Application BASTRI
Fiches Equipes

ABSTRACTION (SR0091IR)

Interprétation abstraite et analyse statique
ABSTRACTION

Statut: Terminée

Responsable : Xavier Rival (Par intérim)

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Preuves et vérification

Période : 01/01/2008 -> 31/12/2013
Dates d'évaluation : 22/03/2011

Etablissement(s) de rattachement : CNRS, ENS PSL
Laboratoire(s) partenaire(s) : DI-ENS (UMR8548)

CRI : Centre Inria de Paris
Localisation : Ecole Normale supérieure Paris
Code structure Inria : 021083-1

Numéro RNSR : 200818329T
N° de structure Inria: SR0091IR

Présentation

Problématique scientifique
Une erreur dans un logiciel critique peut avoir des conséquences humaines ou économiques catastrophiques, en particulier pour les systèmes embarqués. Il est donc particulièrement important de s'assurer que de tels logiciels sont sûrs avant de les mettre en service. ABSTRACTION développe des techniques d'interprétation abstraite, permettant de calculer statiquement une sur-approximation des comportements des logiciels analysés. L'analyse statique par interprétation abstraite est sûre (en cas de réussite, le logiciel analysé est effectivement prouvé correct) mais incomplète (dans certains cas, la recherche de preuve peut échouer à cause des problèmes d'indécidabilité et conduire à de fausses alarmes). En spécialisant l'analyse pour des familles de programmes bien définies, il est possible d'éliminer les fausses alarmes.

Dans ce contexte, les objectifs d'ABSTRACTION consistent à :

- formaliser des modèles sémantiques des programmes et des propriétés à prouver ;
- développer des abstractions adaptées, permettant à la fois un calcul rapide et précis, c'est-à-dire permettant la preuve effective des propriétés souhaitées ;
- implémenter et valider ces techniques par l'analyse de logiciels industriels ;
- rendre possible l'industrialisation de telles techniques à moyen terme.

Les thématiques actuelles concernent plus spécifiquement l'analyse statique précise de logiciels synchrones, quasi-synchrones et asynchrones, de systèmes biologiques et de protocoles cryptographiques.

Logiciels développés
• **ASTRÉE :** analyseur visant à prouver l'absence d'erreurs à l'exécution dans des programmes embarqués de type contrôle/commande avionique écrits en C.

• **ProVerif et CryptoVerif :** outils visant à prouver la sécurité de protocoles cryptographiques.

Fait marquant
Le logiciel **ASTRÉE** est utilisé pour la vérification d'absence d'erreurs à l'exécution dans les logiciels embarqués de commande de vol électrique.

Axes de recherche

Contact

- **Responsable :** Xavier Rival
- **Tél :** 01.44.32.20.64
- **Secrétariat Tél :**

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 6153 (08/04/2008) : création
- 8339 (19/01/2012) : prolongation
- 8946 (13/11/2012) : nomination responsable
- 9321 (05/04/2013) : renouvellement responsable
- 9849 (13/01/2014) : fermeture

Localisation

- **Adresse postale :** École Normale supérieure 45 rue d'Ulm 75005 Paris France
- **Coordonnées GPS :** 48.841898, 2.345021

Logiciels

- ASTREE
- ProVerif
- CryptoVerif

Relations industrielles et internationales

- Contrats : projets européens, contrats ACI, ANR et RNTL, contrats industriels.
- Collaborations industrielles : Airbus France, Astrium Transportation, Esterel Technologies, etc.
- Collaborations académiques : Universités de Berkeley, Harward, Vérone, École Polytechnique, École Normale Supérieure de Cachan.
- Enseignement : École Normale Supérieure, École Polytechnique, Master Parisien de Recherche en Informatique.