de tests.

Les travaux portent sur l'évolution de l'outil, et sur son application à divers domaines (recherche d'interactions, aéronautique, interfaces homme-machine). D'autres activités concernent l'utilisation d'automates étendus.

- L'utilisation de spécifications comme oracle pour des tests générés indépendamment de celles-ci. Il s'agit principalement de spécifications en JML (Java Modelling Language) pour des programmes Java. La génération de données de test s'appuie sur une modélisation de l'utilisateur implantée par des stratégies de test (aléatoire, combinatoire, guidé par des propriétés...). Deux outils (TOBIAS et Jartege) ont été réalisés dans le cadre de ces études. TOBIAS fait l'objet d'un référencement auprès de l'Agence de Protection des Programmes.

- L'utilisation de techniques centrées sur le code, pour générer des tests, évaluer sa qualité ou sa testabilité. Une nouvelle activité a été initiée pendant le dernier quadriennal sur l'évaluation de la testabilité logicielle. Elle trouve notamment des applications dans une collaboration en cours avec le laboratoire LPSC autour d'un système embarqué pour une mission spatiale. D'autres recherches ont porté sur la synthèse de bouchons pour des programmes impératifs, ou sur la mesure de couverture structurelle des tests d'un grand logiciel.

L'essentiel de ces travaux sont menés dans le cadre de collaborations avec des industriels (contrats ou projets RNRT/RNTL).

- Projet RNTL COTE (2000-2002), avec Softeam, France Télécom R&D, Gemplus et l'IRISA

- Projet RNTL INKA (2000-2002), avec Thalès Systèmes Aéroportés, Axlog, l'Université Nice, et l'Université Franche-Comté

- Projet RNRT VALISERV (2001-2003), avec France Télécom R&D, l'Université d'Evry et TNI

- Projet RNTL DANOCOPS (2004-2007), avec Thales Systèmes Aéroportés, Axlog, l'Université Nice, et l'Université Franche-Comté

- Projet RNRT Verbatim (2004-2006), avec France Télécom R&D, AQL, Clearsy, ONERA-Centre de Toulouse et l'Université de Poitiers

- Collaborations industrielles directes : AIRBUS Industries

L'équipe est également présente dans plusieurs réseaux scientifiques sur le test :

- Réseau Européen TAROT (Training And Research On Testing) dans le cadre du Marie Curie Research Training Network (MCRTN).

- Action Spécifique CNRS 111 Techniques de spécification et de test pour les composants logiciels de communication, avec l'INT Evry, l'Université d'Evry, l'Université Paris-Sud, l'Université de Bordeaux, France Télécom R&D et le CEA.
- Action Spécifique CNRS 161 Testabilité des systèmes informatiques avec l'ESISAR/INPG, l'ONERA-Centre de Toulouse, et l'IRISA.

Sous-thème 2.1 : Génération de tests à partir de spécifications

2.1.2.2 Test de logiciels synchrones et applications Les travaux de l'équipe sur le test de logiciels réactifs synchrones ont débuté en 1993. Ils ont abouti à l'outil Lutess (1996) qui intègre de nombreuses techniques bien fondées théoriquement, et mené à de francs succès internationaux (1998).

2.1.2.2.1 Test fonctionnel Deux activités ont été menées sur l'approfondissement et l'évaluation des techniques de test proposés par Lutess.

Nous avons étudié comment mieux exploiter les spécifications formelles de ces logiciels pour rendre plus efficaces (en termes de détection de défauts) et plus automatiques les activités de test. Plus précisément, nous avons mis en oeuvre de nouvelles techniques de génération de données de test guidées par les propriétés de sûreté du logiciel (thèse de Jérôme Vassy, encadrement : Ioannis Parissis et Farid Ouabdesselam, soutenue en octobre 2004). Les propriétés de sûretés sont des formules de logique temporelle, exprimées sur plusieurs instants. l'objectif est de favoriser l'apparition d'erreurs en forçant l'évolution du logiciel vers des situations violant les propriétés. Ceci repose sur la caractérisation d'"états suspects" de l'environnement, et la capacité, pendant l'exécution, à repérer ces états de façon anticipée.

Une validation de l'approche a été réalisée sur un ensemble important de spécifications de services téléphoniques. Ces travaux se sont inscrits en partie dans l'ATIP "Jeune Chercheur" PROSPECT. Dans le cadre de son contrat post-doctoral, Jérôme Vassy réalise au CEA (direction Bruno Marre) la comparaison des outils de test Lutess (LSR) et Gatel (CEA) sur la base de la même étude de cas.

Par ailleurs nous étudions le couplage des techniques de test offertes par Lutess pour traiter des données booléennes (techniques fondées sur la manipulation de BDD) avec la programmation logique avec contraintes pour prendre en compte des données numériques. Ceci fait l'objet de la participation du LSR au projet RNTL DANOCOPS. Ces travaux n'ont démarré que depuis peu (octobre 2004). Nous avons défini une version de Lutess intégrant la résolution de contraintes numériques (thèse de Besnik Seljimi, encadrement : Laurent Trilling et Ioannis Parissis).

2.1.2.2.2 Couverture fonctionnelle L'étude des critères de couverture structurelle pour des programmes Lustre-SCADE trouve son origine dans une recherche

conjointe avec Airbus Industrie. Une préoccupation majeure des utilisateurs de SCADE (version industrielle du langage synchrone Lustre) est de pouvoir définir une notion de couverture fonctionnelle de leurs programmes. Nos premiers résultats [ACT36, ACT37, ACT54] portent sur la définition formelle de nouveaux critères de couverture pour les chemins à travers des réseaux d'opérateurs (graphe de flot de données) et le mode de construction automatique des conditions d'activation de ces chemins. Les critères traduisent la sensibilité des points à atteindre dans un chemin vis à vis de la variation des valeurs en entrée. Les conditions d'activations sont calculables à différents niveaux de profonteur, de façon incrémentale.

Un outil pour la mise en œuvre de mesures de couverture a été développé et validé sur des études de cas industrielles. Ce travail fait l'objet de la thèse d'Abdesselam Lakehal (encadrement Ioannis Parissis et Farid Ouabdesselam).

Cette collaboration a été étendue à d'autres partenaires et vient de faire l'objet d'un projet de STREP (6ème PCRD, appel septembre 2005, pilote Airbus).

2.1.2.2.3 Test d'applications interactives multimodales Le projet RNTL VERBATIM met en évidence de nouveaux besoins pour la validation d'applications interactives multimodales. Habituellement, ces applications sont testées manuellement à l'aide de scénarios décrits informellement. Quelques approches formelles ont été proposées dans le passé portant sur la spécification formelle et la preuve. Nos travaux, et en particulier la thèse de Laya Madani (encadrement : Ioannis Parissis et Farid Ouabdesselam), cherchent à définir une méthode de test automatique s'inspirant de l'approche synchrone mais qui répond pleinement aux attentes des concepteurs. Dans le cadre de ce projet, nous travaillons en étroite collaboration avec le laboratoire CLIPS-IMAG (équipe IIHM) et des équipes de France Telecom R&D. Les premiers résultats [ACT38, ACT61] montrent la possibilité d'exprimer un grand nombre de comportements intéressants des utilisateurs à l'aide des moyens proposés par Lutess (probabilités, scénarios, oracles). Parmi les pistes actuellement explorées figurent la meilleure prise en compte des propriétés liées à la multimodalité dans la génération des tests.

2.1.2.3 Recherche d'interactions Le projet RNRT exploratoire VALISERV a constitué le cadre du travail sur l'intégration de services de télécommunication et la maîtrise de leurs interactions [ACT23].

Dans l'esprit, les architectures de services sont conçues de façon à permettre une extension modulaire, rapide et peu coûteuse de l'ensemble des fonctionnalités du système. Malheureusement, dans la pratique, ce but n'est que rarement atteint car les services ne fonctionnent pas de façon indépendante. Les interactions entre ces services induisent des biais de comportement préjudiciables quand elles sont inattendues et néfastes. Les interactions néfastes correspondent à des effets de bord non prévus d'un service sur l'autre qui déstabilisent l'utilisateur dans le meilleur des cas mais qui peuvent également aboutir à de profonds dysfonctionnements.

Le problème est difficile car il faut prendre en compte toutes les combinaisons potentielles des services au sein de l'architecture. Il est également délicat du fait de la nature quasi subjective de l'existence d'une interaction : ceci découle de la difficulté à cerner les intentions des utilisateurs, rendant très difficile la définition de la "bonne" intégration des services.

Dans ce projet nous avons essentiellement travaillé sur un processus incrémental d'intégration de services et de détection d'interactions néfastes au niveau des spécifications. Ce processus est géré en étroite interaction avec l'expert humain qui conduit l'intégration.

Une particularité notable de VALISERV a été de coupler deux techniques très différentes dans le même processus incrémental, composé de deux phases : en phase «amont» l'intégration est opérée par manipulations et analyses symboliques ; en phase «aval», la validation repose sur le test, en utilisant Lutess.

Une spécification de service se présente sous la forme d'un couple $< Sys, Prop >$. Sys est un ensemble de formules de type précondition/postcondition décrivant le sytème par son comportement et fournissant un modèle exécutable de type réactif synchrone. $Prop$ est un ensemble de formules décrivant les propriétés attendues du système, pour l'essentiel des invariants.

Les attentes des utilisateurs fournies à l'issue de la phase "d'intégration" servent de point de départ à deux activités de la phase de "validation" par le test :

- La construction des oracles exprimant l'absence de comportement non souhaités du système ; les oracles sont engendrés automatiquement par l'outil Lutess à partir de $Prop$.

- La construction des guides de test qui vont servir à focaliser l'effort de test sur des zones d'intérêt.

Pour cela, par l'étude de benchmarks, nous avons déterminé un certain nombre de critères d'interaction potentielle. De tels critères correspondent à la généralisation d'une ou de plusieurs causes d'interactions et sont assimilés à des "fautes métier".

Il faut pouvoir exprimer ces causes d'une manière plus opérationnelle dans le but de les fournir en entrée à un algorithme de production de guides de test.

Nous avons défini un langage de patterns d'actions permettant de décrire de manière formelle des situations qui apparaissent pendant l'exécution des services et qui pourraient induire ou correspondre à une interaction. Les éléments du langage ont été conçus comme une vue abstraite de l'implémentation des services de toute nature (téléphonique, de messagerie...). On retrouve les concepts de ressource avec attribut et de contrôleur avec privilège d'accès.

La génération de guides de test associés à un pattern d'actions nécessite d'avoir annoté la description comportementale du système à tester (Sys) avec les actions du langage de patterns. La génération correspond à un parcours de la spécification annotée en cherchant à retrouver un pattern. Les guides de test sont utilisés par Lutess pour engendrer des données représentant les utilisateurs des services.

