Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Attention,
toute proposition doit faire l'objet d'un résumé enregistré
avant le 28 mars 2003
directement sur le site web de l'ACI :
http://aciSI.loria.fr

Chaque dossier doit être

- déposé avant le 04 avril 2003 sur le site web de l'ACI[1]:

http://aciSI.loria.fr

- envoyé par voie postale avec les signatures requises
avant le 11 avril 2003
(cachet de la poste faisant foi)
à

Ministère délégué à la Recherche et aux Nouvelles Technologies
Direction de la Recherche
Cellule ACI
ACI Sécurité Informatique
1, rue Descartes
75231 Paris cedex 05

[1] En cas de difficulté, une soumission par courrier électronique est possible à l'adresse aciSI@loria.fr

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

I - FICHE D'IDENTITE DU PROJET

Nom du Projet : *(maximum 20 caractères)*

ROOF

Titre du Projet : *(maximum 3 lignes)*

Elaboration d'un modèle unifié pour améliorer la sûreté de fonctionnement (correction, robustesse et intégrité du code) des plates-formes de composants logiciels.

Type du Projet[2]:

Projet de recherche	Projet de recherche multi-thématiques	Projet de recherche avec infrastructure	Autre
X			

Durée du projet[3] : 36 mois

Description courte du Projet : *(une demi-page maximum)*

La sûreté de fonctionnement d'une application, terme qui englobe les problématiques de correction, de robustesse et d'intégrité du code et des données, est liée à la notion plus générale de sécurité informatique.
Ces problèmes liés la sûreté ont parfois été largement étudiés mais souvent de façon séparée ; ils doivent de plus être complètement reconsidérés si l'on se soucie des dernières avancées en matière d'architecture des applications, et de pratique de développement, dont en particulier la modélisation et l'utilisation de composants. On ne trouve actuellement aucune approche unificatrice, aucun modèle dans lequel il soit possible de spécifier, de développer et d'assembler des composants en prenant en compte de façon conjointe les aspects liés à leur correction, leur robustesse et leur intégrité.
De plus, les solutions actuelles aux problèmes précédemment cités sont souvent proposées dans le cadre spécifique d'une technologie de composants particulière et ne sont souvent applicables qu'à bas niveau. Elles permettent rarement aux architectes logiciels d'exprimer, relativement à la sûreté, des contraintes plus abstraites dans les étapes amont du cycle de vie.

Notre proposition, s'articule autour de trois objectifs. Nous souhaitons en premier lieu proposer un modèle de composants logiciels intégrant des solutions, compatibles entre elles, pour les problèmes de correction, de robustesse et d'intégrité. Ce modèle devra être indépendant d'une technologie spécifique mais devra par contre permettre la production de code compatible avec ces mêmes technologies. Nous souhaitons ainsi respecter l'approche MDA (« Model Driven Architecture ») en proposant un modèle de type PIM (« Platform-Independent Model ») et en envisageant sa projection vers des PSM (« Platform-Specific Model »).
Le caractère nécessairement re-configurable des applications actuelles, de plus en plus intégrées dans nos outils quotidiens, nous impose d'inclure comme deuxième objectif, l'étude de la possibilité de gestion et de reconfiguration dynamique des contrôles relatifs à la sécurité (sans exclure définitivement toute analyse statique qui resterait compatible avec cette préoccupation).
Enfin, nous souhaitons permettre l'équipement incrémental des composants d'une application par ajout de nouvelles facettes de sécurité : notre modèle devra donc être extensible tant au niveau des propriétés des composants qu'à celui des contrôles et des traitements qui leurs sont associés.

Notre proposition intègre un ensemble de partenaires ayant des compétences complémentaires (contrats, tests, exceptions, mécanismes d'accès, séparation des préoccupations, points de vue et rôles, composants), ayant parfois déjà collaboré et travaillant dans le contexte unificateur du développement à base de composants logiciels. Elle vise, via une approche tant méthodologique que pragmatique, à contribuer notablement au développement de systèmes à composants sûrs.

[2] Cocher la case correspondante au type du projet soumis.
[3] La durée d'un projet ne peut excéder 36 mois. Des demandes de projets d'une durée plus courte devront être particulièrement argumentées.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Coordinateur du projet

Nom	Prénom	Laboratoire (sigle éventuel et nom complet)
Parigot	Didier	INRIA Sophia Antipolis

Organisme de rattachement financier pour le présent projet

INRIA - Sophia Antipolis

Equipes ou laboratoires partenaires (nom complet et éventuellement sigle)[4]

INRIA Sophia – Antipolis – Projet OASIS-SmartTools
I3S – Université de Nice – Sophia Antipolis / CNRS – Equipe OCL
LGI2P – Ecole des Mines d'Alès – Thème Modélisation orientée objet
LIRMM – Université de Montpellier II
LIRIS – INSA Lyon – Equipe Systèmes d'information communicants
LSR-IMAG – Equipe SIGMA
VALORIA – Université de Bretagne Sud – Equipe Composants

[4] Insérer autant de lignes que nécessaire.

II - PRESENTATION DETAILLEE DU PROJET

A-IDENTIFICATION DU COORDINATEUR ET DES AUTRES PARTENAIRES DU PROJET :

A1- Coordinateur du Projet :
Un unique coordinateur doit être désigné par les partenaires.

M. ou Mme. Prénom Nom[5]	M. Didier Parigot
Fonction[5]	Chargé de recherche
Laboratoire (Nom complet et sigle le cas échéant)[5]	INRIA Sophia Antipolis – Institut National de la Recherche en Informatique Appliquée.
Adresse[5]	I.N.R.I.A. Sophia Antipolis, 2004 Route des Lucioles , BP 93 06902 Sophia Antipolis Cedex FRANCE
Téléphone[5]	04 92 38 50 01
Fax	04 92 38 79 44
Mél[5]	Didier.Parigot@inria.fr

[5] Champ obligatoire

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

A2- Equipes ou laboratoires partenaires du Projet [6]:

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	INRIA Sophia Antipolis – Institut National de la Recherche en Informatique Appliquée.
Adresse	I.N.R.I.A. Sophia Antipolis, 2004 Route des Lucioles , BP 93 06902 Sophia Antipolis Cedex FRANCE

Organisme de rattachement financier de l'équipe pour le présent projet

INRIA Sophia Antipolis

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	M. Didier Parigot
Fonction	Chargé de recherches
Téléphone	04 92 38 50 01
Fax	04 92 38 79 44
Mél	Didier.Parigot@inria.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Parigot	Didier	Chargé de recherche	40%

Références :
Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Didier Parigot

- Carine Courbis, Pascal Degenne, Alexandre Fau, Didier Parigot, and Joseph Variamparambil. Un modèle de composants pour l'atelier de développement SmartTools. In *Systèmes à composants adaptables et extensibles*, Octobre 2002

- Carine Courbis, Pascal Degenne, Alexandre Fau, and Didier Parigot. L'apport des technologies XML et Objets pour un générateur d'environnements : SmartTools. accepté à la revue Objet

- Isabelle Attali, Carine Courbis, Pascal Degenne, Alexandre Fau, Joel Fillon, Christophe Held, Didier Parigot, and Claude Pasquier. Aspect and XML-oriented Semantic Framework Generator SmartTools. In *Second Workshop on Language Descriptions, Tools and Applications, LDTA'02*. ETAPS'2002, Electronic

[6] Une fiche doit être remplie pour chaque laboratoire ou équipe partenaire

Notes in Theoretical Computer Science (ENTCS), 2002.

- Isabelle Attali, Carine Courbis, Pascal Degenne, Alexandre Fau, Didier Parigot, and Claude Pasquier. SmartTools: a Generator of Interactive Environments Tools. In Reinhard Wilhelm, editor, *International Conference on Compiler Construction CC'01*, volume 2027 of *Lect. Notes in Comp. Sci.*, Genova, Italy, April 2001. ETAPS'2001, Electronic Notes in Theoretical Computer Science (ENTCS). Tools Demonstrations at CC'01.

- Isabelle Attali, Carine Courbis, Pascal Degenne, Alexandre Fau, Joël Fillon, Didier Parigot, Claude Pasquier, and Claudio Sacerdoti Coen. SmartTools: a development environment generator based on XML technologies. In *XML Technologies and Software Engineering*, Toronto, Canada, 2001. ICSE'2001, ICSE workshop proceedings

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	Laboratoire I3S / UNSA -- Equipe OCL (Objets et Composants Logiciels)
Adresse	Laboratoire Informatique Signaux et Systèmes de Sophia Antipolis UMR 6070 du C.N.R.S. Les Algorithmes/Bâbtiment Euclide 2000 route des Lucioles, BP 121 06903 Sophia-Antipolis Cedex - France

Organisme de rattachement financier de l'équipe pour le présent projet

Centre National de la Recherche Scientifique (délégation régionale Côte d'Azur)

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	M. Philippe Lahire
Fonction	Maître de Conférences
Téléphone	04 92 94 27 51
Fax	04 92 94 28 96
Mél	Philippe.Lahire@unice.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Philippe	Collet	Maître de Conférences	30%
Pierre	Crescenzo	Maître de Conférences	25%
Philippe	Lahire	Maître de Conférences	40%
Roger	Rousseau	Maître de Conférences	25%

Références :
Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Philippe Lahire & Pierre Crescenzo :

- Gilles Ardourel, Pierre Crescenzo & Philippe Lahire. LAMP: vers un langage de définition de mécanismes de protection pour les langages de programmation à objets . LMO'2003, conférence nationale sur les Langages et Modèles à Objets. Publié dans la revue L'objet : logiciels, bases de données, réseaux, volume X, numéro 1-2/2003 ; Jean-Pierre Briot et Jacques Malenfant. Editions Hermès Science Publications, janvier 2003, 13 pages, Vannes, France.

- Adeline Capouillez, Pierre Crescenzo & Philippe Lahire. Le modèle OFL au service du métaprogrammeur - Application à Java. LMO'2002, conférence nationale sur les Langages et Modèles à Objets. Publié dans la revue L'objet : logiciels, bases de données, réseaux, volume 8, numéro 1-2/2002 ; Michel Dao et Marianne Huchard ; ISSN : 1262-1137 ; ISBN : 2-7462-0403-7. Editions Hermès Science Publications, janvier 2002, 14 pages, Montpellier, France.

- Adeline Capouillez, Robert Chignoli, Pierre Crescenzo & Philippe Lahire. Hyper-généricité pour les langages à objets : le modèle OFL. LMO 2001, conférence nationale sur les Langages et Modèles à

Objets. Publié dans la revue L'objet : logiciels, bases de données, réseaux, volume 7, numéro 1-2/2001 ; Robert Godin et Isabelle Borne ; ISSN : 1262-1137 ; ISBN : 2-7462-0211-5 ; éditions Hermès Science Publications, janvier 2001, 13 pages, Le Croisic, France.

- Pierre Crescenzo & Philippe Lahire. Using both Specialisation and Generalisation in a Programming Language: Why and How? Dans workshop « Managing Specialization/Generalization Hierarchies » de la conférence OOIS 2002 (8ème conférence internationale sur « Object-Oriented Information Systems ». Springer Verlag, LNCS series, septembre 2002, 10 pages, Montpellier, France. Le rapport de recherche I3S/RR--2002-19--FR est une version longue de cet article.

- Pierre Crescenzo & Philippe Lahire. Customisation of Inheritance Dans workshop « The Inheritance » de la conférence ECOOP 2002 (16th European Conference on Object-Oriented Programming). Actes de « the Inheritance Workshop at ECOOP 2002 » ; Andrew P. Black, Erick Ernst, Peter Grogono et Markku Sakkinen ; ISSN : 1236-1615 ; ISBN : 951-39-1252-3 ; University of Jyväskylä, Finlande, et synthèse (Springer Verlag, LNCS series), juin 2002, 7 pages, Malaga, Espagne.

Philippe Collet & Roger Rousseau :

- Philippe Collet & Roger Rousseau " Contrôle d'admission de composants avec des contrats comportementaux " LMO'2003, Vannes (France), 3-5 février 2003. In RSTI L'objet, Vol. 9 / LMO 2003, p. 31-44, Jan. 2003, Hermes Science pub.

