UMR 6241

Laboratoire d'Informatique de Nantes Atlantique

Bilan scientifique 2006–2009

Projet scientifique 2012-2015

Version 1.0 du 15 septembre 2010

UNIVERSITÉ DE NANTES

ECOLE DES MINES DE NANTES

LINA, Université de Nantes – 2, rue de la Houssinière – BP 92208 – 44322 NANTES CEDEX 3
Tél. : 02 51 12 58 17 – Fax. : 02 51 12 58 97 – http://www.lina.univ-nantes.fr/

Table des matières

1 COLOSS **5**

Chapeau-résumé . . . 5

1.1 Composition de l'équipe au 30/06/2010 . . . 6

1.2 Faits marquants 2006-2010 . . . 7

1.3 Fondements scientifiques . . . 8

1.3.1 Spécification et vérification des modèles à objets et composants . . . 9

1.3.2 Intégration de méthodes formelles et analyse multifacette . . . 9

1.4 Applications et enjeux . . . 10

1.4.1 Systèmes critiques, communicants, hétérogènes, embarqués . . . 11

1.4.2 Internet du futur (architectures, composants et services sûrs) . . . 11

1.5 Nouveaux résultats pour la période 2006-2010 . . . 11

1.5.1 Elaboration d'un modèle à composant formel et multi-services . . . 11

1.5.2 Vérification des composants et de leurs assemblages . . . 12

1.5.3 Multiformalisme et analyse multifacette . . . 13

1.6 Logiciels . . . 15

1.7 Contrats et subventions . . . 16

1.7.1 Projets collaboratifs . . . 16

1.8 Rayonnement . . . 17

1.8.1 Évaluation de la recherche . . . 17

1.8.2 Animation de la communauté . . . 19

1.9 Formation par la recherche . . . 20

1.10 Gouvernance . . . 20

1.11 Auto-évaluation . . . 21

1.12 Bibliographie . . . 23

1.12.1 Publications de référence de l'équipe dans la période . . . 23

1.12.2 Bibliographie externe . . . 25

Équipe
COLOSS

Chapeau-résumé

La sûreté des logiciels et des systèmes informatiques de façon générale est historiquement et fondamentalement un enjeu majeur de la recherche en Informatique. Cette problématique est au cœur des *Grand Challenges* internationaux [1](T. Hoare, R. Milner, J. Woodcok, J. Crowcroft, M. Kwiatkowska) posés à la communauté pour les 10-15 ans à venir ; elle apparaît aussi de façon récurrente dans les programmes nationaux (Agence Nationale de la Recherche) et internationaux (programmes européens PCRD, IST). En guise de repère des exemples de ces défis sont : *The Verifying Compiler* (T. Hoare, ACM, 2003), *The Dependable Systems Evolution* (J. Woodcock, 2003), *The Grand Challenge of Trusted Components* (B. Meyer, IEEE, 2003) et *Verified Software : Theories, Tools and Experiments*, (Hoare & Misra, 2005). Le problème central à résoudre à long terme est celui de disposer d'outils scientifiques pouvant justifier la correction et la sûreté des systèmes informatiques (fonctionnalité, disponibilité, sécurité, fiabilité). Il y a plusieurs sous-problèmes. D'où notre thématique de recherche autour des modèles, des composants, des architectures et des logiciels sûrs.
De nombreuses équipes et des travaux à court et moyen termes sont engagés dans cette voie et attaquent différents sous-problèmes. Les solutions de-ci, de-là formeront un puzzle de concepts et outils du logiciel. Les enjeux sont cruciaux non seulement du point de vue scientifique mais également du point de vue socio-économique : s'assurer que les systèmes, équipements et logiciels, de plus en plus utilisés au

1. www.nesc.ac.uk/esi/events/Grand_Challenges/proposals/

quotidien, sont dignes de confiance et facilement maintenables. Sur le plan de la recherche les problèmes à résoudre sont, par exemple : l'adéquation entre modèles formels élaborés et systèmes réels envisagés, la preuve de correction des systèmes développés à partir des modèles y compris la preuve de l'interaction correcte entre différents sous-systèmes, issus de modèles variés, qui composent les systèmes complexes. Des langages de spécification performants, des techniques et des outils de modélisation et d'analyse formelle appropriés sont à élaborer et à mettre au point.

L'ambition de notre équipe est de contribuer à ces défis en fournissant des méthodes, des techniques et des outils pour le développement de composants logiciels sûrs et pour leur assemblage en logiciels sûrs. Nous projetons nos résultats comme des pièces dans le puzzle des concepts et outils du logiciel.

1.1 Composition de l'équipe au 30/06/2010

L'équipe COLOSS (COmposants et LOgiciels SûrS) est créée en 2005 sous la responsabilité de Christian ATTIOGBÉ avec un noyau de 3 membres permanents.

Permanents au 30/06/2010				
Nom	Prénom	Position	Institution	Arrivée
ANDRE	Pascal	MC	UN	01/09/2003
ARDOUREL	Gilles	MC	UN	01/09/2003
ATTIOGBE	Christian	PR2	UN	01/09/1994
LANOIX	Arnaud	MC	UN	01/09/2008
MOTTU	Jean-Marie	MC	UN	01/09/2009
Membres associés au 30/06/2010				
Nom	Prénom	Position	Institution	Remarques
HABRIAS	Henri	PR	UN	Emerite
VAILLY	Alain	MC	UN	Mission Univ. de Rabat
Doctorants au 30/06/2010				
Nom	Prénom	Position	Institution	Arrivée
MESSABIHI	Mohamed	A	UN	01/09/2007
HANOUSSE	Abdelhakim	PdL	UN	01/11/2008

Personnels temporaires sur la période 2006-2010					
Nom	Prénom	Position	Institution	Arrivée	Départ
SOTIN	Pascal	ATER	UN	01/09/2008	01/09/2009

Évolution de l'équipe sur la période 01/01/2006-30/06/2010

Depuis sa création (juin 2005) et le début du quadriennal, l'équipe a vu l'effectif de son noyau passer de trois membres permanents à cinq membres en septembre 2009. En effet, deux nouveaux collègues ont été recrutés successivement en septembre 2008 et en septembre 2009.

Sur la période, deux collègues ont été membres associés à l'équipe ; Henri HABRIAS (PR) a pris sa retraite en septembre 2008, il est maintenant PR Emerite ; Alain VAILLY (MC), directeur de la Miage puis du département Informatique jusqu'en 2008 est maintenant en charge d'une mission pour la création de l'Université Internationale de Rabat.

1.2 Faits marquants 2006-2010

Structuration et thèmes de recherche L'activité de l'équipe autour de la spécification de composants corrects a émergé en 2005 à partir de la rencontre de deux thématiques qui étaient alors séparément développées dans le laboratoire : celle des méthodes et spécifications formelles d'une part et celle des composants et objets d'autre part.

Une partie des activités de l'équipe se fait autour des méthodes et spécifications formelles et le multi-formalisme pour les spécifications hétérogènes. Cette activité démeure une spécificité de l'équipe nantaise. Les défis que nous attaquons dans cette partie relève de l'hétérogénéité sémantique et de l'-analyse globale de systèmes à multiple constituants ; nous focalisons ici sur les algèbres de processus, la méthode B, les réseaux de Petri avec la définition de passerelles sémantiques ou la complémentarité entre ces approches dans la même spécification.

La constatation était faite en 2005 du manque de méthodes pratiques de vérification par la preuve de la correction de composants logiciels, le pari était alors pris d'utiliser les approches formelles pour développer des composants logiciels corrects selon des propriétés énoncées. Parmi les défis à relever, il y a la proposition d'un langage de spécification formelle et simple, marquant une rupture avec des propositions existantes dans un domaine déjà balisé, où de nombreux concepts étaient utilisés pour structurer souvent de façon informelle les composants. L'exploitation des spécifications formelles à des fins de vérification de propriétés ou de développement par raffinements successifs était un autre défi à relever.

Nous avons relevé en partie ces défis dès 2006 avec la proposition concrète d'un langage de spécification de composants abstraits et formels ; nous avons élaboré et publié le langage de spécification formelle de composants et de leurs assemblages : Kmelia [19]. Nous avons développé diverses méthodes et des outils de vérification des propriétés des composants et assemblages. En collaboration avec l'équipe Ascola et dans le cadre d'un projet régional, nous avons démarré une thèse (co-encadrée par les deux équipes) où nous étudions l'intégration des aspects dans les composants.

Recrutements La dynamique de l'évolution de l'équipe s'est manifestée par le recrutement en septembre 2008 de Arnaud LANOIX comme maître de conférences et en septembre 2009 de Jean-Marie MOTTU comme maître de conférences.

Essaimage Un ancien doctorant (2000-2003)de l'équipe, Gwen SALAUN, a été recruté sur un poste de chaire INRIA-ENSIMAG en septembre 2009.