2.1.2.4 Test d'automates étendus Les automates étendus avec des variables (EFSM) sont un modèle privilégié pour la spécification et la représentation de systèmes interagissant de façon asynchrone ou synchrone avec leur environnement. Nous nous intéressons à la génération de tests de conformité pour ces modèles. Nous nous appuyons sur le riche corpus de méthodes et d'outils existant pour la génération de test pour des automates. Comme ces tests s'appuient sur la structure de contrôle que constitue l'automate, nous cherchons à étendre une suite de test donnée pour identifier des fautes résiduelles dans les mises à jour de variables internes qui n'auraient pas été révélées par les tests déjà passés. Nous proposons des modèles de fautes combinés à des techniques d'abstraction pour avoir une représentation compacte des fautes résiduelles, permettant un calcul de séquences discriminantes. Ces travaux [ACL9, ACT59] sont menés en collaboration avec France Télécom (travail doctoral d'Audrey Kermarrec, dirigée par Roland Groz) et avec le CRIM (Alexandre Petrenko).

Sous-thème 2.2 : Utilisation de spécifications comme oracle

2.1.2.5 Test combinatoire Des expérimentations industrielles menées dans le cadre du projet RNTL COTE (2000/2002) nous ont convaincu de l'intérêt de développer l'outil TOBIAS de génération combinatoire de séquences d'appels. L'expérience des industriels associés au projet a montré qu'il est nécessaire de produire de nombreux cas de test (ou objectifs de test) pour tester un système de façon satisfaisante. De nombreuses similarités existent entre ces cas de test, de sorte que leur définition devient une tâche répétitive. TOBIAS est un outil de test combinatoire qui a pour objectif de générer systématiquement des cas de test sur base de similarités identifiées par l'utilisateur.

Cet outil, initialement destiné à générer des objectifs de test pour l'outil TGV de l'IRISA, a ensuite été utilisé avec succès pour générer des cas de test dont l'oracle est fourni par une spécification exécutable (en VDM [COM64] ou en JML[ACT29, ACT27]).

Plusieurs études de cas ont été menées avec TOBIAS, en collaboration avec des partenaires extérieurs à l'équipe (Gemplus [ACT27] et l'équipe IIHM du CLIPS/IMAG [ACT33]). Ces études ont montré la facilité de prise en main de l'outil, sa capacité à détecter des erreurs, son apport à la productivité de l'ingénieur de test, ainsi que la capacité de TOBIAS à structurer une suite de tests. Un autre point fort de TOBIAS résulte du choix de travailler avec des tests abstraits, indépendamment d'une technologie. Ceci a permis de l'adapter à plusieurs langages cibles (Java/JML, VDM, IOLTS pour TGV). D'autres adaptations (C++, test de spécifications en B ou en Z) sont en préparation.

L'outil a fait l'objet d'un référencement auprès de l'Agence de Protection des Programmes en 2005. Plusieurs projets (RNTL, ARA, pôle de compétitivité Minalogic) ont été soumis pour financer son développement futur.

Deux thèses ont été menées dans le cadre de cette recherche.

- La thèse de Pierre Bontron (soutenue en mars 2005, encadrée par Lydie du Bousquet, Yves Ledru et Marie-Laure Potet) a porté sur la définition d'une mesure de couverture de spécifications au niveau d'abstraction offert par l'outil. Cette thèse s'inscrit dans la perspective de l'utilisation de TOBIAS avec TGV. Dans ce contexte, TOBIAS offre une abstraction supplémentaire par rapport au niveau de TGV en agrégeant plusieurs objectifs de test dans une même description. La thèse a établi le lien entre la mesure de couverture qui peut être faite au niveau de description de TOBIAS et la couverture effective des tests produits par TGV [ACL8].

- La thèse d'Olivier Maury (soutenance en novembre 2005, encadrée par Catherine Oriat et Yves Ledru) a abordé le problème de la maîtrise de l'explosion combinatoire des cas de tests produits par TOBIAS. Dans le contexte de JML et de VDM, il a proposé des techniques permettant de filtrer les cas de test produits à la génération ou lors de leur exécution [ACT29]. Cette thèse a également exploré le couplage de TOBIAS avec l'outil UCASTING de l'IRISA [ACT50].

La maîtrise de l'explosion combinatoire est un problème scientifique difficile mais pour lequel de nombreuses solutions pratiques existent. Outre les travaux d'Olivier Maury, plusieurs travaux d'étudiants de Master 1 et 2 ont été menés pour étudier l'adaptation à TOBIAS de solutions proposées par d'autres équipes (génération combinatoire par paires, techniques de réduction de suites de test, ...). Une nouvelle version de TOBIAS sera développée en 2006 pour prendre en compte ces divers résultats.

2.1.2.6 Test aléatoire de programmes Java Pour effectuer des tests unitaires de classes Java, il est nécessaire d'écrire des programmes de test qui appellent les opérations des classes que l'on souhaite tester, appelées "classes sous test". L'écriture de programmes de test est une activité qui prend beaucoup de temps, et qui n'est pas très intéressante. La génération automatique de programmes de test a pour but de produire facilement un grand nombre de tests, afin de réduire l'effort nécessaire au développement d'une campagne de test. L'outil Jartege (Java Random Test Generator) [ACT39], développé par Catherine Oriat, permet de générer automatiquement des tests aléatoires pour des classes Java spécifiées en JML. L'outil permet de guider la génération aléatoire par des profils opérationnels qui favorisent l'appel de certaines méthodes, contrôlent la création ou la réutilisation d'objets et contraignent dynamiquement les valeurs des paramètres des méthodes. Cette approche consiste à produire des programmes de test composés de suites aléatoires d'appels d'opérations des classes sous test. Chaque programme de test peut ensuite être exécuté pour tester le programme, puis ré-exécuté ultérieurement soit après la correction d'une erreur, soit pour effectuer des tests de non régression. L'outil est conçu pour produire des tests unitaires, c'est-à-dire des tests qui comportent des appels à certaines méthodes appartenant à un petit nombre de classes. Dans la

mesure où l'on peut d'une part effectuer un grand nombre d'appels de méthodes, et d'autre part tester ensemble plusieurs classes, le type de test effectué avec Jartege se situe à la limite du test d'intégration. Ses capacités de détection d'erreurs ont été évaluées sur une étude de cas fournie par Gemplus, et comparées à celles de TOBIAS [ACT27]. Le test aléatoire est considéré ici comme un moyen complémentaire de production de programmes de test ; il ne vise pas à remplacer la production manuelle de jeux de tests, mais à mettre en évidence un certain nombre d'erreurs avec un effort minimal. Le test aléatoire peut en particulier aider à détecter des conditions implicites pour certaines méthodes et produire des suites d'appels non triviales, qui pourraient être oubliées lors de la production manuelle de tests. Une autre étude de cas a été menée lors du travail de Master Recherche de N. Berkani[24] .

Sous-thème 2.3 : Techniques centrées sur le code

2.1.2.7 Testabilité Selon Binder[25], la testabilité mesure la facilité (ou le coût) de révéler des fautes logicielles. À conception et développement égaux, un système plus testable sera moins coûteux.

2.1.2.7.1 Testabilité et conception à base d'objets ou de composants L'équipe avait mené des travaux en partenariat avec l'IRISA et l'équipe ValSys (laboratoire LCIS, Valence) dans le domaine de la testabilité et la diagnosabilité des systèmes synchrones [ACL6]. Depuis 2001, VASCO a repris sa collaboration avec l'équipe ValSys, cette fois-ci sur le thème de la testabilité des systèmes logiciels conçus avec une démarche objet ou à partir de composants.

De façon plus précise, notre collaboration vise à établir des indicateurs/métriques évaluables dès les premières phases de conception, permettant de prédire la testabilité de la réalisation à venir. Un premier travail dans ce sens a été réalisé en 2003 (travail de DEA de Boris Baldassari). Des mesures classiques d'évaluation de la testabilité de programmes objets ont été étudiées. Parmi ces mesures, ont été retenues les 6 mesures proposées par Chidamber et Kemerer, et les 4 mesures proposées par R. Martin. Ces mesures s'évaluent respectivement sur le diagramme de classe et les packages. Nous avons identifié 7 d'entre-elles pouvant être appliquées dès les phases de conception. Nous avons réalisé un outil permettant d'évaluer ces métriques à partir de diagrammes UML. Cet outil est utilisé en interne par Thalès Avionic Valence [ACT51].

La collaboration entre ValSys et VASCO a donné lieu à un projet IMAG (CONTEST, 2004-2006), et à l'organisation d'une Action Spécifique CNRS, l'AS Testabilité. Cette AS a regroupé le LSR, le CERT-ONERA, Le LCIS et l'IRISA. Au cours

[24] N. Berkani. *Création de structures d'objets pour le test de programmes Java.*, Rapport de Master 2 Recherche, Université Joseph Fourier, 2005.

[25] R. Binder : *Design for testability in object-oriented systems.* Communications of the ACM 37:9, 87-101, Sep 1994.

de cette AS, un workshop sur la testabilité a été organisé en marge de la conférence ISSRE 2004.

Depuis mars 2005, Chantal Robach (ValSys) et Lydie du Bousquet (VASCO) co-encadrent Samer Housseno en thèse. Ce travail vise à analyser le recueil des besoins (exprimés à l'aide de cas d'utilisation) pour y repérer des constructions a priori non facilement testables. Là encore, il s'agit d'établir des métriques ou des indicateurs permettant de détecter de futurs problèmes de testabilité.

2.1.2.7.2 Testabilité et système embarqué Parallèlement à ces travaux, une collaboration avec le Laboratoire de Physique Subatomique et de Cosmologie (LPSC) a été engagée. Ce laboratoire doit produire un logiciel critique qui sera embarqué sur satellite. Sa fonction consiste à contrôler les équipements cryogéniques pour assurer une température nécessitée par le type de mesures physiques que le satellite doit mener. Le logiciel a été programmé en C et en assembleur DSP.

Une première partie de la collaboration a consisté à suivre la phase de validation mise en œuvre pour ce logiciel. Une seconde partie du travail (en cours) consiste à analyser le code source produit et à évaluer plusieurs mesures de complexité et de testabilité proposées dans la littérature, et de les comparer à l'effort réel de test.

Nous envisageons de travailler ultérieurement sur cet exemple à partir de modèles synchrones, pour évaluer nos approches de test statistique et guider la validation d'un tel logiciel ou de ses évolutions.

2.1.2.8 Test structurel de programmes impératifs Dans le cadre du projet RNTL INKA (2000-2002), nous avons traité la génération automatique de jeux des tests satisfaisant des critères de couverture structurelle pour des programmes C en présence d'appels de fonctions. Ce travail a abordé le problème posé par la création de "bouchons" (substituts aux fonctions appelées). Il s'agit d'un problème difficile tant sur le plan pratique que théorique, sur lequel ont porté très peu de travaux.

