

ACADiE :

Assistance à la Certification d'Applications
Distribuées et Embarquées

Permanents (11) Doctorants (10)

Permanents	Doctorants
Jean-Paul Bodeveix	Julien Brunel
Xavier Crégut	Benoît Combemale
Mamoun Filali	Pierre-Loïc Garoche
Marcel Gandriau	Nassima Izerrouken
Ousmane Kone	Tanguy Le Berre
Philippe Mauran	Odile Nsar
Gérard Padiou	Li Pei
Marc Pantel	Nadège Pontisso
Philippe Quéinnec	Miloud Rached
Martin Strecker	Jean-François Rolland
Xavier Thirioux	

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Méthodes formelles

- Développement de langages d'architecture (COTRE, TOPCASED, SPICES, OpenEmbeDD).
 - transformation vers des cibles de vérification,
 - transformation vers des cibles d'exécution,
 - transformation vers des cibles de test.
- Validation de transformations (TOPCASED, SPACIFY, GENEAUTO).
 - approche fonctionnelle (Isabelle, Coq),
 - approche machine abstraite (B),
 - approche réécriture d'arbres (ASF/SDF),
 - approche grammaire et réécriture de graphes (AGG).
- Etude de propriétés de langages dédiés (CORSS).
 - Description d'ordonnanceurs (BOSSA),
 - description de services téléphoniques.

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Méthodes formelles

- Développement de langages d'architecture (COTRE, TOPCASED, SPICES, OpenEmbeDD).
 - transformation vers des cibles de vérification,
 - transformation vers des cibles d'exécution,
 - transformation vers des cibles de test.
- **Validation de transformations (TOPCASED, SPACIFY, GENEAUTO).**
 - **approche fonctionnelle (Isabelle, Coq),**
 - **approche machine abstraite (B),**
 - **approche réécriture d'arbres (ASF/SDF),**
 - **approche grammaire et réécriture de graphes (AGG).**
- Etude de propriétés de langages dédiés (CORSS).
 - Description d'ordonnanceurs (BOSSA),
 - description de services téléphoniques.

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Méthodes formelles

- Développement de langages d'architecture (COTRE, TOPCASED, SPICES, OpenEmbeDD).
 - transformation vers des cibles de vérification,
 - transformation vers des cibles d'exécution,
 - transformation vers des cibles de test.
- Validation de transformations (TOPCASED, SPACIFY, GENEAUTO).
 - approche fonctionnelle (Isabelle, Coq),
 - approche machine abstraite (B),
 - approche réécriture d'arbres (ASF/SDF),
 - approche grammaire et réécriture de graphes (AGG).
- **Etude de propriétés de langages dédiés (CORSS).**
 - **Description d'ordonnanceurs (BOSSA),**
 - **description de services téléphoniques.**

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Sémantique et analyse statique

- Analyse statique système embarqué asynchrone réparti en Java
 - Maîtrise des aspects dynamiques de Java
 - Expression des aspects répartis asynchrones
- Analyse statique par aspects
 - séparation des considérations sémantiques
 - abstraction séparée des aspects
 - tissage des sémantique abstraite
 - combinaison de sémantiques
- Expression sémantique niveau méta-modèle
 - Axiomatique : Validation des modèles
 - Dénotationnelle : Transformation de modèles
 - Opérationnelle : Exécutabilité des modèles
 - Formalisation
méta-modèles/transformations/vérifications
 - Ingénierie définition des sémantiques d'un méta-modèle
 - TOPCASED : simulation des modèles/animation des modèles
 - Exemple : processus de développement

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

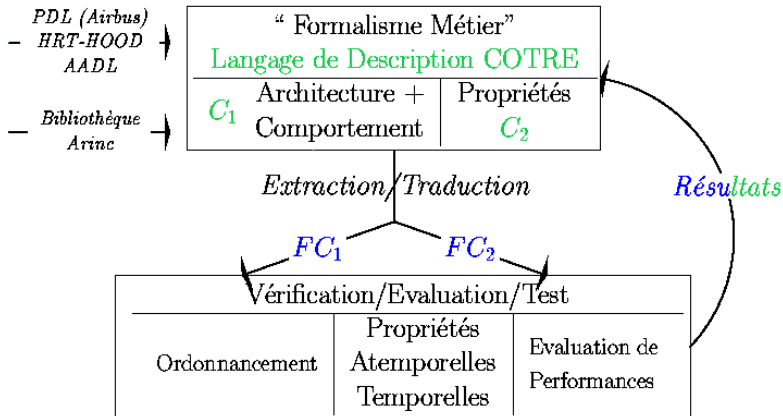
Théorie de la démonstration et du calcul

- Coercions et sous-typage.
- Théorie de la démonstration appliquée à la vérification de la commutativité de diagrammes catégoriques.
- Preuve modulo.
- Isomorphisme de types, invertibilité de termes et leurs applications:
 - recherche de données,
 - pérennité et accessibilité de l'information électronique.
- **Modèles catégoriques pour l'IDM (grammaire de graphes, réécriture de graphes, logiques adaptées)**

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Le projet Cotre

Consortium: AIRBUS, TNI, ENST Bretagne, SVF-FÉRIA.



SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Objectifs

Langage de description d'architectures temporisées

- Architecture hiérarchisée.
- Constructions temporisées.

Vérification de propriétés d'un système ordonnancé

- contexte asynchrone: les propriétés sont en général exprimées et vérifiées sur un système isolé.
- Différents types de propriétés:
 - sûreté, vivacité.
 - temporisées.

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Problèmes abordés

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

- Logique temporisée.
- Composants et comportements paramétrés.
- Logique paramétrée.
- Expression de la préemption.

Approche incrémentale

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

- Aspect temporisé ignoré.
- Parallélisme maximal: autant de processeurs que de processus.
- Introduction d'un ordonnanceur.
- Prise en compte du partitionnement temporel (Système ARINC).
- Introduction de la répartition (non traité).

Vérification d'un système en présence d'un ordonnanceur

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

- Structure du système ordonnancé.
- Spécification d'ordonnanceur.
- Modélisation d'ordonnanceur (préemptif).
- Application au partitionnement.

Vérification de la méthode de modélisation

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

But: Validation de l'expression en automates temporisés d'un ordonnanceur préemptif

- Modèle B abstrait d'un ordonnanceur.
- Introduction à l'aide de raffinements des aspects temporisés.
- Elimination des chronomètres: introduction d'horloges.

Annexe comportementale AADL

première version pour AADL 0.95: par P. Farail et P. Gauffillet.

seconde version: collaboration FÉRIA, AIRBUS, P. Dissaux (TNI-EUROPE).

- Associer un comportement aux threads et aux sous programmes.
- Modes de synchronisation inspirés de HRT-HOOD.
- Définition de propriétés métier et logiques.

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Vérification de transformations

Chaîne de traduction Cotre.

Principe: composition de transformations «élémentaires».

- Elimination des constructions structurelles.
- Transformations vers un noyau «temps réel».

$$T = [T_1; \dots; T_n]$$

- $T_{\text{smv}} = [T_1^s; \dots; T_n^s]$
- $T_{\text{uppaal}} = [T_1^u; \dots; T_n^u]$
- $T_{\text{tts}} = [T_1^t; \dots; T_n^t]$

Prise en compte des aspects génériques

Partage de transformations

Langages pivots

Langages de transformations basés QVT

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

- En général, il n'y a pas ou peu de support pour vérifier que les modèles cibles générés seront corrects.
- Pas de support pour vérifier les propriétés des transformations.

Langages de transformations basés QVT

⇒ trois études:

- approche basée sur la logique d'ordre supérieur (Isabelle/HOL) ou calcul des constructions (Coq)
 - Correction des modèles cibles établies par typage.
 - Specification des transformations: théorème HOL/Coq.
- approche basée sur la théorie des ensembles (B)
 - Correction des transformations établies par des obligations de preuve.
 - Specification des transformations: preuve de raffinement.
- approche basée sur les grammaires et la réécriture de graphe
 - Expression des méta-modèles par des grammaires de graphe
 - Expression des transformations de modèles par la réécriture de graphe
 - Codage dans des assistants de preuve (approche co-inductive, par arbre couvrant et liens, définition mathématique usuelle)

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Validation de règles de transformations ATL

En général, on ne peut pas vérifier qu'un modèle cible est correct.

- Spécification des langages de méta-modélisation (MOF/Ecore/KM3/...) de transformation (ATL/...)
- Définition de règles de correction
- Génération des obligations de preuve
- Coopération avec un assistant de preuve

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL

Sémantique des méta-modèles

- Besoin : Formaliser langages modélisation pour validation (transformation, simulation, vérification, ...)
- Études amonts : outils théoriques pour modélisation
- Ingénierie : moyens/processus de construction et de validation des sémantiques
- Application : sémantique des processus de développement
 - exécution/supervision/simulation (ATL, Kermeta, Java, ...)
 - validation modèles (OCL, réseau Petri, ...)
 - génération interface outils
 - validation transformations

Groupe de travail SéMO

- Sémantique des (méta-)modèles
- Atelier SéMO lors de IDM'07
- Synthèse RTSI/L'objet
- Proposition : Création d'un groupe de travail Action-IDM/portail WEB
- Concrétisation : Rédaction d'un livre blanc sur pré-occupation sémantique dans l'IDM

SÛRETÉ
DE DÉVELOPPEMENT
DU LOGICIEL