Publications majeures de l'équipe sur la période

1. **Revue Technique et Science Informatiques (TSI) Hermès-Lavoisier, 2010**. *Construction de Tests Qualifiés de Transformation de Modèles* [1],
2. **Formal Aspect of Components Software (FACS), 2009**. *Using assertions to enhance correctness of components and their assemblies* [9], FACS est une des meilleures conférences pour les travaux à coloration formelle autour des composants logiciels et services.
3. **Software Composition (SC'08 @ ETAPS), 2008**. *Composing Components with Shared Services in the Kmelia Model*[10], SC adossée à ETAPS, est une bonne référence pour la communauté "composition de logiciels".
4. **International ERCIM Wokshop on Formal Methods for Industrial Critical Systems (FMICS), 2008**. *Using CSP||B Components : Application to a Platoon of Vehicles* [13], FMICS

est reconnue comme une des communautés de référence pour les travaux avancés touchant les systèmes industriels critiques.

5. **International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISOLA), 2008**. *Event-Based Approach to Modelling Dynamic Architecture : Application to Mobile Ad-Hoc Network* [11], ISOLA est une des bonnes conférences sur les approches formelles du logiciel.
6. **Software Composition (SC'07 @ ETAPS), 2007**. *Defining Component Protocols with Service Composition : Illustration with the Kmelia Model* [18].
7. **IEEE Transactions on Software Engineering (TSE), 2007**. *A Formal and Tool-Equipped Approach for the Integration of State Diagrams and Formal Datatypes* [15], TSE est une des revues majeures en Génie logiciel
8. **Electronic Notes in Theoretical Computer Science (ENTCS), 2007**. *Adaptation for Hierarchical Components and Services* [16], revue électronique après sélection d'articles de WCAT'2006.
9. **Software Composition (SC'06 @ ETAPS), 2006**. *Checking Component Composability* [19], C. Attiogbé, P. André, G. Ardourel.
10. **International Conference on Formal Engineering Methods (ICFEM), 2006**. *Multi-process Systems Analysis Using Event B : Application to Group Communication Systems* [21], ICFEM est une des conférences majeures abordant les approches formelles du logiciel.

Prix et récompenses, organisation de conférences majeures, conférences invitées

- C. Attiogbé : conférence invitée à SOFSEM'09 ; *35th International Conference on Current Trends in Theory and Practice of Computer Science (SOFtware SEMinar)*, Czech Republic, Mars 2009, (*Can components/services be proved correct ?*).
- l'équipe COLOSS a participé à l'organisation locale de la conférence internationale ECOOP'2006 à Nantes, en collaboration avec les autres équipes de génie logiciel (Ascola, Atlas).

Tableau récapitulatif

Récapitulatif des publications par catégorie												
ACL	ACLN	ASCL	BRE	INV	ACTI	ACTN	COM	AFF	OS	OV	DO	AP
2	2	0	0	1	19	8	0	0	2	0	4	0

1.3 Fondements scientifiques

Nos travaux sont centrés sur la spécification, l'analyse et le développement formels de *composants* et de *logiciels* garantis *sûrs*.

Par *sûreté* d'un système logiciel, nous entendons un logiciel dont le fonctionnement est prouvé correct (par construction à la DIJKSTRA [45, 42, 41, 37], ou par la preuve à la HOARE[46, 38]) et sans défaillance ; c'est-à-dire un fonctionnement tel qu'il est prévu par les spécifications informelles puis les spécifications formelles. Cet axe de recherche fait l'objet de travaux fondamentaux et les bases théoriques sont solides [47, 39, 40, 44, 46, 43].

La qualité et la sûreté des logiciels complexes reposent sur la sûreté des entités logicielles (services, composants, sous-systèmes) qui les composent et sur la correction de leurs assemblages ; ces problèmes sont également attaqués dans [27, 24].

Nous nous intéressons dans nos travaux à certains des nombreux problèmes fondamentaux et technologiques (dont des ouverts), tels que la construction de modèles formels représentant des entités logicielles, la composition des modèles formels, le raffinement de modèles entre différents niveaux d'abstraction, l'établissement de propriétés globales y compris dans le cas du multi-formalisme.

Cos travaux sont articulés autour de deux actions principales présentées ci-après.

1.3.1 Spécification et vérification des modèles à objets et composants

Le cadre général est celui de l'ingénierie de logiciels à base de composants (CBSE [2]) où plusieurs axes sont développés : conception (*Component-Based Design*) ; programmation (*Component-Based Programming*) et vérification de propriétés. Nous travaillons spécifiquement sur les axes conception de composants et vérification de leurs propriétés.

La préoccupation principale est de s'assurer de la correction des composants utilisés dans les assemblages de composants, et aussi des assemblages qui constituent le logiciel final. Des techniques de spécification sont nécessaires en amont. La spécification formelle d'un composant induit des modèles permettant de vérifier mathématiquement les propriétés attendues. Peu de travaux abordent cette approche formelle.

Contrairement à d'autres approches où un composant est vu comme une entité à l'exécution (Szypersky[31], Ivica[28]) et issue d'un code (souvent objets à la Java, C++) structuré de façon adhoc, notre démarche relève de la construction correcte de composants logiciels en partant de leur spécification formelle [29, 25].

Ce que nous cherchons à faire Nous cherchons un modèle à composants abstrait et formel puis un environnement expérimental de développement associé. Dans cette optique nous poursuivons des pistes de recherche pour :

- concevoir et développer des composants logiciels corrects, réutilisables dans la construction de diverses applications,
- concevoir et développer des systèmes à partir de composants et services prédéfinis et validés,
- faciliter la maintenance et l'évolution des composants et applications,
- vérifier la conformité des interactions entre composants et détecter les incompatibilités,
- faciliter l'adaptabilité des composants pour offrir de nouvelles fonctionnalités.

1.3.2 Intégration de méthodes formelles et analyse multifacette

A travers "intégration de méthodes formelles", on entend les formalisme+la sémantique+les systèmes de raisonnement ; en ce sens le multiformalisme est un des aspects de l'intégration de méthodes. L'-analyse formelle multifacette consiste à analyser des systèmes sous différents angles et avec différents techniques et outils appropriés.

Nous nous consacrons ici à l'élaboration de concepts, de techniques et d'outils *multiparadigmes* (ie prenant en compte les facettes données, dynamique, interaction, temps) pour le développement formel des logiciels où ces facettes sont présentes souvent en même temps. Il faut pouvoir écrire des modèles des parties d'un système dans différents langages appropriés, pourvoir interagir entre ces différents modèles, pouvoir vérifier aisément ces différents modèles [34, 32]. Les techniques de plongement sémantique (*semantic embedding*) sont par exemple étudiées.

2. Component-Based Software Engineering, ACM Sigsoft

L'aspect multiparadigme qui permet l'intégration de plusieurs formalismes et sémantiques, constitue l'une des originalités et aussi les difficultés de ces travaux ; en effet contrairement à d'autres approches formelles, l'accent est mis sur la nécessaire complémentarité des langages, méthodes et outils pour réussir le développement des systèmes complexes, hétérogènes par nature [35, 36, 30, 26].

Ce que nous cherchons à faire Nous nous préoccupons des problèmes

- de spécifications hétérogènes,
- de compositionnalité,
- d'hétérogénéité sémantique relatifs aux méthodes ou modèles intégrés, puis
- de la construction d'environnements d'expérimentation et d'analyse formelle associés (vérification de propriétés globales).

En somme l'intégration de méthodes telle que envisagée ici, s'attaque à la résolution de problèmes ouverts :

- expression dans un cadre formel, homogène ou non, de la description d'un système complexe en utilisant éventuellement diverses logiques et techniques appropriées aux aspects considérés du système.
- hétérogénéité et raisonnement global sur le système modélisé et possibilité de raffinements indépendants (compositionnalité).

Le positionnement des travaux de l'équipe COLOSS dans les communautés clairement identifiées en génie logiciel – *méthodes formelles*, *Component-Based Software Engineering* – se situe à la frontière entre les travaux théoriques fondamentaux et les travaux applicatifs ou technologiques.

1.4 Applications et enjeux

Le champ d'application traditionnel des méthodes formelles a été longtemps représenté par les systèmes dits critiques. En effet, pour ces systèmes on tolère très peu, ou pas du tout, des erreurs ou des mauvais fonctionnements. Les méthodes formelles permettent de s'assurer du bon fonctionnement de systèmes.

Le périmètre des systèmes critiques s'est depuis élargi. Les facteurs taille, concurrence, contrôle et interaction complexe entre les composants d'un logiciel, sont désormais des paramètres de la criticité ; en effet les méthodes empiriques de programmation directe suivie de tests, sont alors inefficaces.