Nous sommes partis du constat que les bouchons classiques sont trop simplistes pour permettre de générer des données représentatives des comportement possibles des fonctions qu'ils remplacent. En conséquence, le taux de couverture obtenu à l'issue du test unitaire n'est pas représentatif de l'utilisation de la fonction testée au sein du logiciel. Par ailleurs, lors du test d'intégration, le test structurel n'est pas envisageable : il faudrait analyser tout le corps des fonctions appelées originales.

Notre solution a consisté à modéliser les fonctions appelées de façon *réaliste pour les besoins du test structurel*. Les bouchons sont construits à partir des modèles. Ces modèles sont réalistes car le processus de génération de données de test pour une entité en appelant une autre modélisée fournit la même donnée que pour cette entité appelant la fonction originale. Ce modèle est généré *automatiquement* à partir d'une analyse statique du corps de la fonction appelée, par des techniques de "slicing".

Un bouchon est composé d'une hiérarchie d'approximations de plus en plus complexes. Chaque approximation représente un ensemble de comportements de l'entité

originale. Les approximations sont considérées les unes après les autres jusqu'à en trouver une permettant la génération d'une donnée de test.

L'implantation exploite la programmation logique avec contraintes (thèse de Karim-Cyril Griche, encadrement : Ioannis Parissis et Farid Ouabdesselam, soutenue en juillet 2005).

2.1.2.9 Mesure de couverture de grands logiciels Une collaboration avec la société Bull s'est déroulée en 2004. Elle s'est concrétisée par un travail de DRT soutenu par Mehdi Kessis en décembre 2004 et co-encadré par Yves Ledru et Jean-Marc Vincent, du laboratoire ID/IMAG. Ce travail a étudié le test de l'intergiciel JONAS développé dans le cadre du consortium ObjectWeb. Nous avons plus particulièrement dirigé la partie de ce travail dont l'objet était la mesure de couverture de suites de test industrielles. Ce travail a notamment montré la faible couverture de telles suites de tests pour des logiciels complexes comme JONAS dont le code doit s'adapter à diverses configurations logicielles, et comporte de nombreuses sections destinées à la couverture d'erreurs exceptionnelles ou à faciliter le débogage [ACT35, ACT60].

2.1.3 Thème 3 : Construction de modèles pour l'expression et la vérification de propriétés de sécurité

Membres permanents de l'équipe impliqués dans cette activité

- Didier Bert (CR CNRS)
- Sylvain Boulmé (MCF INPG)
- Roland Groz (PR INPG)
- Marie-Laure Potet (PR INPG)
- Jean-Luc Richier (CR CNRS)

Membres non permanents (doctorants, post-doctorants, ingénieurs)

- Vianney Darmaillacq (Doctorant MENRT)
- Nicolas Stouls (Doctorant BDI CNRS)

2.1.3.1 Présentation du thème Avec la généralisation des traitements informatiques au cœur de la plupart des systèmes et des activités humaines, la sécurité et la sûreté des systèmes informatiques sont devenus des enjeux de sociétés majeurs. Les deux autres thèmes abordés par l'équipe VASCO concernent la sûreté des systèmes. Le troisième thème est consacré à des aspects de la sécurité, dans le sens de la protection des systèmes informatiques contre des actions malveillantes.

Au sein des problématiques de la sécurité informatique, nous nous intéressons à l'application de techniques issues du génie logiciel à base formelle pour la spécification, la validation et la construction de systèmes assurant la sécurité. Plus précisément, nous basons notre approche sur des modèles de politiques de sécurité, qui permettent de représenter les exigences ou les règles de sécurité appliquées au sein de systèmes ou d'organisations. Bien entendu, les démarches recouvrent celles des autres thèmes de l'équipe; on peut d'ailleurs noter que la modélisation de la sécurité des aéroports relève de la même problématique, mais s'arrête pour l'instant à la construction du modèles, alors que nous étudions dans ce thème l'exploitation des modèles de la sécurité.

Les travaux de l'équipe sur ce thème ont débuté au cours de l'année 2003, faisant suite à la collaboration de Marie-Laure Potet avec l'équipe DCS de Vérimag. Des collaborations avec d'autres partenaires académiques et industriels sont venus enrichir l'activité, débouchant sur le montage de plusieurs projets: le projet MODESTE de l'IMAG (2004-2006), qui fédère l'ensemble de nos activités sur ce thème, et des collaborations avec ST Microelectronics et l'IRISA, ainsi que d'autres en cours de soumission.

Deux principaux aspects ont été abordés au cours de la période:

- modélisation et raffinement, principalement étudiés dans le cadre de politiques de sécurité appliquées aux systèmes embarqués à haut niveau de sécurité comme la carte à mémoire,

- modélisation et test de la mise en œuvre de politiques de sécurité, principalement appliqué au cas des réseaux d'entreprise ou d'établissement.

Les collaborations liées à ce thème sont:

- Projet IMAG MODESTE, avec Vérimag (équipe DCS)
- Projet POTESTAT (ACI Sécurité Informatique), avec Vérimag, IRISA (projets Vertecs, Lande et Distribcom)
- Projet GECCOO (ACI Sécurité Informatique), avec l'INRIA (projets Proval, Cassis, Everest)
- BDI CNRS de Nicolas Stouls avec STMicroelectronics

2.1.3.2 Contexte et présentation du projet MODESTE La prise en compte des exigences de sécurité dans un processus de développement devient, pour certains types d'applications, incontournable. Parmi les besoins on peut décliner l'audit qui doit permettre à des évaluateurs de vérifier les exigences initiales de sécurité et leur mise en œuvre effective dans un système. Cette évaluation peut donner lieu à certification, par exemple en suivant l'approche décrite par les Critères Communs[26] [27]. Les exigences de sécurité font donc maintenant partie, au même titre que les aspects fonctionnels, des spécifications de certains types d'applications. La formalisation des contraintes de sécurité, et les utilisations qui peuvent en être faites (vérification, cohérence, conformité d'une implémentation), constitue actuellement une voie de recherche en développement. Comme dans le cas de la sûreté, les exigences portent sur un sous-ensemble bien isolé des fonctionnalités, ce qui rend les approches formelles applicables. Par contre ce domaine est encore mal maîtrisé et bute sur un certain nombre de difficultés. Déjà il n'y a pas nécessairement de consensus sur certaines propriétés (comme l'anonymat et l'opacité par exemple). D'autre part la modélisation de propriété de sécurité nécessite de définir finement les aspects observationnels mis en jeu (accès aux ressources, flot d'information ...) Finalement les techniques classiques de raffinement basées sur la préservation des comportements qui, par définition, préserve les propriétés de sûreté ne s'appliquent pas directement pour les propriétés de sécurité. Par exemple l'implantation correcte d'un protocole protégeant une donnée ne vérifie plus nécessairement cette propriété. L'implémentation peut introduire des canaux cachés qui peuvent permettre de déduire certaines informations sur cette donnée (observation du temps de calcul, interférence avec des valeurs observables ...).

[26] http://www.ssi.gouv.fr/confiance/certificats.html

[27] National Institute Of Standards and Technology. *Common criteria for information technology security evaluation.* Technical report, U.S. Dept. of Commerce, National Bureau of Standards and Technology, Août 1999.

Le projet IMAG MODESTE[28] (Modélisation pour la sécurité : test et raffinement en vue d'un processus de certification, 2004-2006) a pour objectif de s'intéresser aux modèles pour la sécurité sous différentes facettes, c'est-à-dire des propriétés attendues jusqu'aux solutions techniques. L'objectif est de développer un cadre permettant d'exhiber le lien formel entre différents niveaux d'exigences, comme la confidentialité ou l'intégrité, les politiques de sécurité et les mécanismes logiciels ou matériels implantés. Ce projet implique une quinzaine de personnes des équipes VASCO du LSR et DCS de Vérimag et aborde la vérification à partir de modèles selon deux aspects : l'analyse statique (projet MODESTE, RNTL EDEN et ACI GECCOO) et la génération de tests de conformité (projet MODESTE et ACI POTESTAT). Ceci amène à définir différentes interprétations des modèles : une notion de raffinement paramétré par les aspects observationnels à préserver et une relation de conformité qui met en jeu le niveau d'interaction du testeur avec le système et son degré de contrôlabilité. Cette complémentarité a pour objectif de proposer des formalisations qui, d'un point de vue effectif, vont permettre soit de vérifier *a priori* des applications, soit de produire des tests permettant d'évaluer à l'exécution la conformité de l'application vis-à-vis des propriétés attendues.

Dans la première année le travail réalisé dans MODESTE a consisté à développer des études de cas dans différents domaines (cartes à puce, contrôle d'accès, sécurité réseau) en expérimentant différents outils. Nous nous intéressons actuellement aux problèmes soulevés par ces modélisations et l'implication sur les méthodes de construction et de validation.

2.1.3.2.1 Modélisation, raffinement et vérification d'exigences de sécurité Dans cet axe, nous avons mené une validation des propriétés de sécurité d'un porte-monnaie électronique [ACT31]. Nous développons aussi, dans le cadre d'un Master Recherche (2004-2005) un outil permettant de décrire et vérifier des politiques de contrôle d'accès à l'aide de la méthode B (vérification par preuve et production d'un programme de monitoring). Les politiques actuellement traitées sont les politiques discrétionnaires, les politiques multi-niveaux et les politiques basées sur les rôles. Enfin, un travail de construction par raffinement de moniteurs pour des politiques de sécurité de réseau a été mené à partir de propriétés extraites du cas d'étude sur les réseaux [COM77].

2.1.3.2.2 Modélisation et test de la mise en œuvre de politiques de sécurité Dans cet axe, nous avons mené une étude de cas sur les réseaux, qui nous a permis d'étudier le raffinement de politiques de sécurité dans le but de pouvoir décrire les mécanismes requis à différents niveaux de précision ou suivant différents points de vue. Afin de mieux cerner les problèmes de modélisation, nous avons procédé à un inventaire assez complet des différentes facettes de ce qu'on associe à des politiques de sécurité sur des réseaux et des services Internet, dans le cadre

[28] http://www-verimag.imag.fr/~lakhnech/MODESTE

d'une interconnexion entre établissements et sites. Nous avons évalué différents formalismes, principalement basés sur des règles, proposés ces dernières années pour la spécification de ce type de politiques de sécurité. Nous étudions comment définir et tester dynamiquement la conformité d'implantations et de configurations de systèmes à ces règles [ACT58, COM77].

2.1.4 Autres activités de recherche

Ce paragraphe rassemble des activités qui se sont terminées au début du quadriennal ou ne s'inscrivent pas dans les trois thèmes principaux de l'équipe.

