ACI Sécurité & Informatique

Fiabilité des Assemblages de Composants Répartis

FIACRE

Projet ACI Sécurité et Informatique, 2004-2007

Fiabilité des Assemblages de Composants Répartis

Modèles et outils pour l'analyse de propriétés de sûreté

Eric Madelaine

Fiacre
Fiabilité des Assemblages de Composants Répartis

Plan de la présentation

- Les enjeux (reprise 2004)
- Le projet FIACRE:
  - 1 : Langages de spécification, formats intermédiaires
  - 2 : Génération de modèles
  - 3 : Outils de vérification
- Zoom sur l'axe 2:
  - Génération de modèles comportementaux pour les composants distribués : la plateforme Vercors
- Perspectives

Fiacre
Fiabilité des Assemblages de Composants Répartis

Les enjeux (1)

(ACIs, Toulouse, nov 2004)

- Emergence et importance des composants répartis.
- Programmation par assemblage (COTS).
- Réduction des coûts de développement, et de validation (vérification à l'assemblage avant déploiement).

Fiacre
Fiabilité des Assemblages de Composants Répartis

Les enjeux (2)

- Spécification : comment être sûr qu'un composant « sur étagère » correspond aux besoins.

- Composition : un assemblage de composants élémentaires est-il cohérent ? Remplit-il les besoins pour lesquels il est créé ? Peut-on sans risque remplacer un composant dans une application existante ?

Situation actuelle : vérification de composants

- La spécification, et la vérification de compatibilité des composants sont actuellement réduits à la syntaxe et au typage statique
- Des outils de vérification de composants séquentiels ou multi-threadés existent :
  - Génération de modèles finis : Bandera (KSU), Java PathFinder (NASA), SLAM (Microsoft)
  - Vérification par assertions : MOBIJ (LIACS, Pays-Bas)
  - Modélisation et conception : Cadena (KSU)
- Mais les fonctionnalités permettant de vérifier les aspects “distribués” des assemblages de composants répartis sont peu nombreuses

Situation actuelle : vérification de composants

- La spécification, et la vérification de compatibilité des composants sont actuellement réduits à la syntaxe et au typage statique
- Des outils de vérification de composants séquentiels ou multi-threadés existent :
  - Bandera, Java PathFinder, SLAM, MOBIJ, Cadena (KSU)
- Mais les fonctionnalités permettant de vérifier les aspects “distribués” des assemblages de composants répartis sont peu nombreuses

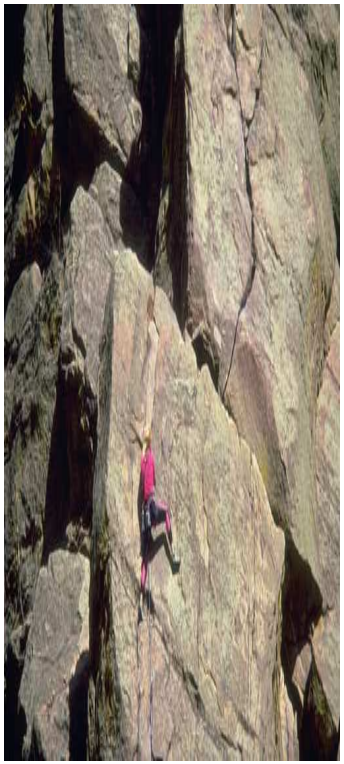
Fiacre
Fiabilité des Assemblages de Composants Répart

Situation actuelle : techniques de vérification de systèmes distribués

- Model checking
  - Exploration des états d'un modèle
  - Supporté par de nombreux outils (CADP, FC2, MEC, TINA, SPIN, nuSMV, Uppaal, etc.)
- Typage comportemental
  - Notion de contrat que doivent satisfaire les composants afin d'assurer un bon assemblage.
  - Pas d'outils
- Besoin d'une méthodologie et d'une chaîne complète d'outils pour l'application aux composants répartis
  - Spécification et vérification des propriétés
  - Maîtrise de l'explosion combinatoire

Fiacre
Fiabilité des Assemblages de Composants Répartis

Une barre à franchir



- Spécification des composants répartis :
  - Proposer un formalisme permettant la vérification compositionnelle: -> vérification « boite noire » des assemblages.
  - Modèles paramétrés et techniques d'analyse associées.
- Mettre ces méthodes à la portée du développeur d'applications :
  - Intégrer une chaîne complète d'outils automatiques.
- Diminuer la complexité de la vérification :
  - Nouveaux algorithmes, nouvelles représentations.