Malgré la relative maîtrise de la correction de logigiels de taille réduite (il existe maintenant de nombreux prouveurs de programmes écrits en langage de haut niveau), on ne sait toujours pas garantir la correction ou le bon fonctionnement de logiciels de grande taille (en millions de ligne de code), avec des composants hétérogènes, à forte interaction, par exemple des applications déployées sur un réseau dense ou à l'inverse de petites applications déployées en très grand nombre (par exemple sur des assistants électroniques).

Les méthodes de spécification et de vérification formelle s'attaquent à ces systèmes critiques ; ils présentent des caractéristiques communes au sens de la complexité : comportement non trivial, fort impact d'un dysfonctionnement, prédominance de contrôle, de données, de contraintes de temps, hétérogénéité, déploiement à grande échelle, etc.

1.4.1 Systèmes critiques, communicants, hétérogènes, embarqués

Nous expérimentons nos propositions sur divers bancs d'essais (*benchmarks*). Nous avons traité par exemple le cas d'étude CoCoMe qui a été utilisé pour confronter diverses méthodes formelles [3]. Ce cas se caractérise par de forte interaction entre de nombreux composants dans un système global.

Nous avons fait des expériences sur la modélisation et la vérification pour la communication de groupe et les architectures dynamiques [11, 21]. Nous avons mis à l'épreuve nos propositions sur la modélisation et la vérification des propriétés de réseaux mobiles à structrure adhoc (les réseaux MANET [4]).

Nous avons montré diverses façons de traiter l'hétérogénéité sémantique par exemple en combinant des modèles à l'aide de réseaux de Petri, de réseaux de processus en Promela ou en B.

Nous cherchons à développer des composants génériques spécifiés conjointement avec les paramètres de l'environnement ciblé pour les accueillir, par exemple une gamme d'équipements avec du contrôle embarqué sous forme de logiciels. Cette approche constiturait à terme une contribution significative au développement prouvé de systèmes embarqués où les méthodes de test prédominent actuellement.

1.4.2 Internet du futur (architectures, composants et services sûrs)

Interaction, hétérogénéité, fiabilité sont des caractéristiques maîtres de l'environnement que structurent dès aujourdhui, les logiciels, les services applicatifs disponibles sur Internet, les grilles de calcul, les assistants numériques, les abonnements des usagers aux services divers, les systèmes de santé, les systèmes bancaires, la domotique, la télémédecine, etc. L'Internet du futur mêle les architectures de réseaux d'ordinateurs, sur lesquelles sont/seront déployés des services nombreux et variés. L'impact des dysfonctionnements des composants logiciels dans cet environnement fortement maillé est critique et doit pour cela être confiné, en exploitant les possibilités des méthodes formelles, par exemple à travers l'emploi de composants et de services sûrs, avec des modèles d'interaction soigneusement analysés au préalable.

Le logiciel est ici encore, un élément important, d'autant plus qu'il est critique voire périlleux de faire dépendre toute une partie d'activités socio-économiques, de services ou composants logiciels non corrects, non fiables et non disponibles.

Le domaine de l'Internet du futur, est par conséquent un de ceux où les approches formelles permettent/permettront de modéliser et développer des services corrects fiables, d'assurer la maintenance des services (disponibilité, évolutions, adaptation, reconfiguration, remplacement, etc) [4, 10].

Dans cette optique, nos travaux contribuent à développer des composants et des services sûrs, pour des environnements hétérogènes, à modéliser le comportement de composants logiciels afin de les analyser et de les corriger avant implantation pour un environnement cible.

1.5 Nouveaux résultats pour la période 2006-2010

1.5.1 Elaboration d'un modèle à composant formel et multi-services

Participants : P. ANDRÉ, G. ARDOUREL, C. ATTIOGBÉ, H. HABRIAS, A. LANOIX

Le problème de la construction de composants dignes de confiance [47, 33] rejoint dans le fond la question de savoir comment construire un programme correct ou des modules de programmes corrects ;

3. http://agrausch.informatik.uni-kl.de/CoCoME/
4. Mobile Adhoc Network

s'y ajoutent pour les composants logiciels généraux, les contraintes de dépendances vis à vis de leur environnement pour les interactions, la forte exigence pour la réutilisation et l'adaptation à l'environnement d'utilisation.

Nous avons apporté une contribution significative en proposant un modèle formel (Kmelia) doté d'un langage éponyme, qui permet de spécifier avec un nombre réduit de concepts, des composants logiciels intégrant plusieurs services et publiant une interface constituée de services [19] ; certains services sont accessibles contextuellement c'est à dire uniquement à travers un appel préalable à d'autres services de l'interface. Nous avons abordé le problème en faisant table rase des multiples notions qui polluent la littérature puis en repartant des concepts élémentaires pour définir un noyau autour duquel nous avons bâti progressivement notre modèle.

Composabilité et compatibilité comportementale Nous avons défini formellement la composabilité des composants. Sur la base de ce résultat [19], nous pouvons désormais vérifier formellement la bonne définition de compositions de spécifications Kmelia. Ce résultat est prolongé par la définition de méthodes d'analyse de la compatibilité comportementale de composants parallèlement composés : ici nous avons utilisé les produits synchronisés de systèmes de transition et des techniques de *model-checking* pour effectuer les expérimentations [19, 23] en nous servant de plateformes comme MEC [5] ou Lotos/CADP [6]. Nous avons développé une plateforme expérimentale COSTO (COmponent Study Toolkit) pour accompagner l'élaboration du modèle, du langage et des outils d'analyse.

Mécanismes de structuration verticale et protocole d'emploi des composants Nous avons proposé dans [18] un mécanisme d'annotation des états des systèmes de transition qui représentent les services, pour permettre la composition des services de façon verticale dans un composant. L'idée est d'autoriser l'appel d'autres services du composant, tout en gardant un système de transition simple. Cette possibilité complète la composition horizontale inter-composant. L'annotation des états puis des transitions par des possibilités ou des obligations d'appel d'autres services, a aussi été utilisée pour exploiter des services comme mode d'emploi des composants : c'est la notion de protocole. L'originalité de la solution proposée réside dans le fait que les concepts de Kmelia ne sont pas multipliés, mais qu'ils restent réduits. Dans le prolongement de ces travaux, nous avons développé des mécanismes d'adaptation pour rendre compatibles du point de vue du comportement, des composants qui ne l'étaient pas. Ces résultats sont consignés dans [16].

Composition avec interaction multi-parties Nous avons étendu le modèle abstrait des composants Kmelia pour permettre la description de composition de composants avec des interactions impliquant plus de deux services [9]. La notion de services partagés a été introduite ainsi que des opérateurs de synchronisation n-aires pour contrôler explicitement les interactions. Ces opérateurs sont des extensions aux opérateurs habituels (émission, réception) de communication entre processus ; nous les avons étendus pour prendre en compte un ou plusieurs émetteurs, des canaux spécifiques, des rôles, des messages et des arguments. Ces travaux peuvent servir à modéliser le comportement d'applications Internet avec de nombreux services ou composants interagissant de façon complètement libre.

1.5.2 Vérification des composants et de leurs assemblages

Participants : P. ANDRÉ, G. ARDOUREL, C. ATTIOGBÉ, A. LANOIX, M. MESSABIHI

5. LaBRi, Bordeaux
6. Inria VASY, Grenoble

Une partie de nos efforts a été consacrée à l'exploitation des spécifications formelles Kmelia à des fins de vérification. Le langage de données de Kmelia a d'abord été étendu pour exprimer des traitements conséquents et des assertions. Les résultats présentés ci-après ont fait l'objet de publications dans des conférences internationales.

Vérification des assemblages à travers des assertions Une des limitations des langages à composants est l'expressivité de leur langage de donnée. Nous avons réduit ce verrou dans Kmelia en définissant un langage de données suffisamment expressif pour un cadre expérimental. Par conséquent nous pouvons exprimer dans le langage, des assertions sous la forme de Pre/Post-conditions pour les services et aussi les invariants des composants. Les assertions sont utilisées pour l'analyse formelle des systèmes conçus à l'aide de composants : la preuve de cohérence des services par rapport à leur assertions pre-post, la cohérence des services par rapport à l'invariant de leur composant. Toutes ces vérifications de propriétés sont basées sur des obligations de preuve clairement élaborées pour notre modèle Kmelia. Ces résultats sont accessibles dans [9, 5]. Nous avons développé divers modules dans notre plateforme COSTO pour expérimenter ces résultats.

Preuve de la cohérence des composants et assemblages Nous avons conçu une méthode de vérification de composants et assemblages Kmelia [3], qui se base sur la plateforme de spécification et de preuve en B (Event-B / Rodin). Nous utilisons les systèmes abstraits B pour montrer la cohérence de composants Kmelia ; pour ce faire, notre méthode permet de générer en extrayant les informations de spécifications Kmelia, des machines abstraites B de telle sorte que leur preuve de cohérence en B corresponde aux obligations de preuve dont nous nous sommes dotés. En ce qui concerne les données très élaborées et les assemblages via les services, nous utilisons les raffinements entre des spécifications B générées à différents niveaux de services. La plateforme Rodin est utilisée pour effectuer les expérimentations [9, 3]. Notre plateforme COSTO propose des modules, par exemple un plugin Kml2B, servant de passerelles.