2.1.4.1 Effets dans les langages Dans la conception d'un langage de spécification et/ou de programmation, on réalise souvent un compromis entre la simplicité de sa sémantique et la richesse des différents effets mis à la disposition des utilisateurs (effets de bords, gestion des exceptions, nature du passage des paramètres, ...). Il en résulte un fossé entre la théorie et la pratique, mais aussi plus immédiatement une interrogation sur les rapports entre une spécification rigoureuse et sa mise en oeuvre par exemple.

Nos travaux, qui résultent d'une collaboration avec Dominique Duval du LMC, s'inscrivent dans ce contexte. Ils apparaissent comme une alternative à l'approche des monades introduite par E. Moggi. Notre point de départ est la *Logique Diagrammatique* [29] qui repose sur un mécanisme éprouvé de description catégorielle et contient sa propre théorie de la preuve. Notons que les monades correspondent à une description catégorielle des théories algébriques. Un point fondamental de l'approche monadique est qu'elle permet de distinguer les notions de valeurs et de calculs tout en les associant dans un cadre algébrique. Notre approche permet de distinguer ces deux notions mais d'autres également suivant les besoins du problème tout en les associant dans le formalisme logique.

Nous avons étudié l'introduction des exceptions et leurs opérations "raise" et "handle". Cet exemple est intéressant comme le suggèrent Plotkin et Power[30] : "*Evident further work is to consider how other operations such as those for handling exceptions should be modelled. That might going beyond monads, as Moggi has suggested to us*". En particulier, nous avons formulé les opérations "raise" et "handle" directement au niveau de la logique [COM66, AP89, AP90].

Ces études, ainsi qu'une autre application de la logique diagrammatique à l'implantation et au raffinement que nous débutons, est experimenté dans le génie logiciel du calcul formel à travers le projet Imag InCa[31] (auquel participe J.-C. Reynaud).

2.1.4.2 Spécification de scénarios multimédia Dans le cadre d'une co-direction de thèse avec l'équipe Drakkar, nous avons mené des travaux sur la conception et la mise en œuvre d'un langage pour la description de scénarios multimédia. En nous appuyant sur d'autres travaux menés par A. Duda au MIT, nous avons suivi une approche algébrique, qui est une compétence de notre équipe.

[29] D. Duval : *Diagrammatic specifications.* Mathematical Structures in Computer Science 13, 857-890, 2003.

[30] G. Plotkin, J. Power : *Algebraic Operations and Generic effects.* Applied Categorical Structures. 11, 69-94, 2003.

[31] URL : http://www-lmc.imag.fr/MOSAIC/InCa/

Grâce à des opérateurs algébriques, le langage **TAO** permet d'assembler des fragments monomédia (texte, vidéo, son, image, etc.) et de les disposer sur un vecteur temporel (en séquence, en parallèle). L'originalité, par rapport à d'autres méthodes basées sur une logique des intervalles, est que les opérateurs assurent la faisabilité (c'est-à-dire la cohérence temporelle) des scénarios [ACL3, ACT45]. Stéphane Lo Presti, dans sa thèse [TH92] (co-dirigée par A. Duda et D. Bert), a défini le langage, donné un certain nombre de propriétés des opérateurs, en vue de leur compilation dans un pseudo-code. Il a défini la machine virtuelle d'exécution. Enfin, il a proposé des extensions pour traiter d'une manière analogue à la description temporelle, les caractéristiques de présentation des scénarios dans l'espace (dimensions 2D, 3D).

2.1.4.3 Modélisation d'architectures logicielles De 1998 à 2001, le LSR et l'entreprise Dassault Systèmes[32] ont collaboré sur le thème de l'architecture logicielle. Jacky Estublier a assuré la direction de cette collaboration. La thèse de Rémy Sanlaville (soutenue en mai 2002, Bourse CIFRE, dirigée par Yves Ledru) portait sur la modélisation des aspects fonctionnels de l'architecture logicielle et la définition d'un Langage de Description d'Architectures. Rémy Sanlaville travaille actuellement comme spécialiste en architectures logicielles chez France-Télécom.

Le contexte industriel de cette recherche imposait de faire des propositions réalistes et directement applicables. En outre, elles ne peuvent déboucher sur des progrès que si elles sont effectivement adoptées dans la pratique quotidienne des ingénieurs de Dassault Systèmes. C'est pourquoi la première phase de cette recherche nous a amenés à comprendre en détail la technologie de composants utilisée par notre partenaire. Ensuite, nous avons adopté une démarche ascendante qui part d'informations directement extraites du code pour construire une abstraction architecturale du logiciel.

Un environnement de support a été réalisé par l'équipe du LSR [ACT21]. Ces outils offrent diverses vues des composants logiciels et permettent aux ingénieurs de Dassault Systèmes de mieux comprendre les implications architecturales des composants sur lesquels ils travaillent. Le couplage de ces outils avec des données réelles nous a permis au début de l'an 2000 de visualiser chacun des 3800 composants du logiciel CATIA.

Ce travail a reçu un excellent accueil de la part des ingénieurs de Dassault Systèmes. Suite à leurs observations, l'outil a été progressivement adapté pour offrir des représentations plus variées et plus pertinentes. Le travail s'est poursuivi par la mise en place de techniques de simulation d'évolutions de l'architecture, afin d'explorer ce que peut constituer un outil d'aide à la décision en matière de conception.

2.1.4.4 Activités de recherche sur les réseaux Jean-Luc Richier collabore également avec l'équipe Drakkar du LSR dans le cadre de recherches sur les réseaux. Cette collaboration s'est traduite par un co-encadrement de thèse (Pawel Hadam)

[32]dont le principal produit est l'environnement de Conception Assistée CATIA.

et la participation à trois contrats (projet RNRT VTHD++, contrats avec Sun et France Télécom sur IPv6).

2.2 *Résultats majeurs*

Les activités de l'équipe VASCO autour du test correspondent à des projets lancés avant l'actuel quadriennal. Ces projets ont abouti avec la soutenance de thèses, des communications internationales, la réalisation d'outils et la labellisation de nouveaux projets. L'équipe VASCO a acquis une visibilité nationale et internationale sur ces thèmes, qui l'amène à participer au réseau européen TAROT et à deux Actions Spécifiques du CNRS.

- L'outil Lutess, développé par l'équipe depuis une dizaine d'années, est au coeur de plusieurs projets RNRT (VALISERV, VERBATIM), RNTL (DANOCOPS), ou de collaborations directes avec des industriels (Airbus). Les résultats scientifiques concernent d'une part des avancées de l'outil [ACL4, ACT20, ACT26, ACT36], dont une partie résultent de la thèse de Jérôme Vassy[TH95], et d'autre part son adaptation à divers domaines d'application [ACT23, ACT38]. Farid Ouabdesselam a fait deux conférence invitées sur ce thème [INV12, INV14].

- L'outil TOBIAS est le fruit du projet RNTL COTE. Il a été utilisé avec succès en dehors de notre équipe (chez Gemplus et au CLIPS/IMAG) et a fait l'objet d'un référencement auprès de l'Agence de Protection des Programmes. Deux études de cas ont montré sa capacité de détection d'erreurs [ACT27, ACT33]. D'autres résultats scientifiques concernent la maîtrise de l'explosion combinatoire [ACT29], et la mesure couverture à un plus haut niveau d'abstraction [ACL8]. Deux thèses ont été menées autour de TOBIAS, l'une a été soutenue en mars 2005 [TH96] et l'autre sera soutenue avant la fin 2005.

- Depuis plusieurs années, l'équipe VASCO a une activité reconnue dans la recherche d'interactions de services. Cette compétence est à l'origine du projet RNRT VALISERV. Elle s'est traduite par des publications internationales [ACT23, ACT25, ACT32], l'invitation de Lydie du Bousquet à des tables rondes, et la nomination de Farid Ouabdesselam comme Président du Comité de Programme de FIW'07.

Les travaux de l'équipe autour de la spécification formelle et du développement par raffinements correspondent d'une part à des actions engagées avant ce quadriennal (projet BOM, HDR de Marie-Laure Potet), mais aussi à de nouvelles actions qui ont débuté pendant le quadriennal et ont déjà donné des résultats visibles.

- Le projet RNTL BOM a débouché sur la réalisation d'un outil de traduction depuis le langage B0 vers du code optimisé mémoire. L'outil est utilisé par

la société ClearSy et a fait l'objet d'expérimentations réussies et de plusieurs publications [ACL7, ACT24]. Cette compétence est à l'origine de notre participation au projet GECCOO de l'ACI Sécurité Informatique.

- Les travaux menés par Marie-Laure Potet sur le raffinement modulaire [ACL5, OS78] ont fait l'objet de son Habilitation à Diriger les Recherches [TH93]. Ils sont également à la base d'activités menées dans le projet GECCOO.

- L'équipe joue un rôle moteur dans la communauté scientifique réunie autour de la méthode B tant au niveau national [DO86] qu'international : Grenoble a accueilli la conférence internationale ZB en 2002 et Didier Bert a présidé à deux reprises (2002 et 2003) son comité de programme [DO82, DO85].

- Les travaux menés sur la spécification et le raffinement de propriétés dynamiques ont fait l'objet de plusieurs publications significatives [ACL11, ACT22, ACT41].

- Une nouvelle activité a vu le jour autour d'outils pour l'analyse et la documentation de spécifications formelles. Deux outils sont en cours de développement dans le cadre de thèses en cours sur ce sujet. Les premiers résultats sont très prometteurs et ont fait l'objet de plusieurs communications internationales [ACL10, ACT28, ACT31, ACT34].

L'équipe VASCO a fait un fort investissement au cours de ce quadriennal dans le domaine de la sécurité informatique. Cet investissement a abouti à la labellisation de plusieurs projets dans le cadre de l'ACI Sécurité Informatique (EDEMOI, GECCOO, POTESTAT) et au montage du projet IMAG MODESTE. En outre, trois projets relatifs à la sécurité ont été proposés dans le cadre des récents appels de l'ANR.

Enfin, il faut rappeler que l'équipe VASCO résulte du regroupement des équipes SCOP et PFL en fin du quadriennal précédent. Ce quadriennal a été marqué par un gros effort d'intégration des deux équipes. Cet effort nous semble avoir été couronné de succès : d'une part parce que plusieurs projets regroupent des membres des deux anciennes équipes, d'autre part parce que l'ensemble des membres de VASCO souhaitent poursuivre leur activité de recherche au sein de l'équipe pour le nouveau quadriennal.

3 Activités d'encadrement

3.1 *Thèses et HDR soutenues depuis le 01/10/01*

Dans la période considérée, il y a eu une HDR soutenue, celle de Marie-Laure Potet [TH93] et 6 thèses [TH92, TH94, TH95, TH96, TH97, TH98].