- Philippe Collet ``Functional and Non-Functional Contracts Support for Component-Oriented Programming" First OOPSLA Workshop on Language Mechanisms for Programming Software Components, OOPSLA'2001, October 15, 2001, Tampa Bay (Florida).

- Philippe Collet ``On Contract Monitoring for the Verification of Component-Based Systems" OOPSLA Workshop on Specification and Verification of Component-Based Systems, OOPSLA'2001, October 14, 2001, Tampa Bay (Florida).

- Philippe Collet " Fiabilité des systèmes à objets persistants : les assertions persistent " LMO'2001, Le Croisic (France), 29-31 Janvier 2001. In L'objet, Vol. 7 No 1-2, p. 115-130, Jan. 2001, Hermes Science pub.

- Philippe Collet & Roger Rousseau ``Efficient Implementation Techniques for Advanced Assertion Languages" In L'objet, Vol. 5 No 3-4, p. 417-442, Dec. 1999, Hermes Science pub.

- Pascal André & Roger Rousseau (Eds) « Méthodes formelles pour les objets », numéro spécial de la revue L'Objet, vol 6, n°1, Hermes Science Pub., Janv. 2000.

- Philippe Brissi & Roger Rousseau « IREC: an object-oriented abstract representation to handle software components in a persistent Framework », In Alagar V.S & Missaoui R. (Eds), Object-Oriented Technology for Database and Software Systems, World Scientific Publishing, Singapore, 1995, pp 6-21.

- G. Castagna, R. Rousseau et J.-C. Royer « Fiabilité des programmes : le typage est-il suffisant ? », L'Objet, vol 4 n°1, avril 1998, Hermes Sciences Pub., pp 89-95

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	LGI2P - Laboratoire de génie informatique et d'ingénierie de production
Adresse	LGI2P - École des Mines d'Alès - Site EERIE Parc Scientifique Georges Besse F 30035 Nîmes Cedex 1

Organisme de rattachement financier de l'équipe pour le présent projet

ARMINES

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Christelle Urtado
Fonction	Maître-assistant
Téléphone	04 66 38 70 30
Fax	04 66 38 70 74
Mél	Christelle.Urtado@site-eerie.ema.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Vauttier	Sylvain	Maître assistant	15%
Urtado	Christelle	Maître assistant	15%

Références :

Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Christophe Dony, Christelle Urtado, Sylvain Vauttier

- Frédéric Souchon, Christophe Dony, Christelle Urtado, Sylvain Vauttier. A proposition for exception handling in multi-agent systems. To appear in the proceedings of the 2nd International Workshop on Software Engineering for Large-Scale Multi-Agent Systems, Mai 2003.

Christelle Urtado, Sylvain Vauttier

- C. Urtado and C. Oussalah. Complex entity versioning at two granularity levels, Information Systems, 23(2/3):197-216, Pergamon, Elsevier Science, 1998.
- S. Vauttier, M. Magnan et C. Oussalah. Extended Specification of Composite Objects in UML, Journal of Object-Oriented Programming, May 1999.
- S. Vauttier and C. Urtado. Improving statechart composition and reuse in UML. In Proceedings of the NîmesTIC 2000 Conference, pages 287-296, Nîmes, France, September 2000.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	LIRIS : Laboratoire d'Informatique en Images et Systèmes d'Information. FRE 2672
Adresse	LIRIS, INSA, Campus de la Doua, Bâtiment Blaise Pascal (501), 20 avenue Albert Einstein, 69621 VILLEURBANNE CEDEX

Organisme de rattachement financier de l'équipe pour le présent projet

INSA de Lyon

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Stéphane Coulondre
Fonction	Maître de Conférences, INSA de Lyon
Téléphone	04 72 43 85 88
Fax	04 72 43 87 13
Mél	Stephane.Coulondre@insa-lyon.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Coulondre	Stéphane	Maître de Conférences	15%

Références :
Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Les publications sont citées dans la fiche du laboratoire LIRMM

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	LIRMM : Laboratoire d'informatique, de Robotique et de Microélectronique de Montpellier. UMR 5506
Adresse	LIRMM; 161 rue Ada, 34392 Montpellier Cedex 5

Organisme de rattachement financier de l'équipe pour le présent projet

Centre National de la Recherche Scientifique (délégation régionale Languedoc-Roussillon)

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	Christophe Dony
Fonction	Professeur
Téléphone	04 67 41 85 33
Fax	04 67 41 85 00
Mél	dony@lirmm.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Ahronovitz	Yolande	Maître de Conférences	25%
Dony	Christophe	Professeur	33%
Huchard	Marianne	Maître de Conférences	15%
Libourel	Thérèse	Maître de Conférences	15%

Références :
Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Gilles Ardourel et Marianne Huchard

- G. Ardourel, M. Huchard. Access Graphs: Another View on Static Access Control for a Better Understanding and Use, « Journal of Object Technologies » nov/dec 2002 (voir http://www.jot.fm/issues/issue_2002_09/)

- G. Ardourel, M. Huchard. AGATE: Access Graph bAsed Tools handling Encapsulation in proceedings of IEEE International conference on Automated Software Engineering, (ASE'2001), pp 311-314, San Diego, USA, November 26-29, 2001.

- Olivier Goût, G. Ardourel, M. Huchard. Access Graph Visualization: A step Towards betterunderstanding of static access control. GraBaTs 2002, Barcelona, Spain, October 7 - 8, 2002, Tom Mens, Andy Schürr, Gabriele Taentzer (Eds) Electronic Notes in Theoretical Computer Science, 72(2), Elsevier Science B. V. http://www.elsevier.nl/locate/entcs/volume72.html

- G.Ardourel, M. Huchard. Synthèse et modélisation des accès dans les langages à classes :vers une formalisation des systèmes de protection. Actes de Langages et modèles à objets (LMO2001), Le Croisic, Herms, L'OBJET vol.7, pages 149-164.

Christophe Dony, Christelle Urtado, Sylvain Vauttier

- Frédéric Souchon, Christophe Dony, Christelle Urtado, Sylvain Vauttier. A proposition for exception handling in multi-agent systems. To appear in the proceedings of the 2nd International Workshop on Software Engineering for Large-Scale Multi-Agent Systems, Mai 2003.

- Alexander. Romanovsky, Christophe. Dony, Jorgen. L. Knudsen, Anand Tripathi, editor.Advances in Exception Handling Techniques, LNCS No 2022. Springer-Verlag, Février 2001.

- C. Dony. A fully object-oriented exception handling system: rationale and Smalltalk implementation., In Advances in Exception Handling Techniques, LNCS 2022, pp. 18-38, 2001.

- A. Romanovsky, C. Dony, J. L. Knudsen, A. Tripathi. Exception handling in object oriented systems. In A. Moreira. J. Malenfant, S. Moisan, editor, Object-Oriented Technology. ECOOP 2000 Workshop Reader. LNCS-1964. 2000.

- Daniel Bardou and Christophe Dony. Split objects: a disciplined use of delegation within objects. Special issue of Sigplan Notice - Actes de ACM OOPSLA'96, 31(10):122-137, October 1996.

Yolande Ahronovitz et Marianne Huchard

- Y. Ahronovitz, M. Huchard. Exceptions in Object Modeling: Finding Exceptions from the Elements of the Static Object Model. In A. Romanovsky, C. Dony, J. L. Knudsen, A. Tripathi (Eds). Advances in Exception Handling Techniques. Springer-Verlag, LNCS-2022 (2001,) pp. 77-93.

- Y. Ahronovitz, M. Huchard. Exceptions in Object Modeling: Questions from an educational experience. ECOOP'00: Workshop « Exception Handling in Object Oriented Systems », Cannes, 12-16 june 2000, France. http://www.cs.ncl.ac.uk/people/alexander.romanovsky/home.formal/ehoos.html

Stéphane Coulondre et Thérèse Libourel

- Stéphane Coulondre et Thérèse Libourel.Towards a New Role Paradigm for OO Modeling. MASPEGHI Workshop (MAnaging of SPEcialization/Generalization Hierarchies), Lecture Notes in Computer Science n°2426, p. 44-52

- Stéphane Coulondre et Thérèse Libourel, « An Integrated Object-Role Oriented Database Model », Revue Data & Knowledge Engineering, Vol 42(1), pp. 113-141, 2002, Elsevier Science

- Stéphane Coulondre et Thérèse Libourel, « Modèle à rôles pour objets variables persistants » 16ème Journées Bases de Données Avancées, Blois, France, 24-27 Octobre 2000, pp. 139-158.

- Stéphane Coulondre et Thérèse Libourel, Viewpoints handling in an object model with criterium-based classes, DEXA'99 : 10th International Conference on Database and Expert Systems Applications (LNCS: 1677), Florence, Italy, August 30-September 3, 1999, pp. 573-582.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	LSR-IMAG (Logiciels, Systèmes, Réseaux - Institut d'Informatique et Mathématiques Appliquées de Grenoble - CNRS/INPG/UJF - UMR 5526), Equipe SIGMA
Adresse	Laboratoire LSR-IMAG ENSIMAG – Bâtiment D - 681, rue de la passerelle Domaine Universitaire de Saint Martin D'Hères - BP 72 38042 Saint Martin d'Hères Cedex 9, France

Organisme de rattachement financier de l'équipe pour le présent projet

CNRS (Délégation CNRS Rhône-Alpes)

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	M. Daniel Bardou
Fonction	Maître de Conférences
Téléphone	04 76 82 72 07
Fax	04 76 82 72 87
Mél	Daniel.Bardou@imag.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Bardou	Daniel	Maître de Conférences	40%
Rieu	Dominique	Professeur	20%
Conte	Agnès	Maître de Conférences	15%

Références :
Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Daniel Bardou :

- Daniel Bardou. Towards a Platform for Experimenting with Split Objects in Java and AspectJ. *AOSD-GI 2003, Proceedings of the 3rd German Workshop on Aspect-Oriented Software Development*, Technical report, March, 2003, Essen, Germany, p. 51-56.

- Daniel Bardou. Roles, Subjects and Aspects: How do they relate? Position paper at the *Aspect Oriented Programming Workshop. 12th European Conference on Object-Oriented Programming (ECOOP '98), Brussels, Belgium*, july 1998. Extended abstract published in *ECOOP '98 Workshop Reader*, Serge Demeyer and Jan Bosch, editors, Lecture Notes in Computer Science (LNCS), vol. 1543, Springer, 418-419, December 1998.

- Daniel Bardou. *Étude des langages à prototypes, du mécanisme de délégation, et de son rapport à la notion de point de vue.* Thèse de Doctorat, spécialité Informatique, Université Montpellier II, 260 pages, avril 1998.

- Daniel Bardou and Christophe Dony. Split Objects: a Disciplined Use of Delegation within Objects. *Proceedings of the 11th Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA '96), San Jose, California, USA.* ACM SIGPLAN Notices (31)10, pages 122-137, october 1996.

Dominique Rieu :

- Ibtissem Hassine, Dominique Rieu, Fethi Bounaas et Omar Seghrouchni. Symphony : Un modèle conceptuel de composants métier. Revue ISI (Ingénierie des Systèmes d'Information), numéro spécial Connaissances métier dans l'Ingénierie des Systèmes d'Information, vol. 7, n° 4, Hermès, 2002.

- Ibtissem Hassine, Dominique Rieu, Fethi Bounaas and Omar Seghrouchni. Symphony : a Conceptual Model based on business Component. IEEE International Conference on Systems, Man and Cybernetics (IEEE SMC), Hammamet, Tunisia, october 2002.

Agnès Conte :

- Catherine Berrut et Agnès Front-Conte. Patterns Retrieval System: a first attempt. 5th International Conference on Applications of Natural Language to Information Systems (NLDB'2000), Versailles, Juin 2000.

Dominique Rieu et Agnès Conte :

- Corine Cauvet, Dominique Rieu, Agnès Front-Conte et Philippe Ramadour. Réutilisation dans l'ingénierie des SI. Chap. 5 dans Ingénierie des SI, Hermès, pages 115-147, 2001.

- Agnès Conte, Mounia Fredj, Ibtissem Hassine, Jean-Pierre Giraudin and Dominique Rieu. A tool and a formalism to design and apply patterns. Proceedings of the 8th International Conference on Object-Oriented Information Systems(OOIS 2002), Montpellier, France. LNCS, Vol. 2425, Springer, September 2002, pages 135-146.