Utilisation des contrats pour la vérification à différents niveaux Dans [2] nous avons montré comment les contracts (sous la forme d'assertions Pre/Post) permettent de systématiser la vérification des assemblages de composants. Ce travail prolonge les résultats présentés dans [9].

Rétroingénierie : exraction d'architecture de composants Dans le cadre du projet ECONET, nous avons élaboré des techniques et des outils pour l'extraction de composants à partir d'applications écrite en Java. Une partie de ce travail est publiée dans [6]

1.5.3 Multiformalisme et analyse multifacette

Participants : C. ATTIOGBÉ, A. LANOIX, J. MOTTU

Modéliser et analyser des systèmes sous différents angles et avec différents outils est une solution pour la maîtrise de leur complexité intrinsèque. Néanmoins peu d'équipes travaillent sur cette problématique. L'hérétogénéité sémantique et son prolongement que constitue l'analyse globale des systèmes sont des préoccupations qui requièrent beaucoup d'énergies. Nous avons apporté des contributions dans ce contexte, et de différentes manières sur ces préoccupations : proposition de méthodes de spécifications, de techniques d'analyse, de techniques de vérification de transformation de modèles par des techniques de tests.

Méthode pour la spécification hétérogène Nous avons mis au point une méthode (*P-B) pour la spécification des systèmes multiprocessus avec architecture dynamique (adhoc) [21].

La méthode combine les machines à états avec la composition de machines abstraites en Event B. Elle permet de spécifier étape par étape des systèmes à multiple processus avec des classes

de comportements identifiées dans l'analyse des besoins. Elle a été appliquée pour modéliser les systèmes de communication de groupe et pour vérifier leurs propriétés [21].

Dans le prolongement de ces résultats, nous avons élaboré une méthode d'analyse multifacette qui consiste à combiner des techniques de preuve de propriétés et des techniques d'évaluation de modèle utilisant le même modèle dit modèle de référence sémantique, afin de prendre en compte de façon cohérente les rétro-actions issues des analyses. Des expérimentations de validation ont été effectuée avec les outils autour de la méthode B [20, 22]. Dans [13], le formalisme CSP||B qui permet le contrôle de machines abstraites B par des processus CSP a été expérimenté pour la spécification de système de contrôle de véhicules. Dans [15] nous avons proposé une méthode générique pour l'intégration de données formellement décrites dans des formalismes à base de systèmes de transition.

Interopérabilité sémantique Nous avons apporté des contributions dans le domaine de l'interopérabilité entre modèles sémantiques en proposant une méthode d'analyse multifacette partant d'un modèle sémantique dit de référence à partir duquel on peut dériver et particulariser différents autres modèles pour en faire l'object d'analyses diverses. Ces résultats sont publiés dans [12].

Dans le cadre de l'intégration de formalismes ou de différentes méthodes nous avons proposé une solution s'appuyant sur un formalisme de référence, générique et abstrait (les systèmes de transition abstraits) dans le quel nous traduisons des formalismes donnés et à partir duquel nous traduisons vers d'autres formalismes. Notre contribution considère des bases de compatibilité sémantique entre les formalismes. Par exemple les systèmes de transition constituent une famille sémantique que nous avons utilisée pour définir des passerelles entre B, les réseaux de Petri, Promela/Spin, etc. Un environnement expérimental accompagne ces recherches et les résultats dans cette voie ont été publiés dans [22, 12] sur l'interaction entre les modèles et les outils de preuve ou de *model-checking*, [8] pour le plongement entre réseaux de Petri et B ou la sémantique opérationnelle des réseaux de Petri est exprimée de façon générique à travers des machines abstraites Event B. Un outil (PN2B) y est consacré comme module de notre plateforme ATACORA.

Méthodes de modélisation en Event B d'architectures dynamiques Nous avons poursuivi et étendu les travaux autour de la méthode *P-B. Les systèmes répartis, à grande échelle, et les systèmes à forte interaction n'ont pas d'architecture fixe prédéfinie. Il est alors difficile de les analyser avec les outils classiques tels que la composition de machines à états. Nous avons proposé une solution basée sur une approche événementielle à la Event-B, pour modéliser et analyser formellement de tels systèmes avec une architecture dynamique. Nous avons expérimenté notre solution sur les réseaux mobiles sans architecture (réseaux adhoc ou MANET) par exemple, les résultats sont publiés dans [11, 7].

Tests de transformation de modèles Nous avons présenté dans un article de synthèse [1] des contributions pour la construction de tests qualifiés (adaptés aux transformations et leurs emplois) pour les transformations de modèles. Nous avons proposé plusieurs fonctions d'oracles et qualifié leur emploi selon leur adéquation avec la complexité et la réutilisation d'une transformation. Pour qualifier les tests construits, nous étudions et modélisons les fautes spécifiques aux transformations de modèles. Cela permet ensuite de qualifier les modèles de test et les oracles encapsulés avec la transformation dans un composant. Les informations fournies par l'analyse de mutation permettent la construction de nouveaux tests qui améliorent la qualité de l'ensemble des tests construits et augmente le niveau de confiance dans le composant.

1.6 Logiciels

Dans la stratégie de valorisation de nos travaux, le développement de prototypes prend une part importante ; nous appuyons nos publications académiques systématiquement sur des expérimentations. Les résultats sont ainsi dans un premier temps publiés dans des ateliers et conférences et, nous visons des revues ou conférences à très fort impact en nous appuyant sur l'accumulation des résultats intermédiaires des travaux abordant aussi bien les concepts, les outils développés et les expérimentaions. Le travail autour de Kmelia/COSTO est une bonne illustration de cette stratégie.

COSTO URL

Participants : G. Ardourel (resp), P. André, G. Ardourel, C. Attiogbé, A. Lanoix, M. Messabihi, J-M. Mottu
Type de licence : non diffusé
Mots clés: COLOSS, Kmelia, Eclipse, Java

COSTO (COmponent STudy Toolkit) est une plateforme construite pour accompagner l'utilisateur lors de la spécification et l'analyse de composants et assemblages avec le langage Kmelia. Le développement de COSTO a commencé en 2005. COSTO comprend un analyseur syntaxique du langage de spécification de composants logiciels (Kmelia), des techniques d'analyse de composabilité de composants et des passerelles vers des outils logiciels éprouvés : LOTOS/CADP, MEC, ATELIER B, KEY. Il est développé dans l'environnement Eclipse et est utilisable sous forme de plugins Eclipse qui s'intègrent ainsi facilement dans les outils de génie logiciel. Parmi les plugins récents développés, il y a KML2B, un traducteur de kmélia vers B (une variante pour Event B est aussi étudiée). COSTO est utilisée pour illustrer les expérimentations appuyant les résultats que nous publions autour de Kmelia. Les publications spécifiques à la plateforme COSTO et son utilisation sont [23, 14].

ORYX/ATACORA URL

Participants : C. Attiogbé (resp), Etudiants Master2
Type de licence : non diffusé
Mots clés: COLOSS, Eclipse, Java, Antlr

ORYX/ATACORA est un prototype logiciel développé dès 2003, dans le cadre d'un projet interne (nommé Projet Atacora) et consacré à l'analyse multifacette, la combinaison des techniques de vérification (*theorem-proving* et *Model-checking*), la combinaison de fomalismes ; l'intégration de modèles sémantiques hétérogènes. Dans ce cadre nous avons envisagé une plateforme pour la génération d'environnements de spécification, avec des interactions entre modèles sémantiques, passerelles entre outils de vérification, B, PVS, Promela/Spin, RdP, Algèbre de processus, ...
ORYX/ATACORA est développé autour d'un formalisme abstrait (*Abstract Transition Systems)* ; il comprend des passerelles entre Promela/Spin, B, réseaux de Pétri, systèmes de transition variés. Un nouveau module (Pn2B) a été récemment développé ; il réalise un plongement sémantique de réseaux de Petri en systèmes abstraits B [8].

