MORSE : Méthodes et Outils pour la vérification formelle de Systèmes intéropérables Embarqués critiques

2002
Précompétitif

Objectifs

- Fournir une méthodologie et des outils prototypes pour le développement d'applications **industrielles certifiables** caractérisées par les contraintes suivantes :
  - *exigences de **fiabilité***
  - *nécessité de **certifier** l'application*
  - *exécution dans un environnement **réparti***
  - *communications **asynchrones***
  - *utilisation du standard de spécification UML*
- Application au domaine des **drones**

Innovation & Points forts

- Exploiter des **méthodes formelles** dans le cadre d'une méthodologie utilisant UML
- Centrer le développement **sur un modèle pivot**, servant de base à la vérification formelle et à la synthèse automatique de programmes répartis
- Allier deux techniques de vérification **automatisables** :
  - méthodes **structurelles** (pas de construction de l'espace d'états) avec les réseaux de Petri
  - **vérification de modèle** (évaluation de formules sur l'espace d'états) avec les Diagrammes de Décisions de Données (DDD)
- Le LIP6 diffuse depuis plusieurs années un AGL de vérification formelle basé sur les réseaux de Petri
- Le LaBRI développe de nouvelles techniques de représentation d'espaces d'états extrêmement compactes (technologie DDD)

Retombées

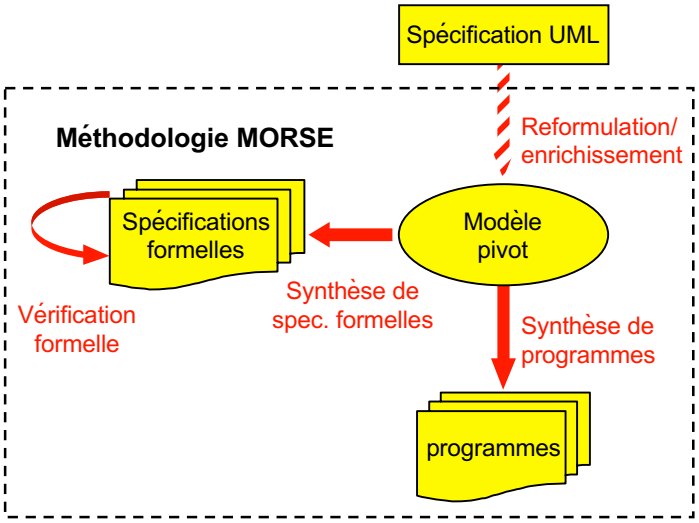
- Augmenter significativement la fiabilité des logiciels embarqués critiques asynchrones
- Compenser l'absence de présence humaine à bord (autonomie)
- Compléter la gamme des Ateliers de Génie Logiciels déjà existants
- Se rapprocher du «zéro-faute» pour toute application requérant de la sécurité, dont le logiciel est réparti et fonctionne à travers un réseau (drone, automobile, etc.)

Partenariat

- SAGEM SA est un pionnier mondial de la certification aéronautique des drones (unique au monde)
- Aonix est un leader mondial dans la fourniture de produits et conseil pour les systèmes critiques
- Le LIP6 (thème SRC) est un expert dans la modélisation et la vérification de systèmes répartis intéropérables
- Le LaBRI est un expert dans les techniques de vérification symboliques

Principes de base

- La méthodologie s'appuie sur le schéma suivant :
  - *enrichissement/reformulation d'une spécification UML pour retirer les ambiguïtés dans la description du comportement. Le résultat est le modèle pivot.*
  - *expression des propriétés à vérifier dans le modèle pivot suivant les termes choisis par les concepteurs du système.*
  - *vérification formelle des propriétés énoncées sur le modèle pivot à l'aide de techniques optimisées*
  - *Synthèse automatique d'un squelette d'application réparti réalisant la partie contrôle de manière conforme au modèle qui a été vérifié formellement.*



Réalisations prévues

- Une méthodologie outillée permettant d'atteindre le niveau de qualité exigée par l'avionique basée sur la notion de spécification et non de programme.
- Un prototype d'Atelier de Génie Logiciel qui implémentera cette méthodologie. Il fournira une aide pour une approche systématique par prototypage, une utilisation simplifiée des méthodes formelles et la réutilisation de code.

- Un premier retour d'expérience industrielle exploitable pour un premier raffinement de l'AGL proposé.
- Des contributions aux propositions visant "UML certifiable"

Contact : DUFOUR Françoise, le ponant de Paris, 27 rue Leblanc, 75512 cedex Paris 15 (Tél. 01 53 23 20 26) – francoise.dufour@sagem.com
http://morse.lip6.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE
SAGEM
Aonix
LIP6
LaBRI
MINISTERE DE LA RECHERCHE