Daniel Bardou et Agnès Conte :

- Daniel Bardou, Agnès Conte et Elizabeth Kendall. Réutilisation dans l'ingénierie des SI. Chap. 5 dans Ingénierie des SI, Hermès, pages 115-147, 2001.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Identification de l'équipe ou du laboratoire

Equipe ou Laboratoire	**Laboratoire Valoria (EA n°2593) - Equipe Composants - Université de Bretagne Sud – Vannes**
Adresse	*Centre de Recherche Yves Coppens* *Campus de Tohannic* *56000 - Vannes – FRANCE*

Organisme de rattachement financier de l'équipe pour le présent projet

Université de Bretagne Sud – Vannes

Responsable du projet au sein de l'équipe ou du laboratoire

M. ou Mme. Prénom Nom	M. Daniel Deveaux
Fonction	Maître de Conférences HC
Téléphone	+33 297 463 175/017 241/010167
Fax	+33 297 634 722
Mél	daniel.deveaux@univ-ubs.fr

Autres membres de l'équipe participant au projet

Nom	Prénom	Poste statutaire	% du temps de recherche consacré au projet
Borne	Isabelle	Professeur	40%
Deveaux	Daniel	Maître de Conférences	40%

Références :

Pour chaque (enseignant-)chercheur participant, liste de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Isabelle Borne

- E.Pulvermueller, I.Borne, N.Bouraqadi, P.Cointe, U.Assmann. Software Composition Workshop. in *ETAPS, Grenoble, April 7 2002*. Electronic Notes in Theoretical Computer Science (ENTCS), Volume 65, Issue 4, http://www.elsevier.nl/locate/entcs.

- G.Arevalo, I.Borne. Architectural Description of Object-Oriented Framework : an Approach. In *Actes de la conférence Langage et Modèles à objets (LMO 2001)*, revue l'Objet, Vol. 7, pp.183-198.

- I.Borne, G.H.Galal, H.Evans, L.Landrade. 2nd workshop on Object-Oriented Architectural Evolution, in *ECOOP 2000 Workshop Reader*, J.Malenfant, S.Moisan (eds), Springer LNCS 1964, pp.138-149. 2002 - E.Pulvermueller, I.Borne, N.Bouraqadi, P.Cointe, U.Assmann. Software Composition Workshop. in *ETAPS, Grenoble, April 7 2002*. Electronic Notes in Theoretical Computer Science (ENTCS), Volume 65, Issue 4, http://www.elsevier.nl/locate/entcs.

Daniel Deveaux

- D. Deveaux. The Design for Trustability Approach. In *Trusted Components workshop* organized by ETH Zürich, Monash University and TOOLS Conferences - Prato (near Florence, Italy) 01/2003. - (PDF).

- D. Deveaux, J.-F. Le Cam and A. Despland. Software Components Development and Follow-up: the « Design for Trustability » (DfT) Approach. In *Proceedings of the information system technology panel symposium*. Bonn (Germany), 9/2002. Research and Technology Agency (NATO). - (PDF).

- J.-M. Jézéquel, D. Deveaux and Y. Le Traon. Reliable Objects: Lightweight Testing for 00 Languages. *IEEE-Software*, 18(4):76-83, 2001. (PDF).

- D. Deveaux, P. Frison and J.-M. Jézéquel. Increase Software Trustability with Self-Testable Components in Java. In D. D. Grant and L. Sterling, editors, *Proceedings 2001 australian sofware engineering conference*, pages 3-11. Canberra - Australia, 8/2001. ASWEC'2001, IEEE Computer Society. (PDF).

- Deveaux and Y. Le Traon. XML to Manage Source Code Engineering in Object-Oriented Development: an Example. In C. Mascolo, W. Emmerich and A. Finkelstein, editors, *Xml technologies and software engineering*, pages 28-31. Toronto, Canada, 5/2001. XSE01 workshop at ICSE'2001. (PDF).

B - DESCRIPTION DU PROJET

B1 – Objectifs et contexte :

On précisera, en particulier, les verrous scientifiques et technologiques à dépasser, l'état de l'art ainsi que les projets concurrents ou similaires connus dans le contexte national et international, en particulier ceux auxquels les équipes du projet participent.

Nous proposons une étude globale de la sécurité informatique selon le point de vue de la sûreté de fonctionnement et dans le contexte novateur défini par les points suivants :

- Les applications de demain s'appuieront de plus en plus sur l'assemblage de composants logiciels disponibles " sur étagères "; composables, assemblables ou utilisables à distance.
- Notre démarche s'inscrit dans une approche MDA. Les composants seront de façon générale conçus par des tiers. Il est nécessaire de concevoir les applications à un haut niveau d'abstraction et sans faire, autant que possible, d'hypothèses sur les langages utilisés.
- On attend des applications aujourd'hui, de plus en plus intégrées dans la vie quotidienne, qu'elles soient sûres mais aussi réparables, configurables et adaptables dynamiquement. Il est donc important de proposer des mécanismes simples et puissants de contrôle statique aussi bien que dynamique.

Sûreté de fonctionnement

La sécurité informatique au sens large du terme peut se décliner selon différents points de vue et nous l'aborderons dans cette proposition sous celui de la " sûreté de fonctionnement des applications logicielles ". Trois grandes problématiques relèvent selon nous de la sûreté : la correction, la robustesse et le respect de l'intégrité des programmes. Les équipes participant à cette proposition disposent d'un savoir-faire et d'une expérience importante dans le cadre du développement par objets d'applications sûres au sens précédent ; nous souhaitons étendre cette compétence au contexte nouveau de la méta-modélisation à base de composants.

- *Correction* : la correction d'un composant logiciel et par extension d'une application est définie par sa conformité avec sa spécification. Cette propriété peut être assurée par une approche contractuelle, en considérant des contrats fonctionnels et non fonctionnels. Ces contrats peuvent être exprimés à l'aide d'un ensemble de sortes d'assertions.
- *Robustesse* : La robustesse d'un système de composants est sa capacité à ne pas interrompre son exécution de manière inopinée, en particulier lorsqu'une situation exceptionnelle survient. La robustesse s'obtient en spécifiant, à l'aide de systèmes de gestion des exceptions, des continuations appropriés pour toutes les situations exceptionnelles possibles.
- *Intégrité du code et des données* : L'intégrité est relative à la capacité de protéger un composant de ceux qui souhaitent l'utiliser. Le respect de l'intégrité suppose d'une part que puisse être spécifié tout ce qui est accessible dans un composant, à qui et dans quel contexte, et d'autre part, que l'on puisse s'assurer que ces spécifications seront respectées à l'exécution.

D'autres points de vue sur la sécurité informatique relatifs à l'authentification, la cryptologie ou le chiffrement devront être pris en compte par la solution générale que nous proposerons mais ils ne feront pas l'objet d'études particulières dans cette proposition.

Principales caractéristiques de l'approche proposée

Notre objectif est de spécifier un modèle unifié et abstrait de composants adaptables sûrs, et de projeter cette spécification dans divers contextes concrets. Nous souhaitons premièrement étudier point par point, dans le contexte de la définition d'un modèle abstrait minimal de composants, chacune des problématiques précédentes relative à la sûreté de fonctionnement et ainsi produire un ensemble de spécifications pour la correction, la robustesse et l'intégrité.
Nous étudierons ensuite une solution globale qui permette d'unifier les spécifications précédentes. Ces spécifications pourront être exprimées dans des environnements de modélisation reconnus comme des standard

(par exemple UML, MOF), ou à l'aide de modèles spécialisés exprimés en XML qui se prêtent aux transformations spécifiques aux facettes de la sûreté.

La dernière partie du travail sera consacrée à l'étude de la projection du modèle global vers des plates-formes à composants existants, éventuellement en restreignent notre proposition. Elle pourra être mise en œuvre via des générateurs de langages et d'environnements tels que SmartTools.

Un aspect important de notre approche, déjà évoqué plus haut, est la volonté de pouvoir spécifier la politique de sécurité d'une application au plus tôt dans le cycle de vie. C'est en ce sens que nos propositions doivent être établies de manière la plus indépendante possible d'une technologie particulière. Néanmoins il est nécessaires que les parties des spécifications qui ne pourront pas être décrites indépendamment d'une plate-forme cible puisse être intégrées au moment d'une projection particulière.

Compte tenu de notre savoir-faire et pour faciliter l'intégration des résultats nous nous appuierons largement sur une modélisation contractuelle et nous nous intéresserons aux approches par séparation des préoccupations et aux approches de transformation de modèles. Au niveau du déploiement, nos propositions pourront se traduire par des outils d'analyse statique sur le modèle ou le code des composants, des instrumentations de code source et des frameworks d'exécution (middleware par exemple) pour supporter les évaluations dynamiques et/ou des générations d'environnements de test et de contrôle d'exécution.

Positionnement du projet

La question de la sûreté de fonctionnement des logiciels construits sur des composants à objets peut apparaître comme marginale dans le thème global de la sécurité informatique, mais c'est en fait un point central : la majorité des solutions de sécurité sont de moindre valeur si elles ne s'appuient pas sur une garantie de correction et de robustesse du code d'implantation. On peut constater en effet que la majorité des problèmes de sécurité identifiés sur le *web* (pertes de données, accès non autorisés, déni de service, *etc.*) sont en fait liés à des défaillances fonctionnelles des logiciels sous-jacents.

Le projet ROOF est une démarche pluridisciplinaire qui propose de faire coopérer des champs de recherche habituellement disjoints :

- sémantique et programmation par objets,
- applications à base de composants,
- programmation contractuelle et tests objet,
- techniques de modélisation et de transformation de modèles

Dans chacun de ces domaines travaillent de nombreuses équipes françaises et européennes et plusieurs projets soutenus par les réseaux français (RNTL) et européens (IST, ITEA) sont en cours. Cependant la majorité de ces recherches vise à une extension des fonctionnalités ou de l'efficacité en n'abordant que très peu les aspects de sécurité ; quand ces aspects sont abordés, le plus souvent un seul point de vue est pris en compte. Durant ses travaux, le groupe ROOF suivra avec attention les travaux et prendra en compte les résultats des équipes et projets qui travaillent dans les domaines connexes ; citons notamment :

- Projet INRIA *Obasco*: Machine abstraite pour les composants (EMN) ;
- Projet INRIA *Sardes*: Modèle pour la programmation distribuée (INRIA Rhône-Alpes – LSR-IMAG) ;
- Projet INRIA *Triskell* : Approche MDA et applications temps réel (IRISA) ;
- Projet INRIA *Lande* : Conception et validation de logiciels (IRISA) ;
- Consortium *ObjectWeb avec OpenCC* et la programmation par aspect pour les composants (LIFL) ;
- Projet RNTL *ARCAD* : Architecture répartie extensible pour composants adaptables ;
- Projet RNTL *COTE* : Test de composants ;
- Projet RNTL *DANOCOPS* : détection des non-conformités aux spécifications en utilisant les techniques de programmation par contraintes (LSR-IMAG)
- Projet RNTL *OADymPPaC* : Outils pour l'Analyse Dynamique et la mise au Point de Programmes avec Contraintes ;
- Projet IST *QCCS* : Quality Controlled Components-based Software development.

En outre, les équipes qui participent au consortium ont actuellement en cours des contrats de recherche dont les résultats vont contribuer directement à l'action ROOF :

- Projet RNTL *MACAO* : modélisation et audit de composants à objets (LIRMM)
- Contrat de Recherche avec France-Télécom pour un modèle de contractualisation fonctionnelle et non fonctionnelle pour la plate-forme de composants Fractal (I3S-OCL)
- Contrat ITR *ScoT* : support de composants testables (VALORIA)

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

B2 – Description du projet : (5 à 10 pages)

Entre autres, le caractère innovant du projet (concepts, technologies, expériences …) devra être explicité et la valeur ajoutée des coopérations entre les différentes équipes sera discutée.

La description du projet s'articule de la manière suivante :

- Présentation rapide des compétences de chaque équipe sur les concepts de sécurité abordés,
- Proposition d'un modèle de composants de base, indépendant des technologies existantes,
- Présentation des verrous pour les différentes facettes de sûreté de fonctionnement abordées dans le contexte d'application par composants,
- Proposition d'un langage à composants permettant de mieux prendre en compte la sûreté de fonctionnement des applications, et description de la mise en œuvre du modèle par projection vers des plates-formes à composants,
- Etude d'une méthodologie de conception pour intégrer les concepts de sécurité dans des composants métiers.