JavaCompExt URL

Participants : P. André,J-C Royer (resp), P. André, G. Ardourel, J-C Royer, Etudiants Master 2
Type de licence : -
Mots clés: COLOSS, ASCOLA, Reverse Engineering, Component, Eclipse, Java JDT

Le projet JavaCompExt est destiné à extraire des informations d'architecture à partir d'un code source Java. Les informations extraites sont des composants et des types de données, la structure de composants, les communications, le sous-typage, services requis et fournis. Ce projet sert à la fois à la recherche d'architectures à composants et à l'analyse quantitative et qualitative de programmes modulaires (restructuration). Une présentation succincte est donnée dans [6].
Un premier prototype CoExAn (*Component Extraction and Annotation*, `www.lina.sciences.univ-nantes.fr/coloss/softwares/indexen.php`) de rétro-ingénierie de composants a été développé dans le cadre du projet Econet (2008).
Ce prototype, basé sur un métamodèle commun et des règles d'annotation de code Java, est une boîte à outils d'extraction-agrégation d'informations. Un processus de rétro-ingénierie consiste à appliquer un outil à chaque itération. On peut annoter un programme Java à partir d'informations utilisateur, construire un modèle à composants à partir d'un programme Java annoté, construire un modèle à composants à partir d'un programme Java non annoté, réaliser des transformations de modèles telles que la fusion, la sélection... sur le couple (code, modèle)... Ce premier prototype définit le cadre global qui est repris dans le projet JavaCompExt, qui en définit une brique.

1.7 Contrats et subventions

Tableau des contrats et subventions

Type	Nom	Institution gestionnaire	Début/Durée	Montant/Equipe
Europe	ECO-NET (Cluj, Nantes, Prague)	Egide, Fr	2007/24mois	20K €/8,5K €
Région	Projet régional MILES-IL (Pays de la Loire)	UN	2007/36mois	200K €/ 33K €
Région	Projet régional COM (Pays de la Loire)	UN	2006/36mois	? ? €

1.7.1 Projets collaboratifs

Actions régionnales

MILES/Ingénierie Logicielle (IL) URL
Début: 01/01/2007, **durée:** 36 mois
Partenaires : ASCOLA, COLOSS, MODAL, Atlas GDD (J. Bezivin) **Coordinateur :** 2007 : P. Cointe ; 2008-2009 : C. Attiogbé et M. Südholt
Participants : F. Benhamou (resp), les équipes GL
Montant équipe : ˜ 3K€(équipe COLOSS) **Montant total :** ˜ 200 K€
Mots clés : Ingénierie Logicielle

Dans le cadre du projet Miles, cinq équipes de génie logiciel de la région (Nantes, Laval-Le Mans) se sont regroupées pour faire emerger un axe ingénierie logicielle au niveau de la région. Des séminaires communs ont été organisés. Deux thèses inter-équipes ont été mises en route dont une sur la combinaison entre les composants (COLOSS) et les aspects (ASCOLA). L'autre thèse est effectuée dans le domaine de l'ingénierie des modèles (Ascola+AtlanMod). Les deux thèses sont en cours. Dans le cadre de ce projet nous avions mené les premières réflexions sur une grande équipe fédérant les équipes nantaises de génie logiciel.

Projets nationaux

En 2009 puis en 2010 nous avions formé un consortium de 4 partenaires universitaires (LINA, LORIA, LIFC, LISI) et de 3 industriels (ClearSy, Somfy, Smartesting) et soumis un projet ANR. Le projet n'a pas été retenu pour financement mais nous entrenenons les collaborations avec les partenaires.

Projets internationaux

ECO-NET Egide : ***Behaviour Abstraction from Code*** URL
Début: 01/01/2007, **durée:** 24 mois
Partenaires : équipe DSRG de Charles University (Prague, CZ), équipe GL de Babes-Bolyai Univ. (Cluj, RM), COLOSS et ASCOLA du LINA **Coordinateur :** P. André
Participants : P. André (resp), équipe COLOSS, ASCOLA du côté nantais
Montant équipe : 8,5 K€ **Montant total :** 20 K€
Mots clés : Rétroingenierie, Méta-modélisation, Composants

Le projet est intitulé *Behaviour Abstraction from Code*. Le cadre général de la préoccupation de ce projet est de trouver des solutions pragmatiques au problème que constitue l'absence de liens et de cohérence entre les modèles ou spécifications initiales et les codes (ou composants) développés de façon industrielle mais empirique. L' approche proposée dans ce projet consiste à partir du code de composants existants et de vérifier qu'ils sont conformes à certaines interfaces ou protocoles. Il s'agit dans ce cas de faire une analyse du programme et d'en extraire des informations qui vont être utilisées pour en vérifier la conformité avec les modèles. Cette approche que nous qualifions d'ingénierie indirecte ou rétro-ingénierie a été très peu explorée dans ce domaine. Le but de ce projet est de contribuer à une meilleure maîtrise de la problématique de l'ingénierie indirecte des composants. Notre solution passe par le développement de techniques pour extraire des informations du code.

1.8 Rayonnement

1.8.1 Évaluation de la recherche

Comités de programme (conférences) et de lecture (revues)

- **Revues**
  - *Comités éditoriaux de revue scientifique*
  - *Les comités de lecture (et numéro spécial d'une revue)*
    - C. Attiogbé : Journal Européen des Systèmes Automatisés (JESA), 2009
    - C. Attiogbé : numéro spécial de *Formal Aspects of Components Software (FACS)*, consacré à une sélection d'articles de la conference ABZ2008, London, 2009.

  - C. Attiogbé : numéro spécial de Technique et Science Informatique (TSI) consacré à la Composition : objets, services, composants, 2009.
  - P. André : *Software and System Modeling (SOSYM)*, 2008.
  - P. André : *Journal of Systems and Software (JSS)*, 2009.
  - P. André : numéro spécial Technique et Science Informatiques (TSI), 2010.
  - P. André : numéro spécial de Revue Africaine de la Recherche en Informatique et Mathématiques Appliquées (ARIMA, Inria, AUF), 2009.
  - J-M. Mottu : *Information and Software Technology (Elsevier)*, lecture en cours 2010.
- **Coordination de revue**
  - P. André, C. Attiogbé : Coordination d'un numéro de la Revue L'OBJET Vol.14(4) : Composants, Services et Aspects, Hermès, 2008
- **Conférences**
  - *Comités de programme*
    - P. André : Langages, Modèles, Objets (LMO), 2007, 2009, 2010
      Conférence Francophone de Modélisation et Simulation, MOSIM (2006),
      UML & formal methods, (UML_FM) (2008, 2009, 2010),
      Conférence Africaine de la Recherche en Informatique (CARI) 2008, 2010.
    - G. Ardourel : Langages, Modèles, Objets, (LMO) 2007.
    - C. Attiogbé : Property Verification of Components and Services (ProVeCS@TOOLS'07),
      Conference ZB'07, Integration of Formal Methods (IFM, 2007),
      Formal Method in Education (FORMED@ETAPS, 2008),
      From Research to Teaching Formal Methods : B Method (TFM-B) 2008, 2009, 2010,
      Integration of Model-based tools (IM_FMT@IFM, 2009).
    - A. Lanoix : Approches formelles d'aide au développement du logiciel (AFADL), 2010,
      From research to Teaching Formal Methods : B Method (TFM-B), 2010.
  - *Rapports pour un membre d'un comité de programme*
    - M. Messabihi : Approches formelles d'aide au développement du logiciel (AFADL), 2010 ;
    - P. André : IFM (2007), BZ 2007
    - J-M. Mottu : AFADL 2010, ICSE (2008),
      ACM/IEEE Model Driven Engineering Languages And Systems (MoDELS 2008),
      CBSE (2008), ICST (2008), Modelisation Verification and Validation (MoDeVVa, 2008),
      ISSRE (2006, 2007), Mutation (2007), ECMDA (2009),

Rapports de thèse, comité de sélection, concours INRIA, ...

- C. Attiogbé : président des comités de sélection (postes de PR et MdC affectés à l'IUT) de l'Université de Nantes, 2009 ;
- C. Attiogbé : Rapporteur, Jury de Inès Mouakher, *Vérification et correction des spécifications B : application à l'assemblage de composants*, Thèse de l'Université Henri Poincaré, Nancy 1 et de l'Université de Tunis, (sous la direction de J. Souquières et Khaled Bsaies), jury prévu fin 2010
- C. Attiogbé : Rapporteur, Jury de Cécile Hardebolle, *Composition de modèles pour la modélisation multi-paradigme du comportement des systèmes*, Thèse de l'Université Orsay Sud, Supélec, (sous la direction de G. Vidal-Naquet et F. Boulanger), Décembre 2008
- C. Attiogbé : Rapporteur, Jury de Eun-Young Kang, *Abstractions booléennes pour la vérification des systèmes temps-réel*, Thèse de l'Université Henri Poincaré, Nancy 1, (sous la direction de S. Merz), Novembre 2007
- C. Attiogbé : Examinateur, Jury de thèse de S. Djoko Djoko, *Analyses et vérification des pro-*

grammes à aspects, Thèse de l'Université de Nantes, EMN (sous la direction de MM Rémi Douence et Pascal Fradet), Juin 2009
- C. Attiogbé : Examinateur, Jury de thèse de L.D. Benavides, *Les aspects distribués : pour une meilleure séparation des préoccupations transverses dans les logiciels distribués*, Thèse de l'Université de Nantes, EMN, (sous la direction de M. Sudholt, P. Cointe), Janvier 2009
- C. Attiogbé : Examinateur, Jury de Miloud Rached, *Spécification et vérification des systèmes temps réels en B*, Thèse de l'Université Paul Sabatier, Toulouse III, (sous la direction de J-P. Bodeveix), Mai 2007