Le projet FIACRE

- projet OASIS, INRIA Sophia-Antipolis (coordinateur)
  - **Développement de la bibliothèque ProActive, sémantique comportementale, génération de modèles paramétrés et vérification pour applications distribuées.**
- projet VASY, INRIA Grenoble, Rhônes-Alpes
  - **Validation et vérification de systèmes asynchrones, développement de la boite à outils logiciels CADP basée sur les algèbres de processus et la logique temporelle.**
- SVF (fédération FERIA, Toulouse)
  - **Modèles pour la concurrence et la communication, techniques de vérification par ordre partiels, outils de vérification.**
- LTCI (CNRS - GET/ENST Paris)
  - **Comportements des composants distribués, contrats et typage comportemental.**

Fiacre
Fiabilité des Assemblages de Composants Répartis

Le projet Fiacre : Réalisations

Fiacre
Fiabilité des Assemblages de Composants Répartis

Axe 1 : Langages de Spécification, Formats Intermédiaires

- Modèle Sémantique: **pNets**

  (parameterized Networks of Labelled Transition Systems) [Forte '04]
- Langage Intermédiaire **FIACRE** (Format Intermédiaire pour les Assemblages de Composants Répartis Embarqués).

  Travail prolongé dans le cadre des projets Topcased (AESE) et OpenEmbeDD (RNTL)
- Logique **MCL**:

  mu-calcul modal régulier avec variables typées [en cours]
- **VCE** (Vercors Component Environment):

  diagrammes UML pour la spécification d'architecture et de comportement de composants répartis [Cocome'07, SCCC'07]

Fiacre
Fiabilité des Assemblages de Composants Répartis

Axe 2 : Génération de Modèles

- Environnement pour la spécification et le développement de composants répartis corrects.
  - Spécifications graphiques
  - Abstraction, génération de modèle intermédiaire, model-checking
- Génération de modèles pour les composants répartis (Fractal, GCM):
  - Sémantique comportementale des composants GCM [soumis]
  - Algorithmes de génération de modèles (pNets) pour composants répartis Fractal, pour composants asynchrones ProActive, pour composants reconfigurables GCM
  - Abstractions des domaines des paramètres
- Génération de code sûr pour composants répartis

Fiacre
Fiabilité des Assemblages de Composants Répartis

Axe 3 : Amélioration et nouvelles fonctionnalités des outils de vérification

TINA

Outils pour l'édition et l'analyse de réseaux de Pétri

- Vérification de systèmes avec *données, temps, et priorités*
- SELT: *LTL model-checker*
- Compilateurs pour RT/Lotos et V-Cotre

CADP

Boite à outils pour le développement et la validation de systèmes répartis:

- Nouveaux formats d'entrées: *réseaux d'automates synchronisés,*
- Génération automatique de contraintes d'environnement pour la vérification compositionnelle [Forte'06]. Amélioration de l'outil *projector*
- Méthodes paramétrées: *logique MCL* implantée dans l'outil CADP 4.0

Gateways

Disponibles: passerelles TINA <-> CADP à travers le format BCG

CADP traduit les réseaux d'automates en format pour TINA

En cours: format Fiacre (avril 2008)

Fiacre
Fiabilité des Assemblages de Composants Répartis

Zoom sur l'axe 2 :