B2.1 Compétences des partenaires

Les partenaires sont présentés dans l'ordre alphabétique.

INRIA

Le projet Oasis conçoit et développe la plate-forme SmartTools, générateur de composants pour des ateliers de développement interactifs fondé sur les nouvelles technologies XML, objets (programmation par aspects) et composants (EJB, « Web Services »). L'un des objectifs principaux est de promouvoir et de valider de nouveaux concepts de développement très innovants pour le développement de logiciel pour les langages dédiés. En effet, SmartTools s'intègre parfaitement dans la nouvelle stratégie de conception de logiciel défini par l'OMG pour les années à venir (« Model-Driven Architecture », MDA). La grande force de cette approche est l'unification des technologies liées aux langages (programmation par aspects), au Web (XML) et aux composants (architecture logicielle).

I3S

L'équipe OCL (Objets et Composants Logiciels) du laboratoire I3S a une expertise reconnue dans le domaine de l'approche contractuelle. Les travaux menés dans cette équipe concernent notamment l'application de cette approche aux plates-formes de composants logiciels, avec pour objectif premier de fournir un modèle général de contractualisation qui prenne en compte la spécification d'aspects fonctionnels (description comportementale, par exemple à l'aide d'assertions exécutables) et d'aspects non fonctionnels (qualité des services, contraintes sur des propriétés non fonctionnelles des composants), ainsi que les techniques nécessaires au contrôle de ces spécifications (analyse statique, contrôle à l'admission, contrôles dynamiques, protocole de certification). L'équipe OCL est aussi fortement impliquée dans la description de métamodèles pour la représentation de la sémantique opérationnelle des langages à objets ; elle en propose un qui est appelé OFL. La diversité des langages nécessite que le méta-modèle proposé soit fortement paramétrable et évolutif. Pour répondre à ce défi et permettre que le modèle puisse être étendu de manière incrémentale (en fonction de l'apparition de nouveaux concepts), notre approche développe des mécanismes basés sur des protocoles méta-objets et sur la séparation des préoccupations.

LGI2P

Au sein de la thématique « Modélisation par Objets », le LGI2P étudie l'apport des approches à objets dans la représentation et la gestion des modèles mis en œuvre lors de la conception (modèles conceptuels) et de l'utilisation (graphes d'objets) des logiciels et des systèmes d'information. Les travaux réalisés portent plus particulièrement sur la modélisation de « systèmes complexes » sous la forme de « graphes complexes de classes et d'objets » et la maîtrise de leur complexité grâce à deux approches complémentaires : celle de la construction de modèles complexes par composition de modèles élémentaires et celle de la construction de modèles complexes de manière incrémentale par versions successives de modèles. Les travaux en cours portent sur l'assemblage de composants logiciels piloté par les modèles (dans une approche de type MDA) et, en collaboration avec le

LIRMM, les exceptions dans les systèmes à agents et à base de composants.

LIRIS

Le modèle Samovar proposé dans la thèse de S. Coulondre dans le contexte des SGBD s'appuie sur le concept suivant : les classes et plus largement les composants sont perçus comme agrégats de rôles éventuellement hiérarchisés. Chaque rôle est défini intentionnellement par un critère de définition et possède structure et comportement. La perception et la manipulation du composant peuvent alors dépendre des rôles qui ont été activés, ceux-ci pouvant être perdus ou acquis au cours du cycle de vie du composant. Les droits potentiels d'accès aux rôles sont définis statiquement tandis que les droits d'accès réels sont définis dynamiquement en fonction du profil du requérant et de l'état du composant.
Ce modèle est adapté à l'heure actuelle dans le cadre d'une thèse au LIRMM (Robin Passama) relative à un modèle de composants dédiés aux applications robotiques.

LIRMM

L'équipe D'OC (Données, Objets, Connaissances pour les systèmes complexes) du LIRMM étudie de nombreux aspects du développement par objets et par composants : évolution des modèles, des méthodes de conception, des langages de programmation, des bases de données et des environnements de développement par objets et par composants, sémantique de représentation des classes et de la spécialisation, calcul automatique, réorganisation de hiérarchies de classes,...
Plusieurs parmi les domaines d'étude dans lesquels nous avons acquis une expertise relèvent de la sûreté de fonctionnement ou peuvent s'y appliquer. Nous avons en premier lieu une expérience reconnue en matière de fiabilité et de gestion des exceptions. Nous sommes actifs relativement aux recherches actuelles dans ce domaine (voir http://www.ecoop.tu-darmstadt.de/workshops/01.phtml) et travaillons en collaboration avec le LGI2P à la spécification de systèmes de gestion de la fiabilité dans les langages à base de composants.
Nous étudions ensuite la modularité et les mécanismes de protection. Nous disposons d'un formalisme de description des graphes d'autorisation d'accès statiques entre objets qui a de bonnes qualités pour la modélisation et la vérification de propriétés sémantiques dans le contexte des langages de programmation à classes. Dans ce même cadre, une collaboration en cours entre le LIRMM et l'I3S a également permis de poser les prémices d'un langage de définition de mécanismes de protection (LAMP).
Nous travaillons enfin sur les rôles et les points de vue et avons développé deux modèles complémentaires de prise en compte des rôles et des points de vue, l'un au sein des langages à objets et basé sur la délégation, l'autre au sein des bases de données objets de type ODMG. Les travaux relatifs à ces modèles se poursuivent respectivement dans l'équipe SIGMA-IMAG et dans l'équipe LIRIS-INSA, en collaboration avec le LIRMM.

LSR-IMAG

Une grande partie des activités de recherche menées au sein de l'équipe SIGMA vise à améliorer la réutilisation dans le cycle de développement des applications à l'aide de fragments de spécification (notamment patrons de types produit et processus, composants métier, rôles).
Les travaux menés autour des notions de rôles et de points de vue y seront poursuivis, afin de faciliter l'intégration des " facettes " de sécurité étudiées par les autres partenaires dans le modèle de composants qui constitue l'objectif principal de ce projet. Ces travaux pourront s'appuyer sur la plate-forme expérimentale SOJA, actuellement en cours de développement. SOJA fait suite au travail de D. Bardou sur le modèle des objets morcelés proposé alors qu'il effectuait sa thèse au LIRMM.
L'équipe SIGMA fera également bénéficier le projet de ses compétences relatives aux méthodes de développement. La gestion de la sécurité des informations et des services entre composants sera étudiée afin d'étendre la méthode SYMPHONY (proposée dans le cadre de la thèse de I. Hassine, sous la direction de Dominique Rieu et Agnès Conte), et de permettre la prise en compte des préoccupations liées à la sûreté dès les premières phases du cycle de vie. SYMPHONY repose sur un modèle de composants métier original (intégrant entre autres une notion de rôle) et une démarche en " Y " fragmentée en patrons de type processus ; c'est un processus unifié conformément à la terminologie de l'OMG.

VALORIA

Le groupe " Composants de confiance " de l'équipe Composants du VALORIA a une expertise sur la mise en œuvre du processus de développement nommé " Design for Trustability " (DfT) qui intègre largement les apports de l'approche contractuelle (Design by Contracts - DbC) proposée par Bertrand Meyer et un support de gestion des

tests intégrés (« Built-in Test »). Ce groupe a notamment développé un outillage et un préprocesseur de classes auto-testables supportant l'approche Dft (« Stclass ») et un modèle d'un méta-langage de description de code source O2CM (« Object Code and Contracts Model »). Par ailleurs ce groupe a également une expertise sur les modèles de description d'architecture logicielle à base de composants et sur les techniques de refactoring (re-structuration d'architecture logicielle).

B2.2 Modèle de composant de base

La première tâche sur laquelle il faut se concentrer est la définition d'un modèle (langage) de composants minimal qui fournisse l'ensemble des fonctionnalités nécessaires à la description des facettes de sûreté de fonctionnement (robustesse, correction et intégrité du code)[7]. La description de ce modèle nous offrira l'opportunité de définir à la fois un vocabulaire, une méthodologie et un support d'expression des propriétés qui soient communs à l'ensemble des partenaires.
Il faut préciser que notre objectif n'est pas ici de proposer un modèle destiné à remplacer les modèles existants mais uniquement de disposer d'une approche commune pour décrire les facettes de sûreté de fonctionnement dans les composants. L'ensemble des partenaires a une bonne expérience des technologies à composants et chaque partenaire a donc une idée des informations qu'il est nécessaire que les composants possèdent pour pouvoir décrire la ou les facettes de sûreté qui les concerne. Ce projet a vocation à capitaliser ces savoir-faire en proposant une approche unifiée.

Le modèle de composants que nous désirons proposer doit avant tout être indépendant des technologies existantes et contenir les entités de base utilisées par l'ensemble des facettes de sûreté. Par exemple notre modèle de composants devra intégrer les notions de connecteur ou de port, d'attribut de configuration, d'information de déploiement, *etc*. On étudiera dans la section B2.3 comment ce modèle sera enrichi par d'autres entités pour exprimer les contraintes de sécurité définies dans les différentes facettes (par exemple une *politique de droits d'accès* sur le *port* d'un *connecteur*). La composition de plusieurs facettes nécessitera certainement l'introduction de mécanismes de points de vue sur ce modèle à composants.

Il est important de noter que nous ne partons pas de rien pour définir ce modèle ; rappelons pour s'en convaincre deux aspects essentiels de la contribution de l'INRIA pour notre projet ; elle concerne SmartTools.
D'une part SmartTools[8] est un outil qui permet de développer des environnements pour des langages (traducteur, générateur, compilateur, etc.), à partir d'un arbre de syntaxe. Ceci nous conduit naturellement à l'utiliser pour prototyper rapidement le modèle à composants et ses extensions. Ces aspects seront décrits dans la section B2.4 relative à la spécification d'un langage componentiel sûr pour la description d'applications à composants.
D'autre part, pour faciliter son évolution SmartTools a été construit sur la base d'une architecture par composants ; celle-ci a rendu nécessaire la définition d'un langage à composants. Nous proposons donc de nous appuyer sur le modèle à composants défini dans SmartTools, et de l'enrichir en introduisant les mécanismes nécessaires à la description des facettes concernant la sûreté de fonctionnement. Le choix de cette démarche repose sur :

- la simplicité du modèle ;
- son indépendance vis à vis des technologies existantes ;
- notre maîtrise du modèle et donc sur la possibilité de disposer d'un outil pour expérimenter les extensions de ce modèle.

B2.3 Plans d'étude relatifs aux différentes problématiques de sûreté

La seconde étape de notre projet consiste en une série d'études relatives aux différentes problématiques liées à la sûreté, dans le cadre unificateur du langage componentiel minimal défini dans la section précédente. La fusion de ces études en une proposition unique fera l'objet de l'étape suivante. Nous indiquons dans cette section, pour chacune des problématiques recensées, quel est globalement l'état de l'art, quels sont les points clés sur lesquels il est nécessaire de faire porter les recherches indépendamment des autres problématiques, et enfin en quoi le

---

7 Ces facettes de sûreté seront décrites dans la section suivante (cf. B2.3).

8 Cette plate-forme utilise fortement les technologies du W3C et de l'OMG.

traitement conjoint des autres problématiques est difficile ou intéressant.

B2.3.1 Robustesse

Equipes participantes: LGI2P, LIRMM

La problématique de la robustesse, de la tolérance aux pannes est de plus en plus importante car nos sociétés sont devenues très dépendantes de l'outil informatique et ne supportent plus que certains systèmes (économie, santé, transports, ...) cessent de fonctionner de façon imprévue. Pour cela, toutes les recherches relatives à l'auto-réparation, à l'adaptation dynamique des applications, ce qui inclut donc leur capacité à tolérer dynamiquement les événements exceptionnels, deviennent ou redeviennent primordiales.

La gestion des exceptions dans les langages de programmation en général et à objets a été étudiée, en particulier du point de vue du contrôle. Différentes alternatives (solution Flavors/Clos/Smalltalk versus solution C++/java versus solution Eiffel, …) ont été proposées et un standard, qui laisse d'ailleurs beaucoup de propositions intéressantes dans l'ombre, a émergé (C++, Java). Elle a été beaucoup moins étudiée du point de vue de la modélisation des programmes et pose aujourd'hui un ensemble de nouvelles questions. Les nouveaux verrous technologiques dans ce domaine sont globalement liés :

- aux besoins des applications : concurrence, distribution, adaptabilité, intéropérabilité,
- à l'évolution des techniques de développement : méta-modélisation, réutilisation, utilisation de composants, nouveaux modèles d'assemblage et de communication.