1.8.2 Animation de la communauté

Participation à des *steering comittees*, des GDR et leurs groupes de travail
- C. Attiogbé : membre du comité de pilotage (*steering committee*) des conférences sur la méthode B (APCB)

Conférences invitées
- C. Attiogbé : *Can Services/Components be proved Correct ?, 35th International Conference on Current Trends in Theory and Practice of Computer Science (SOFtware SEMinar)*, Czech Republic, Mars 2009

Organisation de conférences, d'ateliers, d'écoles d'été
- C. Attiogbé : Co-Chair (avec D. Méry, Loria Nancy) de TFM-B'2010 @ JS 2010, organisée par équipe COLOSS, Nantes, juin 2010
- C. Attiogbé : Co-Chair (avec D. Méry, Loria Nancy) de TFM-B'2009 @ JS 2009, organisée par équipe COLOSS, Nantes, 2009
- C. Attiogbé : Chair (avec Y. Ait-Ameur) de IM_FMT @ IFM 2009, International Conference on integrated Formal Methods, Dusseldörf, 2009
- H. Henri : Chair de TFM-B'2008 @ JS 2008, Organisation par équipe COLOSS, Nantes, 2008
- C. Attiogbé : Co-Chair (avec D. Kroenig, ETH Zurich) de ProVeCS @ Tools, Zurich, 2007
- C. Attiogbé : Workshop (Atelier) AtlanStic « Variété de la nature des Systèmes et Méthodes Formelles » Nantes 2007 ;
- Séminaires inter-équipes dans le cadre du projet régional Miles 2008, 2009
  Invités : Eric Madelaine (Inria OASIS, Janvier 2009) ; Uwe Assmann (Software Engineering Group, Technische Universität Dresden, juin 2009) ; Radu Mateescu (Inria VASY, novembre 2009).
- Ateliers dans le cadre du projet ECONET, P. André (resp), 2007(1), 2008(2)

Collaborations nationales et internationales
- Universität Halle, Wolf Zimmermann, projet Procope
- NII, Shin Nakajima, co-encadrement d'un Master, travaux autour de Event-B, rédaction d'un article (en soumission),
- LRI Orsay / Université de Evry, Pascal Poizat, co-auteur, article IEEE Trans. Soft. Eng. 2007
- Inria Rhones-Alpes, Grenoble, Gwen Salaün, co-auteur, plusieurs articles dont article IEEE Trans. Soft. Eng. 2007
- Charles University, Equipe DSRG, partenaire de projet, Petr Hnetynka, Frantisek Plasil, Ondrej Sery, co-auteurs

– Cluj University, Dan Chiorean, partenaire de projet, co-auteur
– Equipe VESONTIO (Besançon), partenaire de projet, co-auteurs : Olga Kouchnarenko, Julien Dormoy

Bien que le domaine des spécifications formelles et des méthodes formelles en général soit relativement étendu, avec des "écoles" différentes (algébriques, modèles à états, logiques, preuves, etc) et des motivations différentes (fondements théoriques, langages, méthodes, applications), nos travaux sont en rapport avec ceux des groupes ou équipes préoccupés particulièrement par les approches orientées état ou modèle, le raffinement de spécifications et la vérification par la preuve de propriétés et leurs applications directes sur des cas d'étude. Parmi les équipes thématiquement proches de nous et donc à la fois partenaires de recherches et concurrentes potentielles, nous pouvons citer les équipes ou groupes suivants : ACADIE/IRIT (Toulouse), AMAZONES/CITI (Lyon), DEDALE et MOSEL/LORIA (Nancy), Modélisation et Vérification/LaBRI (Bordeaux), VASCO/LSR-IMAG (Grenoble), Projet VASY/Inria (Grenoble), VESONTIO (Besançon), Vérification de systèmes temporisés/logiques, LSV (Cachan),

Research Group in Formal Methods and Verification (Université Libre de Bruxelles), *Formal Methods Research Group (Teesside)*, *High Integrity Systems Engineering (York)*, *Specification and Analysis of Embedded systems*/CWI (Amsterdam), *Software Engineering and Programming Group* (University of Halles), *Distributed Systems Research Group*/Charles University (Prague), *Software Engineering Laboratory* (Mälardalen University), Groupe de recherche en ingénierie du logiciel (Sherbrooke).

1.9 Formation par la recherche

Pilotage d'écoles doctorales, de spécialités de filières, de master

Participation aux enseignements de master, de filière, d'école doctorale

– **Etablissements tutelles**
  – C. Attiogbé : *Construction formelles de logiciels* (48h en Master 2 Alma Parcours GL, 2007/08, 2008/09, 2009/2010)
  – P. André, C. Attiogbé, H. Habrias : *Génie Logiciel* (2*9 h, Module de spécialisation en Génie Logiciel –MS3, Master Recherche ALD, 2006/07)

HDR et thèses soutenues sur la période

HDR				
Nom	Publications	Institution	Soutenance	Devenir
C. ATTIOGBÉ	[17]	UN	13/09/2007	PR Univ. Nantes

1.10 Gouvernance

Organisation de l'équipe, animation scientifique

Séances de réflexions-discussions collectives Puisque l'effectif de l'équipe le permet, nous fonctionnons sur la base de séances hebdomadaires de réflexions-discussions collectives pour confronter les idées sur les questions et les explorations courantes et élaborer puis répartir des pistes de travail pour les prochaines séances de travail ou les rédactions d'articles.

Séminaires internes Aux séances de réflexions collectives, s'ajoutent des séminaires bihebdomadaires où à tour de rôle les membres de l'équipe présentent un travail (relatif aux dernières lectures, au travail de thèse, préparations et retour de conférences, etc). En guise d'illustration, nous avons effectué/planifié dix-huit (18) séminaires internes au cours en 2009/2010, à raison d'un séminaire par quinzaine, et le passage systématique de tous les membres de l'équipe à tour de rôle.

Stratégies de publication

Dans le but d'assurer un bon impact à nos travaux, nous avons ciblé des conférences internationales de bonne réputation plutôt que l'éparpillement dans de multiples *workshops* à faible impact et relativement coûteux en temps et financièrement. La stratégie pour accroître la pertinence de nos résultats en vue de la sélection des soumissions est l'appui des résultats sur des expériences effectives de développement ou d'analyse formelle (vérification). Cela a été un paramètre constant pour soumettre des résultats convaincants. Nous avons ainsi systématiquement étayé nos résultats par des développements de prototypes propres, ou l'expérimentation et l'interfacage avec des outils externes (par exemple Spin, PVS, Lotos/CADP, Mec, AtelierB/Rodin/ProB, KeY, etc).

Nous privilégions systématiquement les conférences spécifiques ou connexes au domaine des méthodes formelles. En tenant compte du fait que la proposition d'un nouveau modèle/langage de spécification est un travail de longue haleine, nous avons décidé et intégré le principe de la publication progressive des résultats étapes par étapes, avec l'ambition de proposer des travaux de synthèse dans des revues comme des points de synthèse de plusieurs étapes.

A côté des conférences internationales mais francophones comme LMO, CAL, AFADL, où nous avons régulièrement publié des résultats intermédiaires de nos travaux, nous avons visé les conférences internationales comme ICFEM, IFM, ETAPS (FESCA, SC), QSIC, FACS, ABZ où certaines de nos propositions ont été acceptées et publiées au cours du quadrienal ; d'autres conférences généralistes de très bonne réputation dans notre domaine sont par exemple FM, FME, ICSE, ISSRE, ICST, CBSE.

Nous avons concentré les efforts de recherche et de développement sur une des thématiques (spécification formelle et développement de composants corrects) afin de faire émerger rapidement notre modèle à composants dans la communauté. Les activités dans l'autre thématique (intégration de méthodes et analyse multifacette) ont en conséquence progressé plus lentement. Cela explique le fait que tous les membres sont co-auteurs de la plupart des articles. Aujourd'hui, avec l'arrivée d'un nouveau collègue dans l'équipe et la création d'une nouvelle équipe en concertation avec l'équipe MODAL, une nouvelle organisation et une révision de la stratégie de publication s'imposent : par exemple des binômes ou des trinômes pour approfondir et finaliser des jalons et autres filons de nos préoccupations et explorations collectives.

1.11 Auto-évaluation

Bilan des activités Il est à noter que l'écart est insignifiant entre les objectifs que nous avions annoncés au début de ce quadriennal et les résultats présentés dans ce rapport en termes de publications et de développement de prototypes ; cela témoigne de la justesse du fil conducteur qui est de plus, confirmé par les tendances générales de la recherche en méthodes formelles et leurs applications. La recherche et le montage de projets avec des partenaires académiques et industriels a un peu impacté nos lignes directrices sans les compromettre. Néanmoins nous avons eu une plus grande part de développement logiciels que prévus. Nous précisons ci-après des aspects de ce bilan.