La liste des thèses soutenues se trouve en annexe 2.

3.2 *Thèses et HDR en cours*

- DARMAILLACQ Vianney, "Modélisation et Test de politique de sécurité pour les applications réseau", direction R. Groz et J-L. Richier, ED MSTII, UJF, Allocation MENRT, première inscription : octobre 2003.
- DERUYTER Thomas, "Proposition d'un méthodologie "multi-vue" pour la génération automatique des modèles et la réécriture d'une chaîne complète de compilation et d'optimisation de code", direction M-L Potet et J.C. Fernandez (laboratoire Verimag), ED MSTII, INPG, bourse CIFRE cofinancée par la société Freescale, première inscription : novembre 2002.
- IDANI Akram, "B/UML : Mise en relation de spécifications B et de descriptions UML", direction Y. Ledru et D. Bert, ED MSTII, UJF, Allocation MENRT, première inscription : octobre 2003.
- KERMARREC Audrey, "Génération automatique de tests par le calcul de séquences discriminantes", direction R. Groz, ED MSTII, INPG, CDD de France Télécom, première inscription : novembre 2002.
- LAKEHAL Abdesselam, "Critères de couverture structurelle des programmes Lustre", direction F. Ouabdesselam et I. Parissis, ED MSTII, UJF, CDD UJF et ATER UJF, première inscription : novembre 2002.
- MADANI Laya, "Application de l'approche synchrone à la validation de services interactifs multimodaux", direction F. Ouabdesselam et I. Parissis, ED MSTII, UJF, Bourse du gouvernement Syrien, première inscription : janvier 2004.
- MAURY Olivier, "Validation de composants à partir de spécifications multi-vues", direction Y. Ledru et C. Oriat, ED MSTII, UJF, Allocataire MENRT jusque 2003 puis salarié dans le privé, première inscription : octobre 2000, soutenance prévue en novembre 2005.
- RUIZ-BARRADAS Hector, "Spécification et construction de systèmes distribués par raffinements successifs à l'aide de la méthode B", direction D. Bert (CNRS), ED MSTII, INPG, bourse de l'Univ. Autonoma Mexico, première inscription : novembre 2002.
- SELJIMI Beznik, "Utilisation de la Programmation Logique avec Contraintes (PLC) pour la détection de non-conformités dans les logiciels synchrones",

direction I. Parissis et L. Trilling (LSR, équipe Pliage), ED MSTII, UJF, CDD UJF, première inscription : novembre 2004.

– STOULS Nicolas, "Outils formels pour la spécification et le développement modulaires de systèmes", direction M-L. Potet et S. Boulmé, ED MSTII, INPG, BDI CNRS cofinancée par la société STMicro, première inscription : septembre 2003.

4 Collaboration et valorisation

4.1 *Principales relations scientifiques hors contrats*

- Alexandre Petrenko (CRIM, Montréal) a séjourné dans l'équipe en tant que Professeur Invité d'avril à juin 2004. Cette visite s'inscrit dans le cadre d'une coopération suivie avec l'équipe du CRIM. Cette collaboration s'est traduite par une publication de très haut niveau [ACL9]. Une nouvelle visite d'A. Petrenko au LSR est prévue pour le printemps 2006, ainsi qu'un séjour d'Y. Ledru à Montréal en juin 2006.

- Une collaboration est menée avec France Télécom autour de la thèse d'Audrey Kermarec, consacrée à la génération de tests à partir d'automates étendus. Alexandre Petrenko participe également à cette collaboration [ACT59].

- Didier Bert anime le groupe de travail B du GDR ALP, consacré à la méthode du même nom.

- Yves Ledru et Marie-Laure Potet animent le groupe de travail AFADL du GDR ALP (Approches Formelles dans l'Assistance au Développement de Logiciels).

- Depuis février 2005, nous collaborons avec le Laboratoire de Physique Subatomique et de Cosmologie (UJF, INPG, CNRS), sur le thème de la "Validation de logiciels embarqués et testabilité", appliquée à un logiciel de contrôle d'équipements cryogéniques d'un satellite.

- Notre équipe participe au projet PLAVIS (Platform for Software Validation and Integration of Space Systems) regroupant des universités et instituts de recherche brésiliens et français et qui est soutenu par le COFECUB(Comité Français d'Evaluation de la Coopération Universitaire avec le Brésil). Nos partenaires sont : INT (Evry), LaBRI (Bordeaux), ICMC-USP (Université de Sao Paulo), Instituto de Computação, Université de Campinas, Instituto Nacional de Pesquisas Espaciais et trois partenaires brésiliens associés.

  L'objectif du projet est de définir, évaluer et intégrer des méthodes, techniques et outils pour la vérification, la validation et le test de logiciels utilisés dans des applications spatiales (systèmes embarqués et au sol). L'équipe VASCO

apporte son expérience dans le domaine de la validation de logiciels synchrones ainsi que celui de la validation des systèmes de télécommunications.

4.2 *Contrats institutionnels*

La liste des contrats institutionnels est fournie dans le tableau en annexe 4.

4.3 *Contrats (co)financés par un industriel*

La liste des contrats à financement industriel est fournie dans le tableau en annexe 4.

4.4 *Création d'entreprise*

4.5 *Brevets et licences*

Les brevets et licences sont présentés dans le tableau en annexe 5.

5 Publications(01-05)

On trouvera en annexe 3 des indicateurs de production scientifique.

Articles dans des revues avec comité de lecture internationales et nationales

---

Année 2001

[ACL1] D. Bert. Spécification algébrique et prototypage du "contrôle d'accès" en LPG. *Technique et Science Informatiques*, 20(7):849–873, 2001.

[ACL2] F. Duclos, J. Estublier, and R. Sanlaville. Architectures Ouvertes pour l'Adaptation des Logiciels. *Revue Génie Logiciel*, 58:19–25, September 2001.

Année 2002

[ACL3] Stéphane Lo Presti, Didier Bert, and Andrzej Duda. TAO: Temporal Algebraic Operators for modeling multimedia presentations. *Journal of Network and Computer Applications*, 25(4):319–342, October 2002.

[ACL4] I. Parissis. Test de spécifications de logiciels synchrones. *Technique et Science Informatiques*, 21(9):1243–1264, 2002.

Année 2003

[ACL5] Marie-Laure Potet. Spécifications et développements structurés dans la méthode B. *Technique et Science Informatiques, RSTI série TSI*, 22(1):61–88, 2003.

[ACL6] Y. Le Traon, F. Ouabdesselam, C. Robach, and B. Baudry. From Diagnosis to Diagnosability: Axomatisation, Measurement and Application. *Journal of Systems and Software*, 65(1):33–50, January 2003.

Année 2004

[ACL7] F. Badeau, D. Bert, S. Boulmé, C. Métayer, M.-L. Potet, N. Stouls, and L. Voisin. Adaptabilité et validation de la traduction de B vers C - Points de vue du projet BOM. *Technique et Science Informatiques, RSTI, série TSI*, 23(7):879–903, 2004.

[ACL8] P. Bontron and M.-L. Potet. Stratégie de couverture de test à un haut niveau d'abstraction. *Technique et Science Informatiques*, 23(7):905–928, 2004.

[ACL9] A. Petrenko, S. Boroday, and R. Groz. Confirming Configurations in EFSM Testing. *IEEE Trans. Software Engineering*, 30(1):29–42, 2004.

Année 2005

[ACL10] A. Idani and Y. Ledru. Dynamic Graphical UML Views from Formal B Specifications. *In Journal of Information and Software Technology*, 2005. Accepted March 2005, to appear, 16 pages, https://www.editorialmanager.com/infsof/.

[ACL11] Héctor Ruíz Barradas and Didier Bert. Propriétés dynamiques avec hypothèses d'équité en B événementiel. *Technique et Science Informatiques*, 2005. (à paraître).

Conférences invitées

Année 2001

[INV12] F. Ouabdesselam. Approaches and Tools for Synchronous System Testing. In *Workshop on Formal design of Safety Critical Embedded Systems (FEMSYS)*, Munich, Germany, March 2001. Invited Talk.

Année 2003

[INV13] F. Ouabdesselam. Black-box Testing of Reactive Synchronous Software. In *Worshop on Testing Real-Time and Embedded Systems, FME 2003*, Pise, September 2003. Invited Talk.

Année 2004

[INV14] F. Ouabdesselam. Testing Synchronous Reactive Software Against Formal Properties. In *16th IFIP International Conference, TestCom 2004*, Oxford, UK, March 2004. Invited Talk.

Communications avec actes internationales et nationales

— Communications internationales avec actes et sélection —
Année 2001

[ACT15] S. Boulmé and G. Hamon. Certifying synchrony for free. In *Logic for Programming and Reasonning, LPAR'01*, pages 495–506. LNAI 2250, 2001.

[ACT16] L. du Bousquet, H. Martin, and J.-M. Jézéquel. Conformance Testing from UML specifications, Experience Report. In Gesellschaft für Informatik (GI), editor, *p-UML workshop*, volume P-7, pages 43–56, Toronto, Canada, 2001. Lecture Notes in Informatics (LNI).

[ACT17] J.-M. Favre, H. Cervantes, F. Duclos, R. Sanlaville, and J. Estublier. Issues in Reengineering the Architecture of Component-Based Software. In *SWARM forum (Software Architecture Recovery and Modeling) at WCRE '2001 (Working Conference on Reverse Engineering)*, pages 36–41, Stuttgart, Germany, October 2001.

[ACT18] J.-M. Favre, F. Duclos, J. Estublier, R. Sanlaville, and J.-J. Auffret. Describing and Supporting an Industrial Software Component Model. In *Proceedings of the 5th European Conference on Software Maintenance and Reengineering (CSMR 2001)*, pages 95–104, Lisbon, Portugal, March 2001.

[ACT19] Y. Ledru, L. du Bousquet, P. Bontron, O. Maury, C. Oriat, and M.-L. Potet. Test purposes: adapting the notion of specification to testing. In *Proceedings of the 16th International Conference on Automated Software Engineering*, pages 127–134, San Diego, November 2001. IEEE Computer Society Press.

[ACT20] I. Parissis and J. Vassy. Strategies for Automated Specification-based Testing of Synchronous Software. In *16th IEEE International Conference on Automated Software Engineering*, pages 364–367, San Diego, USA, November 2001.

[ACT21] R. Sanlaville, J.-M. Favre, and Y. Ledru. Helping Various Stakeholders to Understand a Very Large Component-Based Software. In *Euromicro Workshop on Component-Based Software Engineering*, pages 104–113, Warsaw, 2001.

Année 2002

[ACT22] H. Ruíz Barradas and D. Bert. Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems. In *Integrated Formal Methods (IFM 2002)*, pages 360–379, Turku, May 2002. LNCS 2335, Springer-Verlag.