Les points difficiles sur lesquels nous souhaitons faire porter nos travaux dans le cadre de la définition d'un langage de développement par composants concernent en premier lieu les différents protocoles de communication connus, l'utilisation ou la connexion de composants. La communication asynchrone ou la communication par évènements (schéma de conception « Observateur ») posent ainsi un ensemble de nouveaux problèmes de traitement.

Nous souhaitons ensuite aborder un ensemble de problèmes ouverts de modélisation qui se posent déjà avec l'approche par objets et qui subsisteront dans une approche componentielle. Nous chercherons à déterminer quelles sont les bonnes ontologies d'évènements exceptionnels (point qui n'a jamais été véritablement traité) ? Quels sont les bons schémas de conception de ces ontologies et comment passer de la représentation par objets des exceptions (devenue classique) à une représentation componentielle ? Comment traiter de la décomposition modulaire des applications en présence potentielle d'exceptions (la gestion d'exceptions est-elle un aspect d'une application au sens « AOP ») ? Comment réutiliser en fiabilisant a posteriori, par exemple par spécialisation, un composant?

Enfin la prise en compte des aspects de sûreté connexes à celui-ci ouvre la voie à de nombreux travaux. Les systèmes de gestion des exceptions modifient en effet en profondeur les langages et enrichissent, éventuellement considérablement, la panoplie d'expression des programmeurs. A ce titre, intégrer les réponses exceptionnelles aux interfaces, aux contrats, à la vérification des accès, aux tests, sont des problèmes ouverts que nous pourrons aborder dans le cadre de cette collaboration.

B2.3.2 Correction

Equipes participantes: I3S, VALORIA, LSR-IMAG

La problématique de la correction, de la conformité avec des spécifications, se pose avec l'approche objet et se complexifie avec l'approche componentielle. Selon un rapport récent du *SEI* (« Software Engineering Institute »), un des principaux verrous à l'utilisation de l'approche componentielle réside dans la difficulté qu'il y a à garantir des propriétés (qualité de service) d'un assemblage de composants à partir des propriétés des composants pris individuellement et dans la difficulté à effectuer un *raisonnement compositionnel*. L'approche contractuelle, largement utilisée dans le monde du développement par objets, a montré qu'elle était une voie intéressante pour améliorer le niveau de correction des applications, sans heurter de front les habitudes de travail des développeurs.
Nous proposons d'étudier l'utilisation de l'approche contractuelle dans le cadre de la spécification et de l'exécution d'application développées en assemblant des composants logiciels.

En terme de spécification, elle permettra d'assembler des composants sur la base d'informations sémantiques et d'aller beaucoup plus loin, en terme de vérification des propriétés, qu'avec les approches actuelles à base de langages de description d'interfaces. Nous étudierons quelles sont les nouvelles formes de contrats appropriés qui permettront de spécifier les composants et leur assemblage avec garantie de correction : *co*ntrats d'interfaces pour spécifier les interfaces requises et fournies des composants, contrats de composants pour spécifier des propriétés spécifiques, *contrats d'interaction* ou *contrats d'architecture (*selon la nature des propriétés énoncées*)* pour spécifier les propriétés propres à un assemblage de composants.

En terme d'exécution, la spécification comportementale des composants par contrats sera également étudiée. Les contrats comportementaux, représentés à la base par des exceptions exécutables offrent des solutions puissantes pour effectuer des vérifications sémantiques dans tous les cas de reconfiguration dynamique (échange de composant, restructuration à chaud) ou de réparation des composants qui ne répondent plus aux contraintes posées, par exemple par suite de modification du contexte d'utilisation ou par suite d'occurrence de situations exceptionnelles. Des mécanismes de transformation, s'appuyant sur des techniques de « *refactoring* » , seront étudiés pour assurer la possibilité de mise en conformité d'un composant relativement à des contraintes de sécurité.

L'avantage et l'inconvénient de l'approche contractuelle sont qu'elle intègre l'incomplétude : c'est un avantage par rapport aux approches purement formelles car elle est plus facile à gérer par des équipes de développement dans le monde réel ; c'est à la fois un inconvénient car elle ne peut être à elle seule une garantie de qualité ou de fiabilité. Pour répondre à cet inconvénient, nous proposons également de compléter la définition de contrats de tous niveaux par la mise en œuvre de tests intégrés et de mécanismes de contrôle *a posteriori* inspirés des tests par mutation.

L'ensemble des mécanismes liés aux contrats sont évidemment assez intimement liés à la détection et au traitement des situations exceptionnelles et la définition de traitements appropriés, et l'un des intérêts du projet sera de coupler l'étude « correction » et l'étude « robustesse ».

B2.3.3 Intégrité du code et des données

Equipes participantes: I3S, LIRMM, LIRIS, LSR-IMAG,

L'intégrité d'un code et des données est une troisième problématique fondamentale en terme de sécurité de fonctionnement. Le respect de cette intégrité passe par la possibilité de spécifier de façon cohérente des droits d'accès. Les points d'études suivant sont relatifs au contrôle des droits d'accès aux composants et à la possibilité de spécifier ces droits de façon fine et modulaire sur la base de rôles.

Contrôles d'accès.

Une étude préalable relative aux contrôles d'accès statiques dans les langages de programmation et de modélisation actuels nous a convaincu de la nécessité de disposer en la matière de formalismes suffisamment expressifs, utilisables à tous les stades du développement, mais également dotés d'une sémantique formelle claire qui permette d'effectuer des raisonnements. L'absence ou l'insuffisance de tels formalismes, comme le montre l'étude de certains langages à objets, constitue une faille pour la sécurité.
Dans le cadre de ce projet, nous comptons proposer un formalisme de spécification et de description des contrôles d'accès à l'aide de graphes pour le développement componentiel, en portant plus spécifiquement notre attention sur leurs interfaces. En effet, les modèles les plus classiques identifient, outre la notion de composant qui est une unité autonome d'exécution et de déploiement, les interfaces externes par lesquelles le composant rend des services et les interfaces requises par lesquelles il utilise d'autres services. La description d'un système consiste alors à connecter ces interfaces entre elles. Trouver des composants réutilisables et déterminer les agencements possibles de composants en vue de la réalisation d'une fonctionnalité globale est déjà un problème en soi. Si l'on souhaite de plus sécuriser ces connexions, il convient de se doter d'une description de ce qui est autorisé : une interface externe peut n'être accessible que pour certains composants, certaines connexions, voire certains ensembles de connexions, entre composants peuvent n'être admises que dans certains contextes, *etc*. Notre formalisme semble une base appropriée pour spécifier de telles descriptions. Les composants protègeront leurs code et état en spécifiant les contraintes que devront satisfaire leurs clients potentiels pour accéder à leur services. Les

descriptions devront être indépendantes des langages et paramétrables. Nous étudierons des mécanismes statiques de vérification des contraintes et de signalement des transgressions, en connexion possible avec le système d'assertions, ainsi que les mécanismes de transformation automatisée des descriptions vers des langages cibles.

Rôles et sûreté de fonctionnement

La notion de rôle permet notamment de définir plus finement la structure et le comportement des composants puisqu'elle introduit de manière explicite des « fragments » de granularité intermédiaire entre la définition d'une propriété et la définition globale d'un composant.

Bien qu'aucun langage à objets majeur n'intègre la notion de rôles, de nombreuses études ont été menées à ce sujet et nous disposons d'une expertise dans ce domaine. Un rôle est une unité de modularité intermédiaire avec laquelle peut être spécifiée une partie limitée et sémantiquement cohérente d'un objet ou d'un composant. Il est facilement envisageable de spécifier au niveau d'un rôle des contrôles d'accès spécifiques. Un rôle pourrait même correspondre à la projection d'un contrat sur un composant. Les applications en terme de sûreté de fonctionnement sont nombreuses et importantes.

D'une part, comme avec les mécanismes de vues dans les bases de données, les rôles peuvent être utilisés pour définir des versions partielles mais « sécurisées » d'un composants, utilisables dans des contextes contraints. Inversement un composant peut se voir attribués ou non certains droits selon le rôle qu'il est en train de jouer (modèle des profils utilisateurs dans certains logiciels).
Par ailleurs, si l'on considère un système de composants dans sa globalité, les rapports étroits existants entre les rôles et les approches par séparation des préoccupations telles que le développement de logiciel par aspects, ou encore les approches multi points de vue, pourront fournir une base de réflexion pour la mise en place de la gestion de la sécurité en tant qu'aspect du système.
Enfin, les mécanismes associés à la gestion de rôles permettent l'adaptation dynamique (acquisition/perte de rôles pour un composant). Cette caractéristique impose bien évidemment la mise en place de contrôles dynamiques, plutôt que des contrôles essentiellement statiques, qui reposent généralement sur la définition et l'utilisation d'exceptions dans un modèle approprié : le modèle d'exceptions étendu proposé devra donc être capable d'assurer ces fonctionnalités.

B2.4 Définition d'un langage componentiel pour développer des applications sûres

Une fois établi un langage de composant minimal et disposant d'un ensemble d'études préalables relatives aux diverses problématiques de sûreté abordées, la phase centrale du projet consiste à considérer toutes les études préalables pour les fusionner en un tout cohérent sous la forme d'une spécification de langage à composants spécialisé sûreté. Le seconde partie de cette phase centrale consiste en l'étude des différentes possibilités de projection (de mise en œuvre) de cette spécification.

Ces objectifs constituent selon nous un véritable défi et il est important de montrer dès maintenant que notre démarche est réaliste et qu'elle conduit à une contribution concrète et réellement novatrice en terme de sûreté de fonctionnement des applications à base de composants.

Nous avons montré dans la section B2.2 comment nous désirions utiliser le langage de composants de SmartTools comme base de réflexion pour nos spécifications puis comme support d'intégration des structures de contrôles définies pour répondre aux besoins des diverses problématiques de sûreté.
Le langage de description des composants de SmartTools est indépendant du langage utilisé pour décrire leurs fonctionnalités fonctionnelles. Du point de vue du projet, ceci permet de bénéficier à la fois :

- d'un outil de spécification pour les facettes de sûreté: il fournit un environnement méta (outils de description de langages), pour la définition des traitements sémantiques des structures de contrôle relatifs;
- d'un outil d'intégration du code métier des composants : cet outil permet d'inclure automatiquement un code métier décrit en Java standard et de l'encapsuler dans un composant. Nous pourrons ainsi projeter nos spécification sans avoir à réécrire un langage complet.
- d'un outil de validation : L'architecture de SmartTools est elle-même ouverte et à base de composants.

Cela nous permettra de disposer à moindre coût d'une plate-forme de validation de nos extensions très tôt dans le déroulement du projet ;

- d'un support pour l'approche MDA : le modèle de composants de SmartTools est décrit indépendamment des technologies d'implantation (c'est un PIM). Plusieurs projections vers des technologies existantes ont déjà été réalisées en utilisant les outils de description de langages de SmartTools. Nous envisageons d'utiliser cette démarche pour la mise en œuvre de notre langage de composants ;
- d'une ouverture vers les standards de l'OMG : l'utilisation du formalisme unificateur XML favorise la réalisation de passerelles entre notre langage de composants et d'autres formalismes de modélisation (par exemple UML, MOF, etc.). Les capacités offertes par ces différents standard seront en particulier utiles pour classifier les entités du référentiel, définir les mécanismes de composition ou de points de vue, et plus généralement pour étendre le modèle initial.

