Application BASTRI
Fiches Equipes

MOSEL (SR0057ZR)

Développement prouvé de systèmes informatiques
MOSEL VERIDIS (SR0426IR)

Statut: Terminée

Responsable : Dominique Méry

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Programmation, vérification et preuves

Période : 01/02/2004 -> 31/12/2008
Dates d'évaluation :

Etablissement(s) de rattachement : U. DE LORRAINE, CNRS
Laboratoire(s) partenaire(s) : LORIA (UMR7503)

CRI : Centre Inria de l'Université de Lorraine
Localisation : Bâtiment Ada Lovelace - Centre Inria de l'Université de Lorraine
Code structure Inria : 051023-0

Numéro RNSR : 200418303G
N° de structure Inria: SR0057ZR

Présentation

L'objectif de l'équipe-projet est l'étude de techniques et la réalisation d'outils, pour concevoir des systèmes sûrs, vivaces et équitables. Les moyens d'expressions des modèles et des propriétés sont les systèmes de transition, en particulier à évènements comme B système et les logiques temporelles, comme TLA+. La vérification et la validation des propriétés sont obtenues par la preuve automatique ou interactive et l'exploration algorithmique de modèles. Ces techniques de vérification sont complémentaires et s'appuient dans notre équipe-projet sur le raffinement et l'abstraction.

L'originalité de l'approche réside d'une part, dans la combinaison de ces deux types de techniques de vérification, en utilisant le raffinement et l'abstraction, pour limiter l'explosion combinatoire de l'exploration algorithmique de modèles et augmenter le taux de preuve automatique et d'autre part, dans l'intégration du raffinement dans le processus de développement des systèmes. En particulier, le travail s'appuie sur les diagrammes de prédicats, qui permettent d'abstraire les systèmes modélisés, notamment les systèmes répartis, et d'associer les techniques de vérification exhaustive de type model checking et les techniques de raffinement; ils constituent une première illustration de notre équipe-projet.

Axes de recherche

- FONDEMENTS ET MÉTHODOLOGIE: *étude du développement incrémental prouvé de systèmes, ingénierie de la preuve, raffinement et abstraction de modèles de systèmes spécifiques*.
  Cet axe concerne à la fois des travaux d'expérimentations et de formalisations à partir d'études de cas; il intègre la preuve dans le développement de modèles abstraits et l'étude des systèmes dans le cadre d'un développement assisté par la preuve. Les systèmes complexes sont des systèmes incluant des parties logicielles et dont la taille ne permet pas une maîtrise sans faille par des méthodes plutôt empiriques. Cette maîtrise des systèmes dits «complexes» est un enjeu considérable, dans la mesure où les systèmes intègrent de plus en plus de composants logiciels.

- NOTATIONS ET OUTILS: *étude des diagrammes de prédicats, intégration avec des approches semi-formelles (en particulier, UML)*
  Cet axe se focalise sur une vision unifiée du cadre de développement et se focalise sur les techniques à mettre en oeuvre, notamment les diagrammes de prédicats contribuant à unifier les techniques de vérification et de développement. Des travaux concernant UML sont

Contact

- **Responsable :** Dominique Méry
- **Tél :** 03.83.59.20.19
- **Secrétariat Tél :** 03.83.59.30.65

En savoir plus

- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité :

Documents sur la structure

- Intranet
- Privés

Décisions

- 4029 (09/02/2004) : création
- 5789 (11/09/2007) : prolongation
- 6496 (06/02/2009) : fermeture

Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, Bâtiment Ada Lovelace, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157

envisagés et visent à intégrer le raffinement dans le cadre du langage UML.

- APPLICATIONS: les applications sont développées dans le cadre d'actions de recherche: le développement de systèmes matériel/logiciel (*RNRT EQUAST*), les diagrammes de prédicats (*opération DIXIT du PRST IL QSL*), les outils de validation formelle (*opération ADHOC du PRST IL QSL*), l'analyse formelle d'UML (*projet HUGO avec Munich*).

Logiciels

- Click?n?Prove

Relations industrielles et internationales

- Participation au projet RNRT EQUAST en partenariat avec TDF, Thalès, LIEN-UHP
- Collaboration avec des chercheurs de l'Université de Munich nous étudions des logiques pour la représentation de systèmes mobiles et l'application du model checking aux modèles UML.
- Travaux en commun avec ClearSy et J.-R. Abrial sur le B évenementiel et sur les outils (Balbulette)