Année 2003

[ACT23] K. Berkani, R. Cave, S. Coudert, F. Klay, P. Le Gall, F. Ouabdesselam, and J.-L. Richier. An Environment for Interactive Service Specification. In *7th International Workshop on Feature Interactions in Telecommunication and Software Systems (FIW'03)*, pages 25–41, Ottawa, June 2003. IOS Press.

[ACT24] Didier Bert, Sylvain Boulmé, Marie-Laure Potet, Antoine Requet, and Laurent Voisin. Adaptable Translator of B Specifications to Embedded C Programs. In *FME 2003: Formal Methods*, pages 94–113, Pise, September 2003. LNCS 2805, Springer-Verlag.

[ACT25] L. du Bousquet, F. Ouabdesselam, J.-L. Richier, and N. Zuanon. Testing about some eventuality properties of synchronous software: a case study. In *Synchronous Languages, Applications, and Programming (SLAP'03)*, pages 105–121. Electronic Notes in Theoretical Computer Science (ENTCS), volume 88, July 2003.

[ACT26] I. Parissis and J. Vassy. Thoroughness of Specification-Based Testing of Synchronous Programs. In *14th IEEE International Symposium on Software Reliability Engineering (ISSRE 2003)*, pages 191–202, Denver, Colorado, November 2003.

Année 2004

[ACT27] L. du Bousquet, Y. Ledru, O. Maury, C. Oriat, and J.-L. Lanet. A case study in JML-based software validation (short paper). In *Proceedings of 19th Int. IEEE Conf. on Automated Sofware Engineering (ASE'04)*, pages 294–297, Linz, September 2004. IEEE CS Press.

[ACT28] A. Idani and Y. Ledru. Object Oriented Concepts Identification from Formal B Specifications. In *Proceedings of 9th Int. Workshop on Formal Methods for Industrial Critical Systems (FMICS'04)*, pages 159–174, Linz, September 2004. ENTCS 133 (2005), Elsevier.

[ACT29] Y. Ledru, L. du Bousquet, O. Maury, and P. Bontron. Filtering TOBIAS combinatorial test suites. In *Proceedings of ETAPS/FASE'04 - Fundamental Approaches to Software Engineering*, pages 281–294, Barcelona, 2004. LNCS 2984, Springer-Verlag.

[ACT30] Y. Ledru, S. Dupuy, and H. Fadil. Towards Computer-Aided Design of OCL Constraints. In *Proceedings of CAISE'04 Workshops Vol. 1 -EMMSAD'04: Evaluating Modeling Methods for Systems Analysis and Design*, pages 329–338, Riga, June 2004.

Année 2005

[ACT31] Didier Bert, Marie-Laure Potet, and Nicolas Stouls. GeneSyst: A Tool to Reason about Behavioral Aspects of B Event Specifications. Application to Security Properties. In *ZB2005 Conference*, pages 299–318. LNCS 3455, Springer-Verlag, 2005.

[ACT32] L. du Bousquet and O. Gaudoin. Telephony feature validation against eventuality properties and interaction detection based on a statistical analysis of the time to service. In *Int. Conference on Feature Interactions in Telecommunications and Systems Software (FIW VIII)*, pages 78–95, Leicester, UK, June 2005. IOS Press.

[ACT33] S. Dupuy-Chessa, L. du Bousquet, J. Bouchet, and Y. Ledru. Test of the ICARE platform fusion mechanism. In *12th International Workshop on Design, Specification and Verification of Interactive Systems (DSVIS'05)*, Newcastle upon Tyne, England, July 2005. LNCS, Springer (to appear). 12 pages.

[ACT34] A. Idani, Y. Ledru, and D. Bert. Derivation of UML Class Diagrams as Static Views of Formal B Developments. In *ICFEM'05 - Int. Conf. On Formal Engineering Methods*, Manchester, November 2005. LNCS (à paraître), Springer.

[ACT35] M. Kessis, Y. Ledru, and G. Vandome. Experiences in Coverage Testing of a Java Middleware. In *Fifth Int. Workshop on Software Engineering and Middleware (SEM 2005)*, pages 39–45, Lisbonne, September 2005. ACM (to appear).

[ACT36] A. Lakehal and I. Parissis. Lustructu: A Tool for the Automatic Coverage Assessment of Lustre Programs. In *16th IEEE International Symposium on Software Reliability Engineering (ISSRE 2005)*, Chicago, USA, November 2005.

[ACT37] A. Lakehal and I. Parissis. Structural Test Coverage Criteria for Lustre Programs. In *10th International Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, pages 35–43, Lisboa, Portugal, September 2005.

[ACT38] L. Madani, C. Oriat, I. Parissis, J. Bouchet, and L. Nigay. Synchronous Testing of Multimodal Systems: An Operational Profile-Based Approach.

In *16th IEEE International Symposium on Software Reliability Engineering (ISSRE 2005)*, Chicago, USA, November 2005.

[ACT39] Catherine Oriat. Jartege: A Tool for Random Generation of Unit Tests for Java Classes. In *2nd International Workshop on Software Quality (SOQUA 2005)*, pages 242–256, Erfurt, Germany, September 2005. LNCS 3712, Springer.

[ACT40] V. Prevosto and S. Boulmé. Proof Contexts with Late Binding. In *Typed Lambda Calculi and Applications: 7th, TLCA'2005*, pages 324–338. LNCS 3461, Springer, 2005.

[ACT41] Héctor Ruíz Barradas and Didier Bert. A Fixpoint Semantics of Event Systems with and without Fairness Assumptions. In *IFM 2005 Conference*. LNCS (à paraître), Springer-Verlag, November 2005.

— Autres Communications avec actes (francophones ou de moindre sélection) — Année 2001

[ACT42] D. Bert. Preuve de propriétés d'équité en B : étude du protocole du bus SCSI-3. In J. Souquières, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2001*, pages 221–241, LORIA, Nancy, juin 2001.

[ACT43] P. Bontron, O. Maury, L. du Bousquet, Y. Ledru, C. Oriat, and M.-L. Potet. TOBIAS : un environnement pour la création d'objectifs de test à partir de schémas de test. In *14th International Conference Software & Systems Engineering and their Applications - ICSSEA'2001*, Paris, France, 2001. 7 pages.

[ACT44] Y. Ledru, O. Maury, and C. Oriat. Invariants de liaison pour la cohérence de vues statiques et dynamiques en UML. In J. Souquières, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2001*, pages 23–38, LORIA, Nancy, juin 2001.

[ACT45] S. Lo Presti, D. Bert, and A. Duda. Composition d'objets multimédia à base d'opérateurs. In *7èmes Journées d'études et d'échanges COmpression et REprésentation des Signaux Audiovisuels (CORESA)*, Dijon, novembre 2001.

[ACT46] I. Parissis and J. Vassy. Test des propriétés de sûreté. In *Actes du colloque Modélisation de Systèmes Réactifs (MSR'01)*, pages 563–578. Hermès, 2001.

Année 2003

[ACT47] Frédéric Badeau, Didier Bert, Sylvain Boulmé, Marie-Laure Potet, Nicolas Stouls, and Laurent Voisin. Traduction de B vers des langages de programmation : points de vue du projet BOM. In J.-M. Jézéquel, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2003*, pages 87–102, IRISA, Rennes, janvier 2003.

[ACT48] Pierre Bontron and Marie-Laure Potet. Stratégies de couvertures de tests à haut niveau d'abstraction. In J.-M. Jézéquel, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2003*, pages 173–188, IRISA, Rennes, janvier 2003.

[ACT49] Y. Ledru and S. Dupuy. Expressing dynamic properties of static diagrams in Z. In J.-M. Jézéquel, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2003*, pages 19–34, IRISA, Rennes, janvier 2003.

[ACT50] O. Maury, Y. Ledru, and L. du Bousquet. Intégration de TOBIAS et UCASTING pour la génération. In *16th International Conference Software and Systems and their applications-ICSSEA*, Paris, 2003. 7 pages.

Année 2004

[ACT51] B. Baldassari, C. Robach, L. du Bousquet, and J. Brosse. Early metrics for object oriented designs. In *1st Int. Workshop on Testability Assessment (IWoTA) (in conjunction with ISSRE04)*, pages 62–69, Rennes, France, November 2004.

[ACT52] K. C. Griche and I. Parissis. Automatic Control Flow Based Generation of Stubs for Structural Testing. In *IASTED Int'l Conference on Software Engineering*, Innsbruck, Autria, February 2004.

[ACT53] A. Lakehal, F. Ouabdesselam, I. Parissis, and J. Vassy. Models for Synchronous Software Testing. In *MoDeVa Workshop (satellite event of ISSRE'04)*, pages 41–50, Rennes, France, November 2004.

[ACT54] A. Lakehal, I. Parissis, and L. du Bousquet. Critères de couverture structurelle de programmes LUSTRE. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2004*, pages 185–199, LIFC, Besançon, juin 2004.

[ACT55] T. B. Nguyen, C. Robach, and M. Delaunay. Testability Analysis of Reactive Software. In *1st Int. Workshop on Testability Assessment (IWoTA) (in conjunction with ISSRE04)*, pages 15–25, Rennes, France, November 2004.

[ACT56] H. Ruíz Barradas and D. Bert. Propriétés dynamiques avec hypothèses d'équité en B événementiel. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2004*, pages 299–313, LIFC, Besançon, juin 2004.

[ACT57] N. Stouls and M.-L. Potet. Explicitation du contrôle de développement B événementiel. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2004*, pages 13–28, LIFC, Besançon, juin 2004.

Année 2005

[ACT58] V. Darmaillacq, J-C. Fernandez, R. Groz, L. Mounier, and J-L. Richier. Éléments de modélisation pour le test de politiques de sécurité. In *Colloque sur les RIsques et la Sécurité d'Internet et des Systèmes, CRiSIS*, Bourges, octobre 2005.

[ACT59] A. Kermarrec, R. Groz, B. Parreaux, and A. Petrenko. Machines de mutations pour l'enrichissement de test de protocoles. In *Colloque Francophone sur l'Ingénierie des Protocoles (CFIP 2005)*, pages 33–49, Bordeaux, mars 2005. Hermès.

[ACT60] M. Kessis, Y. Ledru, and G. Vandome. Test de couverture des serveurs J2EE : Etude du serveur J2EE JonAS et de sa suite de tests. In *18th International Conference Software & Systems Engineering and their Applications - ICSSEA'2005*, Paris, novembre 2005. 8 pages.

[ACT61] L. Madani, L. Nigay, and I. Parissis. Testing the care properties of multimodal applications by means of a synchronous approach. In *IASTED Int'l Conference on Software Engineering*, Innsbruck, Austria, February 2005.