Après avoir précisé le contexte de spécification de notre langage à composants il est donc utile de préciser la façon dont nous comptons traiter les principaux aspects novateurs de notre approche : l'intégration des différentes spécifications doit se faire de manière unifiée et incrémentale. Enfin il est nécessaire de prendre en compte le caractère adaptatif (dynamique) des applications auxquelles nous nous intéressons :

- Unifié : afin de pouvoir intégrer les facettes de langages décrites dans les spécifications issues des études décrites en section B2.3, il faudra à la fois, identifier les mécanismes élémentaires communs et les incompatibilités potentielles.
- Incrémental : pour garantir le caractère incrémental de l'intégration des facettes, l'ouverture de l'architecture logicielle de SmartTools sera un élément déterminant. Pour atteindre cet objectif nous envisageons de nous appuyer sur une approche par séparation de préoccupations (approches apparentées à la programmation par aspects).
- Dynamique : Certaines facettes doivent pouvoir prendre en compte une reconfiguration dynamique des composants ; c'est le cas par exemple des contrats comportementaux associés aux composants logiciels qui souvent induisent des échanges et restructurations " à chaud ". L'aspect dynamique doit donc se retrouver aussi bien au niveau de la spécification du langage qu'au niveau des contraintes de mise en œuvre.

Enfin, voici ce que nous suggérons relativement à la mise en oeuvre de notre langage à composants. Nous prévoyons d'étudier deux types de projections :

- une projection vers Java qui consistera à produire pour chacune des facette du code Java qui sera intégré dans les applications finales;
- une projection dans laquelle nous étudierons, à partir de spécifications réalisées dans notre langage, comment produire du code compatible avec une technologie existante intégrant des composants.

Pour la première solution, il nous faudra étudier précisément comment enrichir l'application Java pour qu'elle puisse utiliser implicitement les services proposés par les différentes facettes de sûreté (évaluation de contrats, rattrapage d'exception, clauses de protection, etc.). Cela nécessitera certainement la réalisation de bibliothèques spécifiques à chaque facette. Il faudra ensuite pouvoir les composer et prendre en compte le caractère dynamique des contrôles.
A propos de la deuxième solution, nous ne pourrons pas nécessairement projeter l'intégralité de notre spécification et il sera donc important de choisir une plate-forme de composants qui soit la plus ouverte possible; par exemple la plate-forme Fractal[9].

Quelque soit la solution de mise en oeuvre retenue, nous devrons étudier, pour chaque facette, si l'intégralité de notre spécification peut être intégrée au niveau PIM (indépendant de la projection choisie) ou si une partie de la spécification nécessite une mise en œuvre *ad hoc*. pour chaque projection spécifique.

En conclusion, nous proposons avec SmartTools un support pratique et réaliste pour, d'une part, spécifier notre langage de composant doté de ses extensions pour la sûreté, et d'autre part, pour étudier une mise en oeuvre modulaire et incrémentale des extensions.

---

9 L'équipe OCL est en train d'étudier la possibilité d'intégrer dans Fractal un mécanisme pour la programmation contractuelle.

B2.5 Approche par composants métiers

Un composant métier (*business component*) peut être défini comme une représentation de la nature et du comportement d'une entité du monde réel dans des termes issus du vocabulaire d'une entreprise (d'un métier) : concepts, événements, processus. Les composants métiers sont utilisés pour concevoir et réaliser des systèmes d'information, ils constituent des éléments de conceptions réutilisables.
Il est primordial d'étudier la prise en compte des facettes de sécurité dès les premières étapes du cycle de développement, et de ne pas se limiter aux seuls composants techniques permettant de composer une application. Pour cela il est nécessaire, non seulement de disposer d'un modèle de composants métier qui puisse être utilisé dans ces premières étapes (avant même d'en finaliser la conception dans le modèle PIM proposé dans ce projet), mais aussi de disposer d'une démarche de développement détaillant les activités et les processus par lesquels la sécurité est abordée par les acteurs du développement d'une application.
Plus précisément, il s'agira d'apporter des réponses aux questions suivantes : « comment se déclinent les facettes de sécurités dans les étapes d'expression des besoins, d'analyse, de conception d'un système à base de composants métier ? », « quelles sont les activités de développement à mettre en place pour les prendre en compte ? », « comment représenter la sécurité dans un modèle conceptuel de composants métier ? ».
Ces réflexions seront concrétisées par une évolution de la méthode SYMPHONY à deux niveaux : intégration des propriétés relatives aux différentes facettes de sécurité dans le modèle de composant métier servant et ajout de fragments de démarches, sous forme de patrons de type processus, spécifiques à la sécurité, des. La méthode SYMPHONY dans une telle évolution devrait donc permettre, par sa démarche, de guider les acteurs du développement d'une application pour la spécification des différentes facettes de sécurité dans les étapes de développement situées en amont de leur spécification dans la plate-forme PIM qui constituera l'un des résultats de ce projet. Le modèle conceptuel de composant métier, quant à lui, pourra servir de base à l'élaboration du modèle de composant technique.

B3 – Résultats attendus :

On détaillera l'échéancier des résultats et réalisations intermédiaires et finaux attendus. On précisera les risques scientifiques qui seront pris. On discutera de l'impact potentiel de ce projet sur les scènes européenne et internationale.

B3.1 Résultats et avancées

Les résultats attendus de cette action sont de trois types :

- Mise en commun des différentes compétences de chaque équipe pour élaborer une solution globale pour prendre en compte la sûreté de fonctionnement dans le cadre d'applications à base de composants, et fortement dynamiques. Ce travail devrait aboutir à la définition d'un modèle (PIM) qui propose une sémantique précise des concepts manipulés (robustesse, correction, intégrité).
- Mise en place d'une plate-forme logicielle ouverte qui permette à la fois de mettre en œuvre et d'étendre le modèle, et de prendre en compte les interdépendances entre les divers concepts de sécurité au moment de leur composition. Cette plate-forme sera le support pour valider notre modèle.
- Mise en œuvre de la sémantique d'exécution de notre modèle sur différentes plates-formes d'exécution existantes. Elles seront définies en fonction de leur pertinence et de leur intérêt pour la diffusion de nos travaux.

Ces trois résultats vont permettre de proposer des avancées importantes pour la sécurité informatique sur les points suivants.

- Proposer un modèle de sécurité qui unifie trois grandes catégories de concepts de sécurité (robustesse, correction, intégrité). Selon nous, la prise en compte de ces trois concepts assure un haut degré de sûreté de fonctionnement pour un large sous-ensemble d'applications.
- Traiter plus particulièrement les problèmes relatifs aux contrôles dynamiques associés à ces types de concepts, plutôt que de s'intéresser à la vérification de propriétés qui imposent une connaissance plus statique de l'application. En d'autres termes nous centrerons notre approche sur la définition d'une sémantique permettant d'aborder de façon dynamique des concepts de sécurité.
- Assurer une forte extensibilité de l'approche afin de prendre en compte la forte évolution des besoins des applications en matière de sécurité qui ne manquera pas de donner naissance à de nouveaux concepts de sécurité. L'approche par séparation des préoccupations pour définir le modèle nous semble une avancée majeure et incontournable dans un domaine à fort degré d'évolution. Il diffère nettement de celui des langages de programmation où la sémantique est relative à un contexte figé.
- Factoriser et abstraire la sémantique opérationnelle des différents concepts afin que les projections vers les plates-formes d'exécution existantes soient le plus possible inférées.

B3.2 Organisation du projet et échéancier prévisionnel

Nous proposons que le projet se déroule en trois phases qui correspondent chacune à environ une année :

- La première phase permettra de recenser les divers concepts et contraintes en s'appuyant sur chacune de nos compétences. La définition de notre modèle PIM sera notre " fil rouge " pour cette phase de démarrage de l'action. Cette phase permettra de définir le cahier des charges des deux actions suivantes (à savoir le modèle PIM et la mise en œuvre).
- La deuxième phase va consister à décrire d'une part les concepts du modèle de manière unifiée et d'autre part la méthodologie utilisée pour assurer l'aspect extensible du modèle.
- Enfin la dernière phase correspondra à la mise en œuvre de notre modèle. A ce stade de l'étude il nous sera possible de choisir les plates-formes d'expérimentation pertinentes pour nos travaux.

Calendrier des tâches

- Tâche 1 : Définition du modèle à composant de base
  - Responsable : INRIA
  - Partenaires participant : tous
  - Durée : 6 mois
  - Début : T0 ; Fin : T0 + 6 mois
- Tâche 2 : Définition du concept de sécurité " correction "
  - Responsable : I3S
  - Partenaires participant : I3S, VALORIA, LSR-IMAG
  - Durée : 12 mois
  - Début : T0 ; Fin : T0 + 12 mois
- Tâche 3 : Définition du concept de sécurité " robustesse "
  - Responsable : LIRMM
  - Partenaires participant : LIRMM, LI2PG
  - Durée : 12 mois
  - Début : T0 ; Fin : T0 + 12 mois
- Tâche 4 : Définition du concept de sécurité " intégrité des données et du code "
  - Responsable : LIRMM
  - Partenaires participant : LIRMM, I3S, LIRIS, LSR-IMAG
  - Durée : 12 mois
  - Début : T0 ; Fin : T0 + 12 mois
- Tâche 5 : Définition d'un langage componentiel pour développer des applications sûres
  - Responsable : INRIA
  - Partenaires participant :tous
  - Durée : 22 mois
  - Début : To + 6 ; Fin : T0 + 28 mois
- Tâche 6 : Définition d'une méthodologie de projection vers les plates-formes à composants
  - Responsable : INRIA
  - Partenaires participant : tous
  - Durée : 18 mois
  - Début : T0+18 ; Fin : T0 + 34 mois
- Tâche 7 : Méthodologie de développement d'application à base de composants métiers intégrant les concepts de sécurité.
  - Responsable : LSR-IMAG
  - Partenaires participant : LSR-IMAG
  - Durée : 24 mois
  - Début : T0 + 12 ; Fin : T0 + 36 mois
- Tâche 8 : Evaluation de la plate-forme.
  - Responsable : VALORIA
  - Partenaires participant : tous
  - Durée : 6 mois
  - Début : T0+30 ; Fin : T0 + 36 mois

B3.4 Conclusion

L'hypothèse forte de notre projet est que les composants seront instrumentés, ou pourront l'être *a posteriori* par notre modèle de sécurité. L'indépendance de ce dernier vis à vis des technologies existantes, le spectre des concepts initiaux et son extensibilité, garantissent qu'il sera toujours possible d'instrumenter l'ensemble des composants d'une application. En conclusion, nous pensons qu'il est avant tout important de proposer une approche réaliste (pragmatique) qui d'une part répond bien aux contraintes de sécurité des applications de demain et d'autre part permet de définir un cadre homogène (avec des hypothèses et contraintes transposables sur différentes plates-formes).

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

B4 – Summary (in English) : (1 to 2 pages)

Le Conseil Scientifique pourra solliciter des experts non francophones auxquels sera envoyé l'ensemble des documents. Le présent résumé, entièrement rédigé en anglais, visera à fournir une présentation synthétique de l'ensemble du projet.

Software safety has to do with correction, robustness and integrity of programs and data ; it is also closely related to the more general concept of computer security. Although several works have been done on correction, robustness and integrity, they are most often conducted in a separate way, and need to be reconsidered to cope with the most recent advances pertaining to software architecture and software development practices, in which one can put forward more particularly the component-oriented technology. There is currently no unifying approach, no general model, that supports components specification, programming and assembly, and software safety related aspects at the same time. Moreover, the current solutions proposed to solve software safety problems are often tied to a specific framework or component technology, and can only be applied at a rather low level of abstraction. They rarely allow software architects to express the abstract safety constraints in the early stages of the software life-cycle. Our proposal has the three following objectives :

- We primarily want to propose a software component model in which solutions for the problems related to correction, robustness and integrity can be applied together. This model has to be defined in order to not depend of any specific technology, but should however provide ways to product actual code for well-known technologies. In other words we plan to respect the OMG MDA ("Model Driven Architecture") approach by proposing a PIM ("Platform-Independent Model") and studying its mapping to PSMs ("Platform-Specific Models").

- We also want to study the ways to keep software evolutionary and easily adaptable by providing means to dynamically handle and reconfigure controls that are closely related to software safety. We will however not exclude any static analysis technique that would remain compliant with such dynamic controls.

- Our third objective is to allow software components to be incrementally equipped by adding new safety features to them: our component model will thus have to be extensible with regards to both the definition of properties and the controls and functions that are associated to them.

Our proposal is based on the partnership of seven research teams with complementary skills such as design by contracts, access control mechanisms, separation of concerns, roles and multidimensional design, components). Some collaborations already exist between these research teams, and they all share a common interest for component-based software design. We plan to exploit those complementary skills and meet our objectives by organizing the work as follows.