Forces Nos activités montrent un équilibre entre activités de recherche fondamentale et les applications. L'équipe fédère des compétences variées en langages, méthodes formelles, composants, multi-formalisme, *theorem-proving, model-checking, testing*. Nos activités sont positionnées dans un domaine de recherche actif avec des enjeux scientifiques majeurs : sûreté des logiciels, analyse multifacette des logiciels hétérogènes, modèles de systèmes répartis, etc. Quelques points qui nous distinguent cependant sont : les compétences pour les modèles globalement asynchrones, localement synchrones (GALS) indispensables pour les grands systèmes réels ; la publication de nos résultats dans des conférences réputées (par exemple ABZ, FACS, ICFEM, SC) ; le développement de prototypes ; la collaboration avec des équipes sur des thématiques connexes au niveau national et international (par exemple INRIA VASY à Grenoble, DSRG à Prague, LRI à Orsay, NII à Tokyo, FMRG à Teesside, VESONTIO à Besançon, MOSEL et DEDALE à Nancy, ACADIE à Toulouse).

Faiblesses La principale faiblesse que nous notons est le manque de financements des institutions (ANR, IST, ...) et de contrats industriels ; cela entraîne le manque de doctorants et de post-doctorants, des stagiaires de Master 2, ou des ingénieurs de développement. Les projets en soumission (ANR, EU) devraient permettre de corriger ce point.
Nos relations internationales méritent aussi d'être étendues et accompagnées de publications communes.

Opportunités Notre domaine de recherche est de nouveau mis en lumière par les dernières distinctions, prix Turing (Sifakis), Chaire collège de France (Berry) ; Cela favorise la communication autour des thématiques et pourrait orienter le fléchage de moyens au niveau des agences de moyens. A l'occasion du montage d'un consortium pour le dépôt d'un projet ANR nous avons procédé à l'ouverture du domaine d'application (vers la domotique, par rapport aux partenaires industriels) de nos propositions. L'arrivée de J-M. Mottu ancien doctorant de Triskell (Irisa, Rennes) est une occasion de renforcement de l'axe Nantes-Rennes, autour des compétences complémentaires en test et IDM (vérifications par tests).

Nous saisissons l'occasion de ce bilan et du nouveau quadriennal pour concrétiser le projet d'une nouvelle équipe sur les Architectures et Logiciels Sûrs (AeLoS) en regroupant les forces des équipes COLOSS et MODAL, autour des thématiques partagées (modèles, services, architecture, sûreté). Nous répondons ainsi aux remarques formulées par les experts –concernant la proximité entre nos équipes autour de la thématique services – lors d'une précédente évaluation. L'équipe ASCOLA du même pôle génie logiciel, développe des activités complémentaires autour de langages, programmation, aspects et composition.

Dans le cadre du nouveau quadriennal, nous présenterons la continuité de nos travaux dans le contexte de cette nouvelle équipe AeLoS.

Risques Dans notre domaine, peu attractif pour une grande partie des industriels, la concurrence nationale et internationale pour l'obtention des moyens est rude entre chercheurs et équipes très visibles ; il y a un risque de ≪famine≫ pour les moyens venant des institutions et des agences de moyens. Pour ce faire nous essayons de développer des alliances avec d'autres équipes parmi nos partenaires et aussi la recherche de partenaires industriels comme nous l'avons fait pour les projets ANR en 2009 et en 2010. Le pari sur la création d'une nouvelle équipe (AeLoS), présente aussi un risque de restriction ou de dispersion des moyens humains et financiers (bourses de thèse, financement des missions) ; en réaction, nous prévoyons une montée en puissance progressive en appui sur les points de convergences identifiées de nos activités actuelles.

1.12 Bibliographie

1.12.1 Publications de référence de l'équipe dans la période

[1] http ://hal.archives-ouvertes.fr/hal-00483585/en/
J.-M. MOTTU, B. BAUDRY, et Y. Le TRAON. Construction de tests qualifiés de transformations de modèles. *Technique et Science Informatiques (TSI)*, 2010, 29 : 537–569

[2] http ://hal.archives-ouvertes.fr/hal-00483755/en/
P. ANDRE, G. ARDOUREL, C. ATTIOGBE, et A. LANOIX. Contract-based Verification of Kmelia Component Assemblies using Event-B. In *8th International Workshop on Formal Engineering approaches to Software Components and Architectures (FESCA @ ETAPS'2010)*, Paphos, Grèce, 2010

[3] http ://hal.archives-ouvertes.fr/hal-00483236/en/
P. ANDRE, G. ARDOUREL, C. ATTIOGBE, et A. LANOIX. Using Event-B to Verify the Kmelia Components and their Assemblies. In *ASM, B, Z International Conference (ABZ'2010)*, Oreford, Canada, volume 5977 of *LNCS*, page 410. Springer, 2010

[4] http ://hal.archives-ouvertes.fr/hal-00420051/en/
C. ATTIOGBE. Can Component/Service-Based Systems Be Proved Correct ? In SPRINGER, réd., *Current Trends in Theory and Practice of Computer Science, (SOFSEM'2009)*, Spindleruv Mlýn, République Tchèque, volume 5404 of *LNCS*, pages 3–18. Springer, 2009

[5] http ://hal.archives-ouvertes.fr/hal-00423658/en/
P. ANDRÉ, C. ATTIOGBÉ, et M. MESSABIHI. Correction d'assemblages de composants impliquant des interfaces paramétrées. In *Conférence Francophone sur les Architectures Logicielles (CAL'2009)*, Nancy, France, volume RNTI-L-4 of *Revue des Nouvelles Technologies de l'Information*, pages 34–44. Cépaduès-Editions, 2009

[6] http ://hal.archives-ouvertes.fr/hal-00457219/en/
P. ANDRÉ, N. ANQUETIL, G. ARDOUREL, J.-C. ROYER, P. HNETYNKA, T. POCH, D. PETRASCU, et V. PETRASCU. JavaCompExt : Extracting Architectural Elements from Java Source Code. In *Working Conference on Reverse Engineering (WCRE' 2009)*, Lille, France, pages 317–318. IEEE, 2009

[7] http ://hal.archives-ouvertes.fr/hal-00420009/en/
C. ATTIOGBÉ. Modelling and Analysing Dynamic Decentralised Systems. In *Pacific-Rim Distributed Computing Conference (PRDC'2009)*, Shanghai, Chine, IEEE Computer Society, pages 109–114, 2009

[8] http ://hal.archives-ouvertes.fr/hal-00483237/en/
C. ATTIOGBE. Semantic Embedding of Petri Nets into Event-B. In *Integration of Model-based Formal Methods Tools (IM_FMT @ IFM'2009)*, Dusseldorf, Allemagne, 2009

[9] http ://hal.archives-ouvertes.fr/hal-00423672/en/
P. ANDRE, G. ARDOUREL, C. ATTIOGBÉ, et A. LANOIX. Using Assertions to Enhance the Correctness of Kmelia Components and their Assemblies. In M. SUN et B. SCHATZ, réds., *Formal Aspects of Component Software (FACS'2009)*, Eindhoven, Pays-Bas, volume SEN-E0902, pages 115–129. CWI, 2009

[10] http ://hal.archives-ouvertes.fr/hal-00423639/en/

P. ANDRE, G. ARDOUREL, et C. ATTIOGBÉ. Composing Components with Shared Services in the Kmelia Model. In Cesare PAUTASSO et Eric TANTER, réds., *7th International Symposium on Software Composition (SC'2008)*, Budapest, Hongrie, volume 4954 of *Lecture Notes in Computer Science*, pages 125–140. Springer, 2008

[11] http ://hal.archives-ouvertes.fr/hal-00420017/en/

J. C. ATTIOGBE. Event-Based Approach to Modeling Dynamic Architecture : Application to Mobile Ad Hoc Network. In *International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'2008)*, Porto-sani, Grèce, volume 17 of *CCIS (Communications in Computer and Information Science)*, pages 769–781. Springer, 2008

[12] http ://hal.archives-ouvertes.fr/hal-00482872/en/

C. ATTIOGBE. Mastering Specification Heterogeneity with Multifacet Analysis. In *Modeling, Validation, and Heterogeneity (MoVaH @ ICST'08)*, Lillehammer, Norvège, 2008

[13] http ://hal.archives-ouvertes.fr/hal-00286431/en/

S. COLIN, A. LANOIX, O. KOUCHNARENKO, et J. SOUQUIÈRES. Using CSP——B Components : Application to a Platoon of Vehicles. In *International Workshop on Formal Methods for Industrial Critical Systems (FMICS'2008)*, Italie, volume 5596 of *LNCS*, pages 103–118. Springer-Verlag, 2008