Génération de modèles comportementaux pour les composants distribués

L'environnement VERCORS

Fiacre
Fiabilité des Assemblages de Composants Répartis

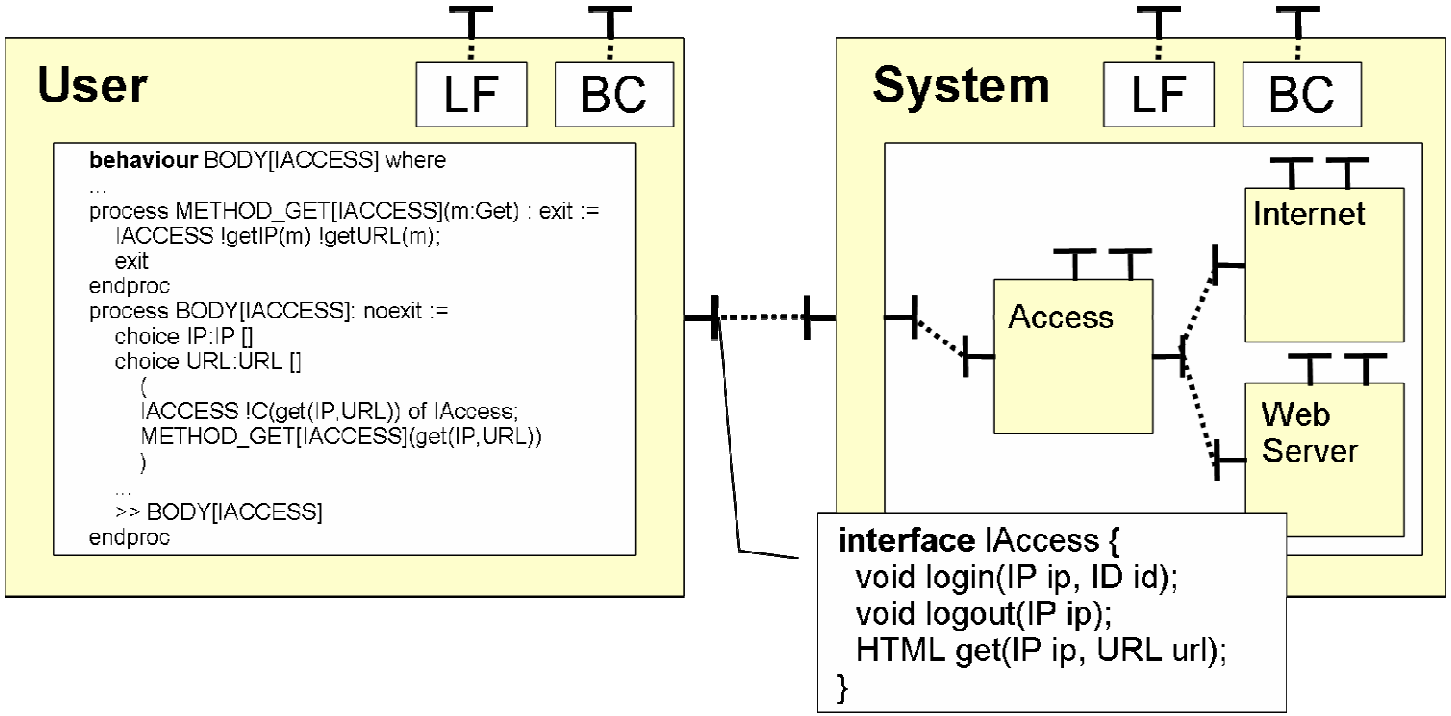
Motivations - Ambitions

- Assemblage correct de composants
  - Intégration des descriptions architecturales (ADL) et comportementales (pNets)
  - Compatibilité dynamique de l'assemblage, vérification de propriétés de logique temporelle
  - Aspects spécifiques des applications distribuées : asynchronisme, communication de groupe, reconfiguration.
- Spécification formelle des composants
  - Défi: fournir un outil de spécification et de vérification, accessible aux non-spécialistes
  - De l'analyse statique à la génération de code sûr

Fiacre
Fiabilité des Assemblages de Composants Répartis

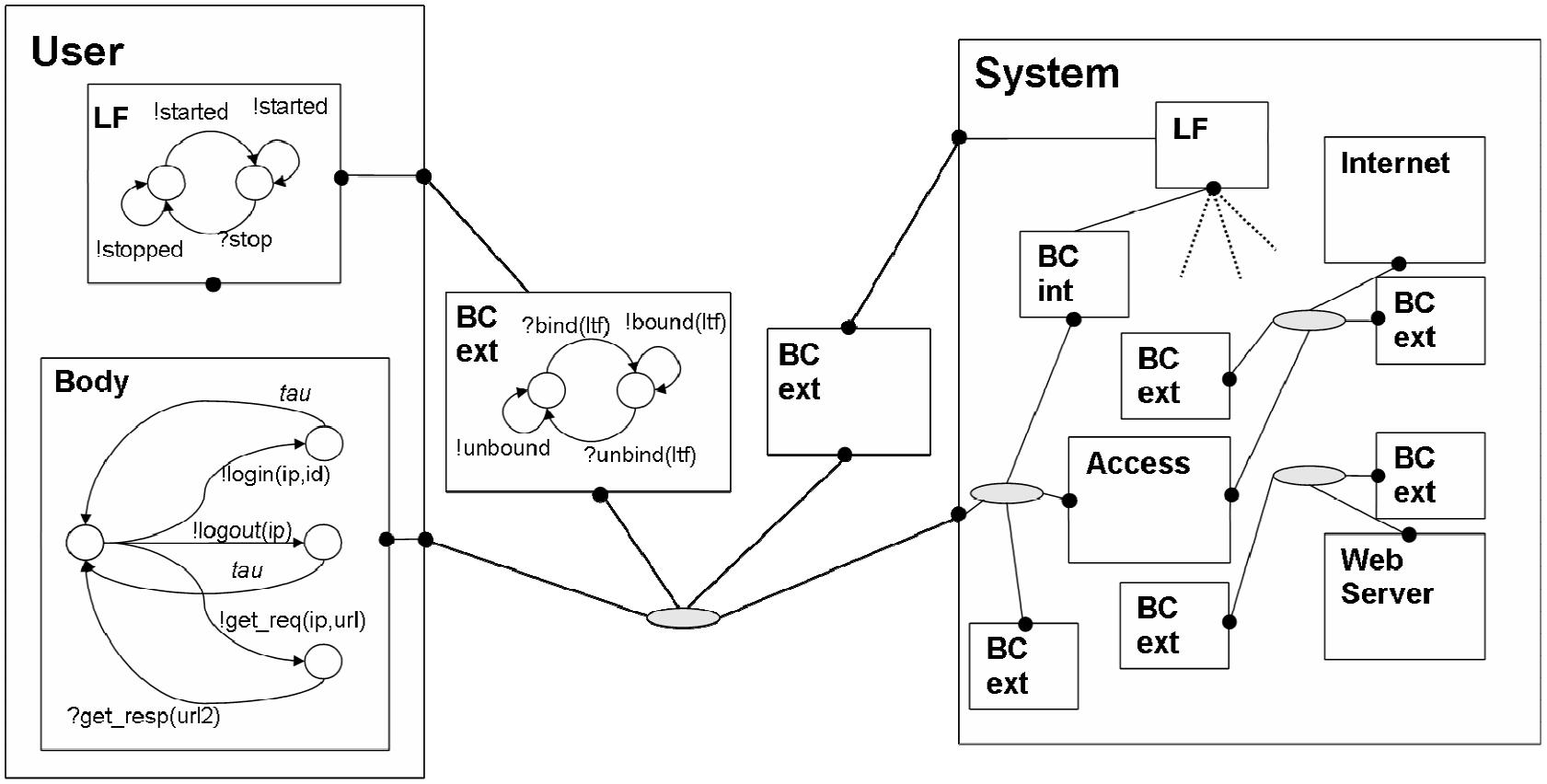
Fractal/GCM (Grid Component Model)

- Composants hiérarchiques, répartis, asynchrones, contrôle non-fonctionnel, communications pour la grille



Fiabilité des Assemblages de Composants Répartis

Modèle sémantique : Réseaux paramétrés d'automates synchronisés [Forte '04]