In the first phase of the project (1 year duration), all the partners will agree on a common component model that will serve as a basis for further work related to correction, robustness and integrity. This reference model will be mainly inspired by earlier work done on the SmartTools framework (INRIA). Study and definitions of solutions addressing the three safety concerns that will be emphasized will immediately follow.

- **Correction** will be mainly enforced by exploiting the partners' skills related to design by contracts (I3S, VALORIA). The design by contract approach will provide advances both at the specification and at the execution phases. In terms of specification, it will allow to assemble components according to semantic criteria and thus provide advanced property checking capabilities. In terms of execution, it will allow to verify components' semantics in case of dynamic reconfiguration of the component assemblies being executed.

- **Robustness** can be improved by exception-based mechanisms (LIRMM, LGI2P). If exception handling has been widely studied in programming languages (among which are object oriented languages), few work exists in relation with program modeling and new problems arise in relation with new application needs (such as concurrency, distribution, adaptability, interoperability) or new development techniques (such as meta-modeling, reuse, component based programming, new assembly or communication models). Addressing these new problems will provide means to increase the robustness of the common

component model.

- **Integrity** will be addressed by the definition of access controls (I3S, LIRMM, LISI, LSR-IMAG). In order to ensure the reliability of component assemblies, an access control specification and description formalism is needed. It will focus on component interfaces and allow components to protect their code and state by specifying constraints their clients will have to fulfill in order to be authorized to access the components' services.

The second phase of the project (about 1.5 year duration, following first phase) will mainly aim to put the results of the first phase together in order to provide a new component model in which all the safety concerns can be considered jointly. The newly defined model can be regarded as a PIM, it will be independent of any specific component-oriented technology.

The third phase of the project (about 1.5 year duration, partly concurrent to the second phase and ending the project) will consist of studying and providing mappings from the PIM resulting from the second phase and concrete validation of the project results. Mechanisms and their possible variations for ensuring correction, robustness and integrity will be studied and implemented. This last phase will also aim to provide a software development method allowing to consider software safety in the early stage of the software life-cycle: the SYMPHONY method (LSR-IMAG) will be extended both in its business-component model and its process to achieve the management of security concerns starting at the requirement engineering stage.

Collaborative work will be encouraged by organizing regular meetings of the partners (3 meetings per year). Funding will also serve for hardware and software renewal, and for attending valuable events or conference in the fields related to the project. Some software engineers will be temporarily hired in order to ensure the implementation of the platform validating the project's results ; a doctoral and a post-doctoral position will also be open to help the partners in their works. This project should notably contribute in the development of software systems based on safe components.

C – MOYENS FINANCIERS ET HUMAINS DEMANDES PAR CHAQUE EQUIPE[10]

Comme indiqué dans les tableaux ci-dessous, on distinguera

- *les financements via le Fonds National pour la Science qui peuvent inclure*
  - ** du fonctionnement*
  - ** de l'équipement*
  - ** des mois de personnel temporaire (CDD) pour un montant ne pouvant excéder 50% du financement total attribué. La durée du ou des contrat(s) prévus, qui ne peuvent excéder 24 mois chacun, sera précisée.*
- *les moyens demandés aux organismes de recherche qui peuvent inclure*
  - ** des postes de post-doc*
  - ** des demandes de délégation ou détachement pour des enseignants-chercheurs*
  - ** des accueils de chercheurs étrangers*
- *les demandes d'allocations de recherche*

Les diverses possibilités concernant l'attribution de moyens pour recruter ou accueillir des personnels seront globalement très limitées pour l'ensemble des ACI. Leurs demandes devront donc être particulièrement justifiées. Si les bénéficiaires de ces demandes sont connus ou pressentis, les CV correspondants seront joints à la présente demande.

Dans le cas des moyens alloués par les organismes, il n'est pas nécessaire de préciser à quel organisme (CNRS ou INRIA) ces moyens seront demandés, sauf cas particulier à expliciter. Ces moyens seront en effet répartis globalement au niveau de l'ACI, en tenant compte bien sûr des règles et contraintes propres à chaque organisme.

On présentera une justification scientifique des moyens demandés pour chacune des équipes impliquées dans le projet.

[10] Une fiche C doit être remplie pour chaque laboratoire ou équipe partenaire

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : INRIA (SmartTools)

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	5,00	0,00	0,00	5,0
Fonctionnement (dont CDD décrits ci-dessous)	8,78	61,23	61,23	131,23
Total / année	**13,78**	**61,23**	**61,23**	**136,23**

Dépenses de personnels (CDD) [11]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	Ingénieur expert ou post-doc
Durée de l'emploi (en mois)[12]	24
Coût total de l'emploi	104,90 (52,45 par an)

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[13]	1 (12 mois)	0	0	1
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[14]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	0	0	0	0

[11] Un tableau doit être rempli pour chaque demande de CDD.
[12] Doit être inférieure à 24 mois
[13] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[14] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

La demande d'un CDD de 2 ans pendant les deux dernières années correspond aux besoins du projet nécessaires à la mise en œuvre d'un prototype pour la validation et comme support pour les publications.
La première année est plutôt réservée à la mise en commun de nos compétences et à des travaux de conception. Elle ne nécessite donc pas la présence d'un personnel supplémentaire attaché à des tâches d'implantation. Par contre les deux dernières années, il sera indispensable de recevoir l'aide d'un ingénieur ou d'un post-doc capable à la fois d'implémenter, de comprendre ou d'intervenir dans les travaux de recherche réalisés par les différents partenaires. C'est pour cela que le profil demandé est ingénieur ou chercheur. Sa localisation à l'INRIA découle naturellement du choix d'utiliser SmartTools comme support pour la réalisation du prototype.

La demande d'un post-doc, la première année par l'INRIA est elle aussi tout à fait justifiée. Elle permet d'expérimenter une première utilisation de SmartTools pour valoriser certains aspects relatifs à l'intégrité du code. Les " feedbacks " de ce premier travail servira aux autres partenaires pour mener à bien la conception des extensions du modèle à composant. Le choix de mener cette première expérimentation sur cette partie repose sur l'opportunité de recruter pour ce travail Gilles Ardourel (LIRMM), qui a terminé une thèse sur un sujet connexe cette année et qui participe à une action COLOR[15]. Nous espérons ainsi faire profiter le projet de ses compétences.

Les autres demandes de fonctionnement sont calculées *au prorata* des personnes impliquées. Il est à remarquer que pour ce partenaire, nous comptons la personne en CDD (car elle est cruciale pour la cohérence du projet). La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

Projets en cours ou en soumission :

- Projet IST : **QUESTION-HOW** avec le W3C (http://www-sop.inria.fr/oasis/Didier.Parigot/SmartTools/W3C)

- Projet RNTL Plate-Forme **Modathèque** : composants MDA (en soumission) (http://www-sop.inria.fr/oasis/Didier.Parigot/MDA)

- Action R&D **Syntax** (INRIA): Traitement du document électronique (http://www-sop.inria.fr/oasis/Didier.Parigot/SYNTAX)

- Action COLOR (INRIA/LIRMM/I3S) **Protection dans les langages de programmation** – Année 2003 : l'objectif est de réaliser une plate-forme générique qui permettra de définir/spécifier les mécanismes de protection des langages de programmation et de vérifier que les applications décrites avec le langage choisi sont conformes (http://www-sop.inria.fr/oasis/Didier.Parigot/COLOR).

[15] Cette action COLOR est menée conjointement avec l'INRIA, le LIRMM et le laboratoire I3S.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : Laboratoire I3S

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	6,91	0,0	0,0	6,91
Fonctionnement (dont CDD décrits ci-dessous)	8,75	8,75	8,75	26,26
Total / année	**15,67**	**8,75**	**8,75**	**33,17**

Dépenses de personnels (CDD) [16]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	
Durée de l'emploi (en mois)[17]	0
Coût total de l'emploi	0

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[18]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	1 (3 mois)	2 (3 mois)	1 (3 mois)	4 (12 mois)
Nombre d'accueils en délégations ou détachements[19]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	1	0	0	1

[16] Un tableau doit être rempli pour chaque demande de CDD.
[17] Doit être inférieure à 24 mois
[18] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[19] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

La compétition entre les équipes universitaires et l'INRIA est rude pour l'attribution des stages de DEA et des allocations de thèse au sein de l'école doctorale.
L'équipe OCL de l'I3S a besoin d'une allocation de recherche sur le thème de l'approche contractuelle pour exploiter les résultats déjà obtenus dans la collaboration avec France Télécom et les développer dans le cadre de cette ACI. Le bénéfice de cette bourse profitera bien sur aux autres partenaires qui travaillent plus spécifiquement sur cet axe de recherche comme par exemple le VALORIA, et elle permettra de renforcer leur collaboration.
Par ailleurs concernant la modélisation du langage à composants, cette équipe travaille en collaboration avec deux chercheurs roumains qui préparent leur thèse sur un sujet connexe. Il sera intéressant pour le projet de pouvoir les faire venir environ 3 mois par an afin de capitaliser leur travail. Au cas où il n'est pas possible d'obtenir de poste pour l'accueil de chercheurs étrangers, il sera intéressant de pouvoir bénéficier d'un montant supplémentaire de 5200€ permettant de financer leur mission et leurs frais de séjours.

Les autres demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

- Contrat de Recherche Externe France Télécom R&D « Modèle de contractualisation pour composants : application à la plate-forme Fractal », montant 32 696 € HT sur 18 mois (août 2002 - janvier 2004)

- Action COLOR (INRIA/LIRMM/I3S) **Protection dans les langages de programmation** – Année 2003 : l'objectif est de réaliser une plate-forme générique qui permettra de définir/spécifier les mécanismes de protection des langages de programmation et de vérifier que les applications décrites avec le langage choisi sont conformes (http://www-sop.inria.fr/oasis/Didier.Parigot/COLOR).

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : LGI2P

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	1,13	0,0	0, 00	1,13
Fonctionnement (dont CDD décrits ci-dessous)	3,02	3,02	3,02	9,06
Total / année	**4,15**	**3,02**	**3,02**	**10,19**

Dépenses de personnels (CDD) [20]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	
Durée de l'emploi (en mois)[21]	0
Coût total de l'emploi	0

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[22]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[23]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	0	0	0	0

[20] Un tableau doit être rempli pour chaque demande de CDD.
[21] Doit être inférieure à 24 mois
[22] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[23] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

Les demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : LIRMM

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	6,94	0,0	0,0	6,94
Fonctionnement (dont CDD décrits ci-dessous)	10,52	62,96	10,52	83,99
Total / année	**17,45**	**62,96**	**10,52**	**90,93**

Dépenses de personnels (CDD) [24]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	1
Durée de l'emploi (en mois)[25]	12
Coût total de l'emploi	44

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[26]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[27]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	1	0	0	1

[24] Un tableau doit être rempli pour chaque demande de CDD.
[25] Doit être inférieure à 24 mois
[26] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[27] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

La demande d'un post-doc, la dernière année par le LIRMM trouve sa raison d'être dans le fait qu'elle permet à Frédéric Souchon (en thèse au laboratoire), qui aura terminé sa thèse sur un sujet relatif à la contribution du LIRMM pour cette ACI à la fin de sa deuxième année puisse continuer à faire profiter le projet de son travail.

Tout comme pour le laboratoire I3S, La compétition entre les équipes universitaires et l'INRIA est ici aussi très rude pour l'attribution des stages de DEA et des allocations de thèse au sein de l'école doctorale.
L'équipe D'OC du LIRMM a besoin d'une allocation de recherche sur le thème du traitement des exceptions pour améliorer les résultats déjà obtenus par Frédéric Souchon. Le bénéfice de cette bourse profitera bien sur aux autres partenaires qui travaillent plus spécifiquement sur cet axe de recherche comme par exemple le LGI2P avec lequel le LIRMM co-encadre la thèse de Frédéric Souchon.

Les autres demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …)

- Action COLOR (INRIA/LIRMM/I3S) **Protection dans les langages de programmation** – Année 2003 : l'objectif est de réaliser une plate-forme générique qui permettra de définir/spécifier les mécanismes de protection des langages de programmation et de vérifier que les applications décrites avec le langage choisi sont conformes (http://www-sop.inria.fr/oasis/Didier.Parigot/COLOR).