Communications sans actes

— Communications avec sélection ou sur invitation —

Année 2001

[COM62] L. du Bousquet. An Approach to Evaluate Testability. In *2nd Int. Workshop on Automated Program Analysis, Testing, and Verification (WAPATAV)*, Toronto, Canada, 2001. 4 pages.

[COM63] Y. Ledru and S. Dupuy. From UML to Z, a support for requirements engineering with RoZ. In *Formal Methods Europe 2001*, 2001. Tutorial.

Année 2002

[COM64] O. Maury, Y. Ledru, P. Bontron, and L. du Bousquet. Using TOBIAS for the automatic generation of VDM test cases. In *Third VDM Workshop (in conjunction with FME2002)*, Copenhagen, Danemark, 2002. 15 pages.

Année 2003

[COM65] Y. Ledru. RoZ, un outil intégrant UML et Z pour la modélisation des systèmes d'information. In *Journée QSL (Qualité et Sureté du Logiciel)*, Nancy, 27 mars 2003.

Année 2005

[COM66] D. Duval and J.-C. Reynaud. Diagramatic logic and exceptions: an introduction. In *Proc. of the Dagstuhl Seminar 05021, Materials, Mathematics, Algorithms, Proofs*, January 2005. http://www.dagstuhl.de/05021/.

[COM67] R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, and F. Peureux. Application of Requirements Analysis Techniques to the analysis of civil aviation security standards. In *First International Workshop on Situational Requirements Engineering Processes (SREP'05), organized by IFIP WG8.1 Method Engineering Task Group, in conjunction with the 13th IEEE International Requirements Engineering Conference*, Paris, France, August 2005.

— Autres Communications —

Année 2001

[COM68] Y. Ledru. Introduction à la journée "Architecture Logicielle". In *Club SEE "Systèmes Informatiques de Confiance"*, Paris, 2001.

Année 2002

[COM69] Y. Ledru. Panel on Future Research Directions in Automated Software Engineering. In *17th International Conference on Automated Software Engineering*, Edinburgh, UK, 2002.

[COM70] Y. Ledru. The TOBIAS Test Generator and Its Adaptation to Some ASE Challenges (position paper). In *Workshop on the State of the Art in Automated Software Engineering, ICS Technical Report UCI-ICS-02-17.* Université de Californie à Irvine, USA, 2002. 5 pages.

[COM71] H. Martin, F. Combret, L. du Bousquet, P. Bontron, and O. Maury. Toward testing automation. In *Gemplus Developer Conference*, Singapore, 2002.

Année 2003

[COM72] L. du Bousquet, J.-L. Lanet, and H. Martin. Enhancing Java Card applet validation process: a methodology and its associated tools. In *e-SMART*, Sophia Antipolis, France, 2003.

[COM73] L. du Bousquet, F. Ouabdesselam, I. Parissis, J.-L. Richier, J. Vassy, and N. Zuanon. Black-box testing of reactive synchronous software. In *SoftTest: UK Testing Research II*. Department of Computer Science, University of York, September 2003.

[COM74] Y. Ledru and S. Dupuy. RoZ, un outil intégrant UML et Z pour l'ingénierie des exigences. In J.-M. Jézéquel, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2003*, IRISA, Rennes, janvier 2003. Tutoriel.

Année 2004

[COM75] D. Bert. Translating CASL Specifications into First Order Logic with Set Theory. In *17ème Workshop on Algebraic Development Techniques, WADT'04*, Barcelone, march 2004.

[COM76] H. Ruíz Barradas and D. Bert. Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems. In *17ème Workshop on Algebraic Development Techniques, WADT'04*, Barcelone, march 2004.

Année 2005

[COM77] N. Stouls and V. Darmaillacq. Formalisation et implantation de politiques de sécurité de réseaux. In *Majecstic 2005*, Rennes, novembre 2005. Poster avec publication d'un papier court.

Ouvrages scientifiques (ou chapitres)

Année 2001

[OS78] M.-L. Potet. Composition des machines et des raffinements. In Henri Habrias, editor, *Spécification formelle avec B*, pages 301–332. Hermes-Lavoisier, Science Publications, 2001.

Année 2002

[OS79] J. Estublier, J.-M. Favre, and R. Sanlaville. An Industrial Experience with Dassault Systèmes' Component Model. In Ivica Crnkovic and Magnus Larsson, editors, *Building Reliable Component-Based Software Systems*, pages 375–386. Artech House Publishers, July 2002.

Direction d'ouvrages

— Édition de livres —

Année 2002

[DO80] G. Cizault. *IPv6, Théorie et pratique (3ème édition).* O'Reilly, 2002. Ouvrage en nom collectif, édité par L. Toutain et J-L. Richier.

— Édition d'actes de colloques, numéros spéciaux de revues —

Année 2001

[DO81] Y. Ledru and M.-L. Potet. Numéro spécial - Approches formelles pour l'aide au développement de logiciels. *Technique et Science Informatiques*, 20(7), 2001.

Année 2002

[DO82] D. Bert, J. P. Bowen, M. C. Henson, and K. Robinson, editors. *ZB2002: Formal Specification and Development in Z and B, 2nd International Conference of Z and B Users*, Grenoble, France, janvier 2002. LNCS 2272, Springer.

[DO83] Y. Ledru and D. Redmiles. Report on the Workshop on State of the Art in Automated Software Engineering. In *17th International Conference on Automated Software Engineering*, pages 307–308, Edinburgh, UK, 2002. IEEE Computer Society Press.

[DO84] B. Marre and F. Ouabdesselam. Numéro spécial - Test de logiciel. *Technique et Science Informatiques*, 21(9), 2002.

Année 2003

[DO85] Didier Bert, Jonathan P. Bowen, Steve King, and Marina Walden, editors. *ZB 2003: Formal Specification and Development in Z and B, 3rd International Conference of Z and B Users*, Turku, Finland, Juin 2003. LNCS 2651, Springer.

[DO86] Didier Bert, Henri Habrias, and Véronique Viguié Donzeau-Gouge (Eds.). Méthode B. *Technique et Science Informatiques, RSTI série TSI*, 22(1), 2003.

Année 2004

[DO87] R. Groz and R. M. Hierons, editors. *Testing of Communicating Systems, 16th IFIP International Conference, TestCom 2004*, Oxford, UK, March 2004. Springer.

[DO88] P. Gruenbacher and Y. Ledru (Eds.). Special issue. *ERCIM News on Automated Software Engineering*, 58, july 2004. http://www.ercim.org/publication/Ercim_News/enw58/.

Autres publications

Année 2003

[AP89] D. Duval, C. Lair, C. Oriat, and J.C. Reynaud. A zooming process for specifications with an application to exceptions. RR 1055 I, IMAG-LMC, 2003.

Année 2005

[AP90] D. Duval and J.-C. Reynaud. Diagrammatic logic and effects: the example of exceptions. Rapport de recherche, LSR, février 2005. http://hal.ccsd.cnrs.fr/ccsd-00004129.

[AP91] H. Ruíz Barradas and D. Bert. Proof obligations for specification and refinement of liveness properties under weak fairness. Rapport de recherche, LSR, février 2005. http://hal.ccsd.cnrs.fr/ccsd-00004181.

Thèses et habilitations

Année 2002

[TH92] Stéphane Lo Presti. *Langage de spécification et de description de présentations multimédias*. Thèse, INPG, Grenoble, France, novembre 2002.

[TH93] Marie-Laure Potet. *Spécifications et développements formels : Etude des aspects compositionnels dans la méthode B*. Habilitation à diriger des recherches, INPG, Grenoble, France, décembre 2002.

[TH94] Rémy Sanlaville. *Architecture logicielle : une expérimentation industrielle avec Dassault Systèmes.* Thèse, Université Joseph Fourier, Grenoble, France, mai 2002.

Année 2004

[TH95] Jérôme Vassy. *Génération automatique de cas de test guidée par des propriétés de sûreté.* Thèse, Université Joseph Fourier, Grenoble, France, octobre 2004.

Année 2005

[TH96] Pierre Bontron. *Les schémas de test : une abstraction pour la génération de tests de conformité et la mesure de couverture.* Thèse, Université Joseph Fourier, Grenoble, France, mars 2005.

[TH97] Karim-Cyril Griche. *Génération Automatique de bouchons pour le Test Structurel basée sur l'analyse du flot de contrôle.* Thèse, Université Joseph Fourier, Grenoble, France, juillet 2005.

[TH98] Pawel Hadam. *Protocoles de distribution du contenu sur des réseaux IPv6 à très haut débit.* Thèse, INPG, Grenoble, France, juin 2005.

6 Principales responsabilités scientifiques et administratives

6.1 Responsabilités scientifiques

Didier Bert est ou a été :

- Coordinateur scientifique du groupe de travail B du GDR ALP (CNRS).
- Responsable du site web de la communauté internationale des utilisateurs de B : http://www-lsr.imag.fr/B/
- Membre du groupe WG1.3 de l'IFIP : Foundations of software specification : http://www.fiadeiro.org/jose/IFIP-WG1.3/
- Président de l'association ("steering committee") pour les conférences B (APCB) : http://www.sciences.univ-nantes.fr/asso/APCB/
- Président du comité de programme B pour les conférences ZB2002 (Grenoble), ZB2003 (Turku).
- Membre du comité de programme de IFM2002 (Turku), IFM2004 (Canterbury), IFM2005 (Eindhoven).
- Membre du comité de programme de UTP'06 (Symposium on Unifying Theories of Programming, Teeside).
- Membre du comité de rédaction de TSI, jusqu'en 2002.
- Expert pour le RNTL en 2003 et 2005.

Sylvain Boulmé a été :

- Membre du comité de programme de la conférence JFLA'2004 (Journées Francophones des Langages Applicatifs).

Lydie du Bousquet est ou a été :

- membre du comité de programme de JAST (Journal of the Association of Software Testing).
- membre du comité de programme de IWoTA (Int. Workshop on Testability Assessment).

Roland Groz est ou a été :

- Rapporteur de la commission 4 (logiciels) du RNRT.
- Membre de la commission d'évaluation du RNTL.
- Membre du comité de rédaction de la revue "Annales des Télécommunications".
- Membre du Steering Committee de la conférence TestCom.
- Coorganisateur (avec Rob Hierons, de Brunel University, UK) du colloque Testcom-2004, 17-19 mars 2004 à Oxford.
- Membre du comité de programme de FORTE/PSTV (Formal Description Techniques/Protocol Specification, Verification and Testing) en 2003.
- Membre du comité de programme de Testcom (Test of Communication Systems) en 2003, 2004, 2005.
- Membre du comité de programme de CFIP (Colloque Francophone sur l'Ingénierie des Protocoles) en 2003 et 2005.