Fiacre
Fiabilité des Assemblages de Composants Répartis

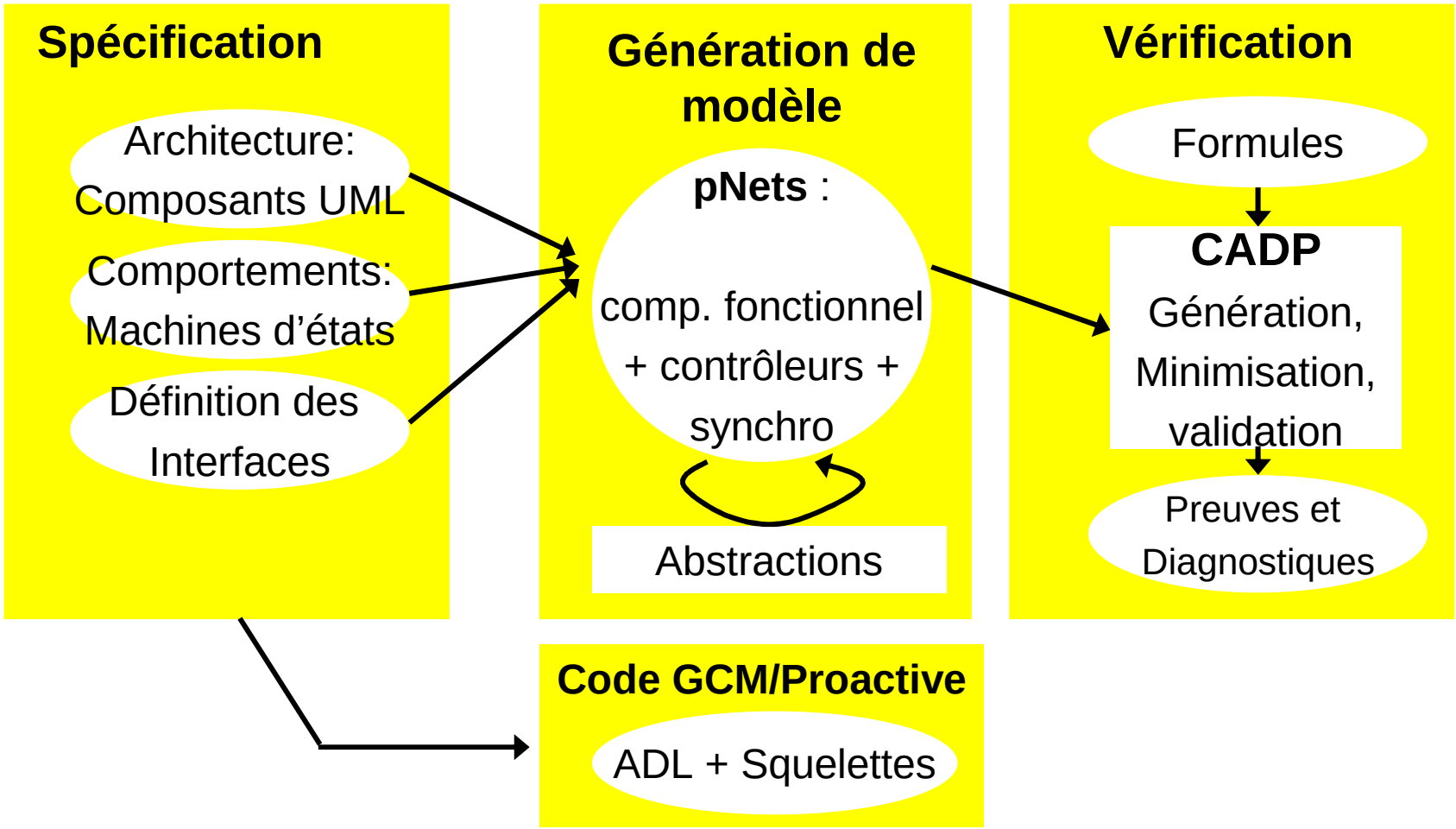
Modèle sémantique : Réseaux paramétrés d'automates synchronisés [Forte '04]

+ Structures hiérarchiques synchronisant des LTSs
+ Vecteurs de synchronisation d'Arnold-Nivat
+ Calcul avec passage de valeur à la Lin + topologies paramétrées
+ Reconfiguration à la Lotomaton

- Expressivité (codage simple des modes de communication de CCS, CSP, SCCS, Lotos, ELotos…)
- Bas niveau : adapté à la manipulation en machine
- Compact

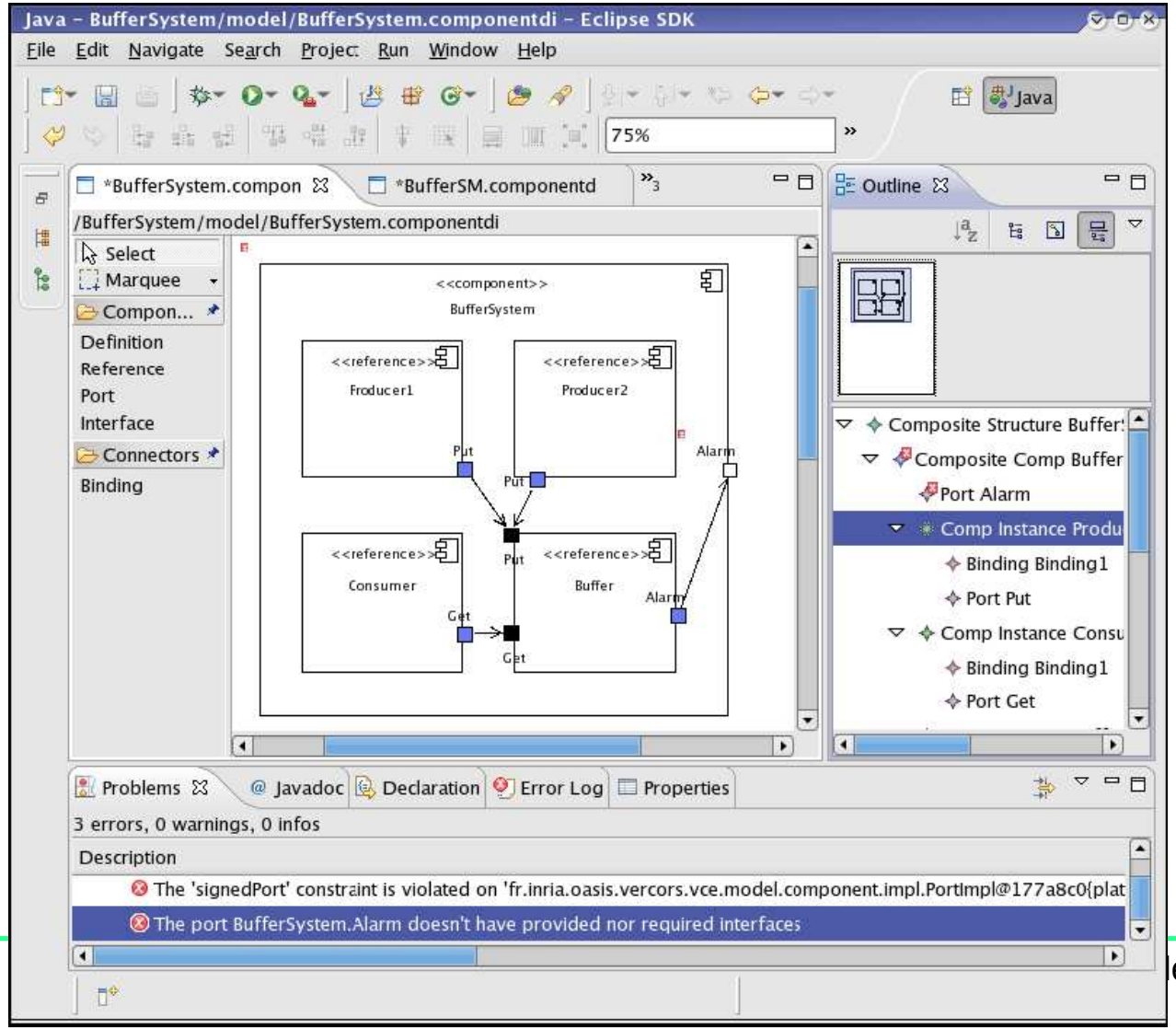
Fiacre
Fiabilité des Assemblages de Composants Répartis

Vercors: Architecture



Fiacre
Fiabilité des Assemblages de Composants Répartis

Environnement de spécification



- Diagrammes UML 2.0
- Composants hiérarchiques + machines d'états
- Plugins de validation et de passerelle vers CADP
- Intégré dans Eclipse.
- V0.5 disponible

Fiacre
Fiabilité des Assemblages de Composants Répartis

Génération de modèles

- Source: objects actifs [Forte'04], composants Fractal [Spin'05], composants GCM [Facs'06, Cocome'07]
- Vers le format **pNets**

- Prise en compte des données, (passage de valeurs et paramétrage de la topologie)
- Génération des contrôleurs non-fonctionnels de Fractal, => capacité de modéliser la reconfiguration
- Abstraction des types de données utilisateur

Fiacre
Fiabilité des Assemblages de Composants Répartis

Moteurs de vérification

- Boite à outils CADP:
  - Génération compositionnelle ou à la volée
  - Minimisation (forte ou de branchement)
  - Vérification de modèles (Evaluator)

- Améliorations durant le projet:
  - Format d'entrée "vecteurs de synchronisation" (Exp-open 2.0)
  - Génération distribuée d'espaces d'états
  - Ordres partiels: tau-confluence
  - Réduction contextuelle (Projector)

Fiacre
Fiabilité des Assemblages de Composants Répartis

Etudes de cas

- Fractal:

  Réseau Wifi d'aéroport (cas d'étude FT), partiellement spécifié et analysé avec Vercors, 4 niveaux de hiérarchie… [Facs'06]

- GCM/Proactive:

  CoCoME (Common Component Modelling Example), étude d'une infrastructure distribuée pour la gestion de caisses de magasins [Cocome'07]

  Interactions données/topologie, communications de groupe, espaces d'états de l'ordre de 10^6

Fiacre
Fiabilité des Assemblages de Composants Répartis

Génération de code

- Ecriture / Lecture de l'ADL Fractal/GCM
- Production de code pour les composants primitifs Java/ProActive, garanti respecter le comportement prouvé en Vercors:
  - méthodes implantant le comportement (runActivity)
  - méthodes des contrôleurs non-fonctionnels
  - squelettes des méthodes implantant les services offerts.

Fiacre
Fiabilité des Assemblages de Composants Répartis

Vercors: Conclusions et Perspectives

- A court terme :
  - Extension de l'outil pour la spécification de composants GCM (profile UML spécifique)
  - Génération de code garanti correct
- A long terme :
  - Modélisation spécifique des structures de communication asynchrone (queues de requètes, proxies de futures)
  - Prise en compte des communications de groupe (interfaces Multicast / Gathercast)
  - Spécification des aspects non-fonctionnels des composants (reconfiguration, autonomicité)
  - Intégration dans l'environnement de développement ProActive

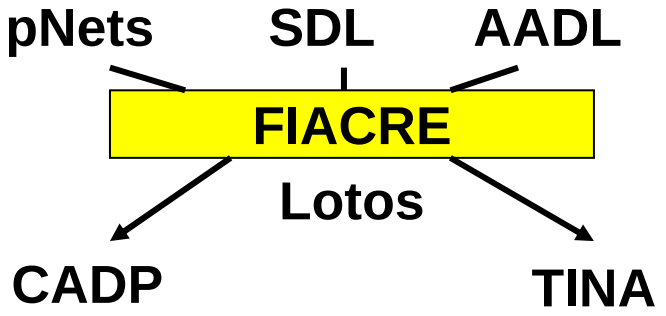
Fiacre
Fiabilité des Assemblages de Composants Répartis

Projet Fiacre : Conclusions

- Sur le plan scientifique
  - ~ 40 articles confs/workshops internationaux
- Sur le plan technique
  - Améliorations des boites à outils de vérification
  - Prototype du VCE
  - Inclusion dans les standards Fractal et GCM
- Nouveaux défis
  - Reconfiguration des systèmes à base de composants :
  - Grilles : systèmes de grande taille, parallèles, P2P, etc.

Collaborations et prolongements

- Les outils de la plateforme Vercors sont utilisés, et leur développement continue, dans le cadre du NOE **CoreGrid** et du projet FP6 **GridComp**.
- Les travaux sur la logique temporelle avec données sont prolongés dans le cadre du projet de pôle de compétitivité (AESE) **Topcased**.
- Le développement des techniques de vérification compositionnelle est prolongé dans le cadre du projet de pôle de compétitivité (Minalogic) **Multival**.
- Le développement du langage Fiacre continue dans le cadre de **Topcased** et de **OpenEmbeDD**:



Fiacre
Fiabilité des Assemblages de Composants Répartis

Bibliographie abrégée

- **SCCC'07** "*Specifying Fractal and GCM Components With UML*." Iquique, Chile, Nov. 2007. IEEE.
- **CAV'07** "*CADP 2006: A Toolbox for the Construction and Analysis of Distributed Processes*".
- **FMOODS'06** "*Bounded Analysis and Decomposition for Behavioural Descriptions of Components*", Bologna, June 2006.
- **STTT #8(1)'06** "*CAESAR_SOLVE: A Generic Library for On-the-Fly Resolution of Alternation-Free Boolean Equation Systems*".
- **FACS'06** "*Model Checking Distributed Components: the Vercors Platform*", Prague. Sept 2006
- **SPIN'06** *"Distributed on-the-fly model checking and test case generation".*
- **ERTS'06** "*Behavioural descriptions in architecture description languages: Application to AADL",* Toulouse, jan 2006
- **FORTE'06** "*Refined Interfaces for Compositional Verification",* Paris, 2006
- **TACAS'05** "*Bisimulator: A modular tool for on-the-fly equivalence checking*"

Fiacre
Fiabilité des Assemblages de Composants Répartis

http://www-sop.inria.fr/oasis/fiacre