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : LIRIS

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	0,25	0,0	0,0	0,25
Fonctionnement (dont CDD décrits ci-dessous)	1,33	1,33	1,33	3,98
Total / année	**1,58**	**1,33**	**1,33**	**4,23**

Dépenses de personnels (CDD) [28]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	
Durée de l'emploi (en mois)[29]	0
Coût total de l'emploi	0

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[30]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[31]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	0	0	0	0

[28] Un tableau doit être rempli pour chaque demande de CDD.
[29] Doit être inférieure à 24 mois
[30] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[31] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

Les demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : LSR-IMAG

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	4,30	0,0	0,0	4,30
Fonctionnement (dont CDD décrits ci-dessous)	9,98	9,98	9,98	29,95
Total / année	**14,29**	**9,98**	**9,98**	**34,26**

Dépenses de personnels (CDD) [32]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	
Durée de l'emploi (en mois)[33]	0
Coût total de l'emploi	0

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[34]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[35]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	0	0	0	0

[32] Un tableau doit être rempli pour chaque demande de CDD.
[33] Doit être inférieure à 24 mois
[34] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[35] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

Tout comme pour le VALORIA, il sera intéressant pour ce partenaire de pouvoir expérimenter (soit par des études théoriques, soit par la mise en œuvre de mini-prototypes exploratoires) quelques solutions possibles avant d'envisager de les intégrer dans la plate-forme finale. Ainsi il sera très utile de pouvoir financer quelques stages de DESS ou de DEA pour réaliser ces travaux. Cela explique le montant plus important qui est demandé (le montant de 11 700€ contient seulement 9000€ pour les stages et 2700 € pour les autres besoins). Il serait bienvenu que l'on puisse rémunérer ces étudiants comme des vacataires plutôt qu'à travers une simple gratification de stage dont le montant (environ 350€ par mois), dissuade les bonnes candidatures.

Les autres demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

- Participation au réseau STIC-Génie Logiciel (programme franco-marocain, 2002-2005, http://www.univ-tlse2.fr/grimm/isycom/reseauSTIC/reseauSTIC.html) « *Conception et mise en œuvre de composants multi-vues — Application aux systèmes d'information* ».

- Participation au projet Centr'ACTOLL (ministère de l'industrie, 2001-2003, http://www adele.imag.fr/Les.Groupes/centractoll/) « *Construction d'une plate-forme logicielle de gestion du péage pour les réseaux de transports et les services urbains et interurbains* », dans le cadre duquel elle valorise ses compétences en composants.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

C1 - Demandes effectuées dans le cadre de l'ACI pour le présent projet :

Nom de l'équipe ou du laboratoire : Laboratoire VALORIA

Moyens demandés dans le cadre de la présente ACI (en K€ TTC) :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	3,22	0,0	0,0	3,22
Fonctionnement (dont CDD décrits ci-dessous)	8,17	8,17	8,17	24,51
Total / année	**11,39**	**8,17**	**8,17**	**27,73**

Dépenses de personnels (CDD) [36]**:**

Nature de l'emploi (post-doc, ingénieur, assistant-ingénieur,…)	
Durée de l'emploi (en mois)[37]	
Coût total de l'emploi	

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[38]	0	0	0	0
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	0	0	0	0
Nombre d'accueils en délégations ou détachements[39]	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	0	0	0	0

[36] Un tableau doit être rempli pour chaque demande de CDD.
[37] Doit être inférieure à 24 mois
[38] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.
[39] Certaines des demandes déjà faites pour 2003-2004 pourront être attribuées au titre de l'ACI.

Justifications scientifiques de l'ensemble des demandes :

Il sera intéressant pour ce partenaire de pouvoir expérimenter (soit par des études théoriques, soit par la mise en œuvre de mini-prototypes exploratoires), quelques solutions possibles avant d'envisager de les intégrer dans la plate-forme finale. Ainsi il sera très utile de pouvoir financer quelques stages de DESS ou de DEA pour réaliser ces travaux. Cela explique le montant plus important qui est demandé (le montant de 11 700€ contient seulement 9000€ pour les stages et 2700 € pour les autres besoins). Il serait bienvenu que l'on puisse rémunérer ces étudiants comme des vacataires plutôt qu'à travers une simple gratification de stage dont le montant (environ 350€ par mois), dissuade les bonnes candidatures.

Les autres demandes sont calculées *au prorata* des personnes impliquées. La justification de ces demandes est faite globalement dans la partie D de ce document.

C2 - Autres soutiens financiers apportés au projet :

On mentionnera les autres actions relatives au projet dans lesquelles l'équipe ou le laboratoire est engagé (projets européens, RNRT, RNTL, autres ACI, …).

- projet régional SCoT (Support de Composants Testables) (www.univ-ubs.fr/valoria/scot/) avec la Région Bretagne, l'IRISA et le GICAB

D - RECAPITULATIF GLOBAL DES DEMANDES DU PROJET :

Financements via le Fonds National de la Science :

	2003	2004	2005	Total
Equipement	27,76	0,0	0,0	27,76
Fonctionnement (dont CDD décrits ci-dessous)	50,55	155,44	103,00	308,99
Total / année	**78,31**	**155,44**	**103,00**	**336,75**

Dépenses de personnels (CDD) :

Nombre d'emplois	2
Durée cumulative des emplois (en mois)	36
Coût total des emplois	157,34

Financements via les organismes de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre de post-docs (préciser pour chaque demande la durée en mois)[40]	1	0	0	1
Nombre d'accueils de chercheurs étrangers (préciser pour chaque demande la durée en mois)	1 (3 mois)	2 (3 mois)	1 (3 mois)	4 (12 mois)
Nombre d'accueils en délégations ou détachements	0	0	0	0

Allocations de recherche :

	2003-2004	2004-2005	2005-2006	Total
Nombre d'allocations de recherche débutant en :	2	0	0	2

[40] Sauf demande argumentée, la durée d'un contrat de type post-doc ne pourra excéder 12 mois.

Action Concertée Incitative
SECURITE INFORMATIQUE
Descriptif complet du projet

Justification de la demande de financement (récapitulatif)

Frais de fonctionnement (hors personnel)

Dans ce chapitre de dépenses on distingue :

- Les missions de coordination utilisées pour permettre aux partenaires du projet de se réunir afin de coordonner les travaux menés par chacun tout au long du projet, et plus généralement de collaborer pour l'avancement des différentes tâches du projet. entre les partenaires. Nous prévoyons environ 2700 € (soit 3220 € TTC) par personne impliquée dans le projet (cf. partie A.2), afin qu'elles puissent participer à deux à trois réunions annuelles ainsi qu'à des réunions ponctuelles entre partenaires d'une même tâche.

- Les stages d'étudiants : plusieurs équipes souhaitent mettre en œuvre des prototypes intermédiaires. Cet aspect sera justifié pour chacun des partenaires concernés. Le montant de rémunération prévu est de l'ordre de l'ordre de 3000 € (soit 3576 € TTC) pour une durée de 6 à 10 mois. Nous souhaiterions (pour avoir des étudiants plus motivés) pouvoir payer les étudiants sur un tarif de vacation sur 6 mois plutôt que de leur donner une gratification de stage sur 10 mois.

- Le fonctionnement interne recouvre :
  - la publication de résultats dans des congrès et des revues : la participation aux congrès permettra à la fois de rencontrer d'autres chercheurs (en particulier ceux citées dans la partie B1), de présenter les articles relatifs à l'action ;
  - l'organisation de séminaires pour assurer la visibilité du projet ;
  - le paiement de fournitures ;
  - la formation interne ;
  - les autres frais divers.

  L'ensemble de ces frais représente le coût de fonctionnement du personnel qu'il soit permanent, engagé sur les fonds du projet, déjà en thèse (financement externe au projet) ou exerçant les fonctions d'ATER. Le montant demandé est donc proportionnel au nombre de personnes, à leur taux et à leur durée d'implication dans le projet. La règle est la même pour chaque partenaire, ce qui permet une répartition équitable (en fonction de l'effort fourni), mais en contrepartie, les montants diffèreront selon les partenaires. Le montant pour une personne durant une année effective a été fixé à 1500 € (soit 1788 € TTC).

- Les frais de gestion : ils concernent les prélèvements opéré par l'organisme auquel est rattaché un partenaire. Le montant représente en moyenne 10% du total des sommes reçues (hors frais de personnel).

Il est important de noter que l'ensemble des demandes concernant ces différents points sont, pour chaque partenaire, réparties également sur l'ensemble des trois années.

Frais de Personnel

En ce qui concerne le personnel nous avons besoin d'aide pour mener à bien le projet. Cette aide concerne principalement les deux points suivants :

- L'implémentation d'un prototype doit être considérée principalement comme un support de validation et de publication. Ce prototype s'appuiera sur SmartTools développé par l'INRIA ; il semble donc naturel qu'une grosse partie de l'implémentation soit réalisée par l'INRIA et c'est pour cela que nous demandons pour ce partenaire un CDD à partir de la 2ème année. Il est essentiel que la personne recrutée s'implique sur la durée (2 ans) et possède à la fois les qualités d'un ingénieur (implantation) et les qualités d'un chercheur (compréhension et mise en œuvre des idées développées par l'ensemble des partenaires). C'est pour cela que le profil est mixte ingénieur/chercheur.

- L'aspect recherche proprement dit concerne le besoin des équipes pour effectuer un travail de recherche en relation avec l'ACI :
  - deux partenaires (I3S et le LIRMM) ont besoin d'être soutenus et demandent chacun une bourse

de thèse pour travailler sur deux des trois problématiques de la sûreté traitées dans le cadre du projet : la " correction " pour l'un, et la " robustesse " pour l'autre ;

- deux partenaires ont déjà des étudiants en thèse ou qui viennent de la terminer ; elles veulent permettre au projet de bénéficier du savoir-faire de ces chercheurs (notamment pour la troisième problématique relative à " l'intégrité du code et des données "). Elles ont donc besoin pour chacun d'un poste de post-doc pour financer ces derniers : une demande de post-doc sous forme de CDD pour le LIRMM (personne pressentie Frédéric Souchon) et une autre sous forme de poste pour l'INRIA (personne pressentie Gilles Ardourel) ;

- enfin d'autres partenaires (Valoria, LSR-IMAG) ont besoin de stagiaires de DEA ou de DESS pour les aider ponctuellement dans leur travail de recherche, à la fois pour défricher des aspects spécifiques ou pour réaliser de mini-prototypes afin de faciliter les échanges avec le CDD chargé de l'implantation à l'INRIA.

Frais d'équipement

Les différents partenaires du projet ont besoin de l'informatique pour les différentes tâches (rédaction de rapports, développement, etc.). Ces demandes d'équipements permettent à la fois d'offrir une aide au renouvellement ou à la mise à jour du matériel informatique des différents partenaires, et également de fournir un poste de travail aux personnes accueillies par les partenaires (post-doc, stagiaires, CDD). Ces demandes concernent les besoins en équipement de l'ensemble du personnel qu'il soit, permanent, engagé sur les fonds du projet, déjà en thèse (financement externe au projet) ou exerçant les fonctions d'ATER. Comme nous l'avons fait pour " le fonctionnement interne ", le montant demandé est aussi proportionnel au nombre de personnes, à leur taux et à leur durée d'implication dans le projet. La règle est la même pour chaque partenaire, ce qui permet une répartition équitable (en fonction de l'effort fourni), mais en contrepartie, les montants diffèreront selon les partenaires. Le montant pour une personne durant une année effective a été fixé à 1000 € (soit 1192 € TTC). Pour plus d'efficacité nous avons planifié toutes les dépenses de matériel la 1ère année.

E - ENGAGEMENT DU COORDINATEUR DU PROJET :

La présente page ne sera remplie que dans la version sous forme papier.

Je soussigné, Didier Parigot, coordinateur du projet ROOF, m'engage dans l'hypothèse où le présent projet serait retenu à :

- fournir un rapport d'évaluation à mi-parcours permettant au Conseil Scientifique d'apprécier l'avancement des travaux et la coopération des équipes participantes.
- un rapport à la fin de l'exécution du projet.
- maintenir régulièrement une page web résumant l'ensemble des activités du projet.

Signature du coordinateur du projet :

Visa du Directeur du Laboratoire ou de l'Unité de Recherche auquel appartient le coordinateur du projet: