

Sixième appel à propositions
«METHODES DE VERIFICATION DES LOGICIELS ET SYSTEME»
publié le 10 juin 2008

Résumé des 5 projets retenus pour financement

Mise en ligne : vendredi 12 décembre 2008

Rappel : La décision de financement de ces projets est conditionnée par la validation des budgets des projets, par les résultats de l'analyse financière des partenaires privés et par la fourniture par chaque partenaire des informations administratives et financières nécessaires.

La liste des projets définitivement financés par la FNRAE sera rendue publique au terme des instructions administrative et financière.

ALPROSE

Architecture et Langage pour la PROgrammation et la vérification de Systèmes perceptifs Embarqués

Ce projet vise à définir une architecture informatique à déclenchement par le temps qui permette de vérifier formellement des propriétés importantes d'un système en particulier la garantie du maintien des échéances temporelles. Les systèmes ciblés sont des systèmes perceptifs embarqués à bord de petits drones. Ces systèmes impliquent des composants très variés, tout en imposant des contraintes extrêmement fortes en embarquement, sûreté et fonctionnement temps réel. L'architecture développée doit supporter l'ensemble des composants de ces systèmes perceptifs. Le projet vise également la définition d'un langage formel permettant de décrire les spécifications logiques et temporelles imparties aux différents applicatifs embarqués. Il vise à vérifier par calcul si l'exécution des applicatifs peut se conformer aux spécifications. Les applicatifs sont alors exécutables et le contrôle de l'exécution est produit par les compilateurs.

Partenaires :

ONERA/DTIM

Coordonnateur et contact :

Bruno d'AUSBOURG
Bruno.d.Ausbourg@onera.fr

Durée :

36 mois

Date de démarrage :

TBD

ASCERT

Analyses Statiques CERTifiées

Nous proposons d'étudier la certification formelle des analyses statiques en utilisant l'assistant de preuve Coq. Nous aborderons plusieurs techniques permettant de démontrer mécaniquement la validité sémantique du diagnostic d'un analyseur : programmation certifiée correcte de l'analyseur, certification d'un vérificateur de résultat et validation déductive des invariants générés par un analyseur. Nous étudierons plusieurs composants clés de l'analyseur Astrée. Notre première tâche se consacrera à la certification des opérateurs de la bibliothèque de domaines abstraits Apron. Nous étudierons ensuite un interpréteur abstrait avant/arrière pour un langage impératif simple. Enfin nous relierons cet interpréteur à une des sémantiques formelles de C, développés dans le projet CompCert. Tous ces objectifs ont pour ambition commune de pouvoir, au terme du projet, évaluer le coût d'une certification formelle d'un tel analyseur.

Partenaires :

CR INRIA Rennes

École Normale Supérieure, équipe "Sémantique et interprétation abstraite" (P. Cousot, R. Cousot, L. Mauborgne)

Coordonnateur et contact :

David PICHARDIE

david.pichardie@irisa.fr

Durée :

36 mois

Date de démarrage :

TBD

CAVALE

Combinaison d'Analyses pour la VALidation des Logiciels Embarqués Acronyme

La vérification de code embarqué critique est aujourd'hui essentiellement effectuée par analyse dynamique sous la forme de jeux de test. Les méthodes formelles d'analyse statique seront amenées à jouer un rôle de plus en plus important, compte tenu de l'augmentation de la taille des systèmes ainsi que des exigences de certification. Chaque méthode (interprétation abstraite, preuve de propriété par calcul de plus faible précondition, etc) possède ses forces et ses faiblesses propres et nécessite une mise en œuvre spécifique. L'objectif de ce projet est double. Il s'agit d'une part d'étudier et de proposer un cadre pour la collaboration d'analyses statiques afin d'en améliorer la précision et d'en faciliter le passage à l'échelle; et d'autre part de permettre une intégration harmonieuse de ces analyses dans les processus de validation et vérification utilisés actuellement.

Partenaires :

ONERA/DTIM/ISC
IRIT-CNRS

Coordonnateur et contact :

Pierre-Loïc GAROCHE
pierre-loic.garoché@onera.fr

Durée :

36 mois

Date de démarrage :

TBD

QUARTEFT

Qualifiable Real Time Fiacre Transformations

Les nouvelles chaînes de développement de systèmes critiques reposent sur des langages de modélisation spécifiques au métier ciblé et sur des transformations qualifiées (assurance que la transformation préserve les propriétés d'intérêts) entre langages. Le projet FIESTA vise à développer les technologies pour faciliter cette approche dans le contexte des systèmes embarqués temps-réel. Il s'appuie d'une part sur la définition de langages pivots dédiés et sur l'exploitation de techniques formelles pour prouver la correction des transformations. L'étude proposée s'appuie sur le langage FIACRE, un des langages pivots pour la vérification formelle des aspects temps-réel dans le projet TOPCASED (<http://www.topcased.org>) ; il factorise et optimise la chaîne de traduction entre les langages "métier" tels que SDL, AADL, ... et les outils de vérifications de modèles tels que TINA et CADP. Cette proposition vise à renforcer cette approche sur deux aspects complémentaires : d'une part, définir des extensions de FIACRE lui permettant de prendre en compte de façon native des concepts de haut niveau tels que les modes, les notions de partitionnement temporel, les constructeurs temps-réel; et d'autre part développer les techniques de validation et vérification des transformations de FIACRE étendu (nommé RT-FIACRE) vers FIACRE et les outils de vérification pour disposer d'une chaîne sûre complète allant des outils de modélisation métier aux outils de vérifications.

Partenaires :

LAAS-CNRS groupe OLC
IRIT
ONERA-DTIM
INRIA Grand Est
AIRBUS France
Ellidiss (PME)

Coordonnateur et contact :

François VERNADAT
Francois.Vernadat@laas.fr

Durée :

36 mois

Date de démarrage :

TBD

SARDANES

Sémantique, Analyse et tRansformation Des Applications Numériques Embarquées
Synchrones

SCADE est un langage largement utilisé pour le développement de systèmes embarqués critiques synchrones. D'abord utilisé pour la spécification, la simulation et la vérification de propriétés de sûreté de haut niveau, ce langage permet aussi de produire un code final via un processus de compilation. Il est alors légitime que l'utilisateur souhaite que les propriétés prouvées sur le modèle soient garanties pour le code objet. Actuellement, le principal obstacle à cela est que la sémantique de SCADE spécifie que les calculs sont effectués en nombres réels. Or le programme final utilise des nombres flottants dont l'arithmétique est très différente de celle des réels, notamment à cause des erreurs d'arrondi. Le but de ce projet est d'utiliser des techniques de transformation d'expressions tenant compte de la précision des calculs pour garantir la préservation des propriétés numériques lors de la compilation de SCADE. Les preuves de correction reposent sur une interprétation abstraite des différentes traces d'exécution obtenues.

Partenaires :

*Université de Perpignan / Laboratoire ELIAUS-DALI
Ecole Normale Supérieure*

Coordonnateur et contact :

Matthieu MARTEL

Durée :

36 mois

Date de démarrage :

TBD