Yves Ledru est ou a été :

- Co-responsable du groupe de travail AFADL du GDR ALP.
- Président du comité de pilotage de la Conférence Internationale IEEE/ACM on Automated Software Engineering (2001-2005).
- Expert auprès de la DSPT9 du Ministère Délégué à la Recherche et aux Nouvelles Technologies, Mission Scientifique Technique et Pédagogique, Département STIC, DS9.
- Membre du comité de programme des conférences internationales ASE, FME, ICFEM, ICSE, SOQUA, ZB.
- Membre du comité éditorial du numéro spécial de la revue "International Journal of Software Tools for Technology Transfer" (Springer) consacré à une sélection d'articles de FM'03 (à paraître en 2005).
- Membre du comité éditorial de la revue JAST (Journal of the Association of Software Testing), créée en 2005.
- Membre en 2003 de l'advisory board de ACM SIGART.

Farid Ouabdesselam est ou a été :

- Directeur du laboratoire LSR depuis janvier 2003.
- Membre de plusieurs comités de programme dont : 26ème "International Conference on Software Engineering" Edimbourg 2004, 7ème et 8ème "Feature Interactions in Telecommunications and Software Systems" Ottawa 2003 et Leicester 2005 (président du 9ème à venir).
- Membre du comité de coordination du réseau de formation par la recherche Marie Curie "TAROT" (Training And Research on Testing).

Ioannis Parissis est ou a été :

- Membre du comité de programme de ISSRE en 2004.

Marie-Laure Potet est ou a été :

- Membre du comité de programme (ZB, inforsid, AFADL).
- Membre du comité de rédaction de TSI.
- Co-responsable du groupe de travail AFADL du GDR ALP.

Jean-Luc Richier est ou a été :

- Expert pour les appels d'offre du 6ème PCRD (IST - Infrastructure) en 2003 et 2005.
- Expert pour l'évaluation d'un projet du 6ème PCRD.

6.2 Responsabilités administratives

Pierre Berlioux est :

- Directeur des études de l'ENSIMAG.

Roland Groz est :

- responsable de l'option ARR du département Télécom de l'INPG.

- membre de la commission consultative d'enseignement du département Télécom de l'INPG.

Yves Ledru est ou a été :

- Responsable de l'équipe VASCO (Validation, Spécification et Construction de logiciels) du laboratoire LSR/IMAG.
- Président de la Commission de Spécialistes de l'UJF 27e section de 2001 à 2004.

Farid Ouabdesselam est ou a été :

- Vice président, de 1998 à 2002, du Conseil d'administration de l'Université Joseph Fourier, en charge du budget et des relations avec le Ministère de l'Education Nationale et 1er vice président.
- Chargé de mission Formation Continue auprès du président de l'UJF en 2003.
- Membre de la commission de spécialistes 26-27 de l'INPG de 2000 à 2004.
- Responsable de l'équipe Vasco du LSR de 1996 à 2002.
- Depuis juin 2005, chargé de mission pour le secteur "Informatique" auprès du vice président recherche de l'UJF ; membre de la Coordination Recherche de l'UJF.

Catherine Oriat est :

- Membre de la commission de spécialistes (section 27) de l'INPG.
- Membre de la commission de spécialistes (section 27) de l'Université de Franche-Comté.

Ioannis Parissis est :

- Responsable de la spécialité Génie Informatique (Professionnalisante) du Mastère Mathématiques, Informatique de l'UJF (anciennement DESS Génie Informatique).

Marie-Laure Potet est ou a été :

- Responsable de l'option Ingénierie des systèmes Informatiques de l'Ensimag.
- Membre élu du CEVU de l'INP Grenoble.
- Membre nommé du Conseil de laboratoire LSR.

Jean-Luc Richier est ou a été :

- Membre nommé de la commission de spécialistes (section 27) de l'INPG de 2003 à 2004.
- Membre de la Commission des moyens informatiques de l'IMAG.
- Président commission moyens informatiques du LSR.

7 Perspectives de recherche 06-10

Les perspectives de recherche de l'équipe VASCO pour 2006-2010 s'inscrivent dans la continuité. L'objectif à long terme reste le développement de méthodes, techniques et outils pour la construction et la validation de logiciels et de systèmes. L'objectif est de pouvoir établir la qualité et la confiance de tels logiciels et systèmes. De nombreux projets et thèses ont démarré au cours des deux dernières années. Leur finalisation marquera le début du nouveau quadriennal et plusieurs d'entre eux devraient se prolonger sur les quatre années.

7.1 Sécurité, construction prouvée

L'activité relative à la sécurité, qui n'existait pas dans l'équipe VASCO il y a trois ans, a pris un très gros essort dans l'équipe VASCO. Trois projets, soutenus par l'ACI Sécurité Informatique, sont en cours et se termineront en 2006 ou 2007. Trois projets liés à cette thématique ont été soumis en 2005 aux appels à projets du RNTL et du RNRT. Tous ces projets montrent une synergie forte entre les thèmes traditionnels de l'équipe (construction prouvée et test) et la thématique sécurité. En ce qui concerne les recherches relatives à la construction prouvée, elles sont toutes menées en liaison avec des projets liés à la sécurité.

- Le projet EDEMOI, consacré à la modélisation de la sécurité des aéroports, a nécessité un fort investissement dans un domaine très spécifique. Nous avons établi des contacts suivis avec les autorités internationale (ICAO/OACI) et européenne (ECAC/CEAC) en la matière. Celles-ci marquent un réel intérêt pour les modèles que nous réalisons, et plusieurs applications de ces techniques sont envisagées (production de check-lists pour les inspections d'aéroports, logiciel d'autoévaluation de la sécurité). Un nouveau projet sera proposé en 2006 aux appels de l'ANR avec les partenaires académiques d'EDEMOI, et d'autres pistes de financement seront étudiées.

- La participation de VASCO au projet GECCOO correspond à des recherches plus fondamentales sur le développement modulaire et sur le dévéloppement formel de programmes à objets. Un objectif à moyen et long terme est le développement d'un calcul du raffinement qui permette de modéliser les aspects objets tout en gardant une maîtrise de l'activité de preuve.

- Le projet POTESTAT étudie la génération de tests de conformité à des politiques de sécurité. Deux projets (POSE, POLITESS) soumis aux appels RNTL et RNRT 2005 renforcent cet effort de recherche en l'appliquant au domaine de la carte à puce d'une part et à l'administration des réseaux d'autre part.

- Deux projets soumis à l'appel RNTL 2005 (POSE, déjà cité, et PEPS, consacré à la validation de règles de sécurité dans les micro-noyaux) s'intéressent égale-

ment à l'utilisation des techniques de preuve, et l'application de la méthode B, au domaine de la sécurité de la carte à puce.

- Enfin, les deux thèses d'Akram Idani et Nicolas Stouls correspondent à une thématique nouvelle, en liaison avec les projets EDEMOI et GECCOO. Elles contribuent à faciliter la compréhension des spécifications formelles. Cet effort sera finalisé dans le cadre de ces deux thèses, notamment par la réalisation de deux outils (GENESYST et B/UML), et nous souhaitons le prolonger au delà de ces deux thèses.

7.2 Test

Nos perspectives en matière de test s'inscrivent d'une part autour de l'évolution et de l'utilisation de nos outils (Lutess, TOBIAS et Jartege), et d'autre part dans des activités plus exploratoires en génération de tests et en testabilité.

- Le développement de l'outil Lutess restera soutenu, avec deux projets en cours (DANOCOPS et VERBATIM) et 3 thèses. Le projet DANOCOPS, et la thèse de Besnik Seljimi, visent l'intégration de techniques de résolution de contraintes numériques dans Lutess. Le projet VERBATIM, où s'inscrit la thèse de Laya Madani, concrétise la collaboration naissante avec l'équipe IIHM du CLIPS et explore un nouveau domaine d'application pour Lutess : les applications interactives multimodales. Enfin notre collaboration avec Airbus, soutenue par la thèse d'Abdesselam Lakehal sur la couverture fonctionnelle d'applications SCADE, devrait se continuer : un projet européen (STREP) a été déposé sur ce thème.

- L'avenir de TOBIAS passe par un effort de réécriture de son noyau de génération de tests. Le mémoire d'ingénieur CNAM de S. Ville sera consacré à ce thème de janvier à décembre 2006. L'objectif est de disposer d'une architecture logicielle ouverte pour d'une part y intégrer diverses techniques de maîtrise de l'explosion combinatoire, et d'autre part garder la notion de tests abstraits instanciables vers une variété de cibles technologiques. D'autres efforts concernent l'application de TOBIAS à de nouveaux domaines. Le projet RNTL POSE (proposé en 2005 à l'ANR) porte notamment sur son application au test de politiques de sécurité. Enfin, un rapprochement est envisagé avec l'atelier Mélusine de l'équipe ADELE, construit sur une démarche d'ingénierie dirigée par les modèles. Le projet ALPE, proposé au RNTL en 2005 et qui s'inscrit dans le cadre du projet régional EMSOC (dans le cadre du pôle de compétitivité Minalogic), s'appuie sur une telle démarche appliquée à une ligne de produits de Schneider Electric.

- La recherche d'interactions de services restera une compétence de l'équipe. Un projet de collaboration (PAI) avec le Nara Institute of Science and Technology

a été déposé en 2005. Il s'agit d'appliquer nos techniques au domaine de la domotique.

- Le projet IMAG CONTEST et notre collaboration avec le Laboratoire de Physique Subatomique et de Cosmologie soutiendront l'activité exploratoire consacrée à la caractérisation de la testabilité du logiciel. Deux directions de recherche seront explorées : d'une part l'établissement de métriques de testabilité basées sur l'expression des besoins (cas d'utilisation) d'un système informatique, et d'autre part l'évaluation de mesures de complexité du code proposées dans la littérature.

- Une nouvelle activité démarre fin 2005 en collaboration avec France Télécom R&D. Il s'agit d'étudier la caractérisation de la qualité d'un assemblage de composants pour lesquels on ne dispose que d'informations partielles (fournies par le fabriquant ou résultant de leur observation). Cette activité est soutenue par une bourse de thèse de FT R&D.

7.3 Domaines d'application

Au cours des dernières années, nos recherches ont principalement été appliquées aux domaines des télécommunications (multiples collaborations avec France Télécom R&D) et des systèmes embarqués (carte à puce, applications aéronautiques et spatiales). Ces domaines d'application seront au coeur de nos futures activités, mais d'autres sont pressentis comme la sécurité des aéroports. Notons enfin que l'adhésion de VASCO au LIG devrait faire émerger l'informatique ambiante comme un nouveau domaine d'application de nos techniques. Le projet d'application des techniques de détection d'interactions à la domotique va dans ce sens, ainsi que les applications visées par le projet VERBATIM.