[14] http ://hal.archives-ouvertes.fr/hal-00423690/en/

P. ANDRE, G. ARDOUREL, et C. ATTIOGBÉ. A Formal Analysis Toolbox for the Kmelia Component Model. In Christian ATTIOGBÉ et Daniel KRÖNING, réds., *ProVeCS 2007 - Satellite Event of TOOLS Europe*, Zürich, Suisse, volume 567 of *ETH TR*, pages 10–25, 2007

[15] http ://hal.archives-ouvertes.fr/hal-00470280/en/

C. ATTIOGBE, P. POIZAT, et G. SALAÜN. A Formal and Tool-Equipped Approach for the Integration of State Diagrams and Formal Datatypes. *IEEE Transactions on Software Engineering*, 2007, 33(3) : 157–170

[16] http ://hal.archives-ouvertes.fr/hal-00423697/en/

P. ANDRE, G. ARDOUREL, et C. ATTIOGBÉ. Adaptation for Hierarchical Components and Services. *Electronic Notes in Theoretical Computer Science*, 2007, 189 : 5–20

[17] http ://tel.archives-ouvertes.fr/tel-00481602/en/

C. ATTIOGBÉ. *Contributions aux approches formelles de développement de logiciels : Intégration de méthodes formelles et analyse multifacette*. Hdr, Université de Nantes, 2007

[18] http ://hal.archives-ouvertes.fr/hal-00397713/en/

P. ANDRE, G. ARDOUREL, et C. ATTIOGBÉ. Defining Component Protocols with Service Composition : Illustration with the Kmelia Model. In Markus LUMPE et Wim VANDERPERREN, réds., *6th International Symposium on Software Composition, (SC'2007)*, Braga, Portugal, volume 4829 of *LNCS*, pages 2–17. Springer Berlin / Heidelberg, 2007

[19] http ://hal.archives-ouvertes.fr/hal-00397694/en/

C. ATTIOGBÉ, P. ANDRÉ, et G. ARDOUREL. Checking Component Composability. In *5th International Symposium on Software Composition*, Vienne, Autriche, volume 4089 of *LNCS*, pages 18–33. Springer Berlin / Heidelberg, 2006

[20] http ://hal.archives-ouvertes.fr/hal-00482855/en/

C. ATTIOGBE. Combining B Tools for Multi-Process Systems Specification. In M. A. E. BADOUEL, Y. SLIMANI, réd., *African Conference on Research in Computer Science (CARI'2006)*, INRIA, pages 35–42, 2006

[21] http ://hal.archives-ouvertes.fr/hal-00420015/en/

J. C. ATTIOGBE. Multi-process Systems Analysis Using Event B : Application to Group Communication Systems. In *International Conference on Formal Engineering Methods (ICFEM'2006)*, Macao, Chine, volume 4260 of *LNCS*, pages 660–677. Springer, 2006

[22] http ://hal.archives-ouvertes.fr/hal-00420050/en/

C. ATTIOGBE. Tool-Assisted Multi-Facet Analysis of Formal Specifications (Using Alelier-B and ProB). In P. KOKOL, réd., *IASTED (SE'2006)*, Innsbruck, Autriche, pages 85–90. Acta Press, 2006

[23] http ://hal.archives-ouvertes.fr/hal-00458119/en/

P. ANDRÉ, G. ARDOUREL, et C. ATTIOGBÉ. Vérification d'assemblage de composants logiciels Expérimentations avec MEC. In *conférence francophone de MOdélisation et SIMulation (MOSIM'2006)*, Rabat, Maroc, pages 497–506. Lavoisier, 2006

1.12.2 Bibliographie externe

[24] Z. LIU, C. MORISSET, et V. STOLZ. rcos : Theory and tool for component-based model driven development. In F. ARBAB et M. SIRJANI, réds., *FSEN*, volume 5961 of *Lecture Notes in Computer Science*, pages 62–80. Springer, 2009. ISBN : 978-3-642-11622-3

[25] S. BLIUDZE et J. SIFAKIS. The algebra of connectors - structuring interaction in bip. *IEEE Trans. Computers*, 2008, 57(10) : 1315–1330

[26] L. CRUZ-FILIPE, A. SERNADAS, et C. SERNADAS. Heterogeneous fibring of deductive systems via abstract proof systems. *Logic Journal of the IGPL*, 2008, 16(2) : 121–153

[27] papers/Basu-Mounier-Poulhies-Pulou-Sifakis-07.pdf

A. BASU, L. MOUNIER, M. POULHIÈS, J. PULOU, et J. SIFAKIS. Using bip for modeling and verification of networked systems – a case study on tinyos-based networks. In *NCA*, pages 257–260, 2007

[28] I. CRNKOVIC. Component-based software engineering for embedded systems. In G.-C. ROMAN, W. G. GRISWOLD, et B. NUSEIBEH, réds., *ICSE*, pages 712–713. ACM, 2005

[29] G. GÖSSLER et J. SIFAKIS. Composition for component-based modeling. *Sci. Comput. Program.*, 2005, 55(1-3) : 161–183

[30] T. MOSSAKOWSKI. Heterogeneous theories and the heterogeneous tool set. In Y. KALFOGLOU, W. M. SCHORLEMMER, A. P. SHETH, S. STAAB, et M. USCHOLD, réds., *Semantic Interoperability and Integration*, volume 04391 of *Dagstuhl Seminar Proceedings*. IBFI, Schloss Dagstuhl, Germany, 2005

[31] C. A. SZYPERSKI. Component technology - what, where, and how ? In *ICSE*, pages 684–693. IEEE Computer Society, 2003

[32] J. EKER, J. W. JANNECK, E. A. LEE, J. LIU, X. LIU, J. LUDVIG, S. NEUENDORFFER, S. SACHS, et Y. XIONG. Taming heterogeneity - the ptolemy approach. *Proceedings of the IEEE*, 2003, 91(1) : 127–144

[33] citeseer.ist.psu.edu/meyer03grand.html

B. MEYER. The Grand Challenge of Trusted Components. In *Proceedings of IEEE International Conference on Software Engineering (ICSE'03)*. IEEE Computer Society Press, 2003

[34] E. A. LEE et A. L. SANGIOVANNI-VINCENTELLI. A framework for comparing models of computation. *IEEE Trans. on CAD of Integrated Circuits and Systems*, 1998, 17(12) : 1217–1229

[35] W.-T. CHANG, S. HA, et E. A. LEE. Heterogeneous simulation - mixing discrete-event models with dataflow. *VLSI Signal Processing*, 1997, 15(1-2) : 127–144

[36] J. T. BUCK, S. HA, E. A. LEE, et D. G. MESSERSCHMITT. Ptolemy : A framework for simulating and prototyping heterogenous systems. *Int. Journal in Computer Simulation*, 1994, 4(2) : 0–

[37] R.-J. BACK. A calculus of refinements for program derivations. *Acta Informatica*, 1988, 25 : 593–624

[38] C. A. R. HOARE. Proof of correctness of data representation. In *Language Hierarchies and Interfaces, International Summer School*, London, UK, pages 183–193. Springer-Verlag, 1976. ISBN : 3-540-07994-7

[39] D. L. PARNAS. "the influence of software structure on reliability". In *Proceedings of the international conference on Reliable software*, New York, NY, USA, pages 358–362. ACM Press, 1975

[40] D. L. PARNAS. On the Criteria To Be Used in Decomposing Systems Into Modules. *Communications of the ACM*, 1972, 15(12) : 1053–1058

[41] N. WIRTH. "program development by stepwise refinement". *Commun. ACM*, 1971, 14(4) : 221–227. ACM Press. ISSN : 0001-0782

[42] E. W. DIJKSTRA. A constructive Approach to the Problem of Program Correctness. *BIT*, 1968, 14(8) : 174–186

[43] J.-R. ABRIAL. *The B Book : Assigning Programs to Meaning*. Cambridge University Press, 1996

[44] R.-J. BACK. *Correctness Preserving Program Refinements : Proof Theory and Applications*, volume 131 of *Mathematical Center Tracts*. Mathematical Centre, Amsterdam, The Netherlands, 1980

[45] E. W. DIJKSTRA. *A Discipline of Programming*. Prentice Hall, Englewoods, Cliffs, NJ, 1976

[46] C. A. R. HOARE et J. HE. *Unifying theories of programming*. Prentice-Hall, NJ, 1998

[47] D. M. HOFFMAN et D. M. WEISS, réds. *"Software fundamentals : collected papers by David L. Parnas"*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001. ISBN : 0-201-70369-6

LINA, Université de Nantes – 2, rue de la Houssinière – BP 92208 – 44322 NANTES CEDEX 3
Tél. : 02 51 12 58 17 – Fax. : 02 51 12 58 97 – http://www.lina.univ-nantes.fr/