Projet CORSS:
Composition et Raffinement de Systèmes Sûrs
ACI SI

Mamoun Filali

FéRIA SVF

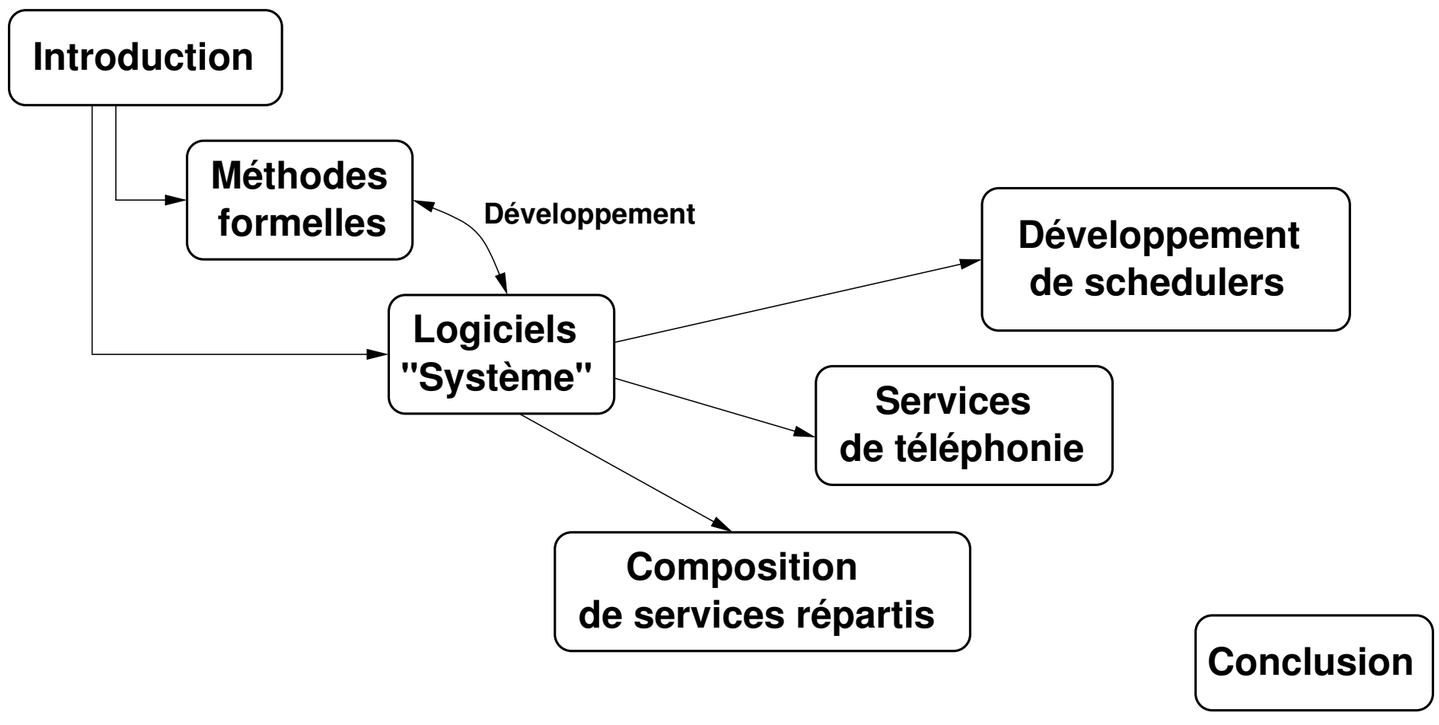
Toulouse

Rennes

11 décembre 2003

Participants :

- ARLES-INRIA : Valérie Issarny.
- COMPOSE-INRIA : Charles Consel.
- MOSEL-LORIA : Dominique Méry.
- SVF-FéRIA : Mamoun Filali.
- OBASCO-EMN : Gilles Muller.


Introduction
Méthodes formelles
Développement
Logiciels "Système"
Développement de schedulers
Services de téléphonie
Composition de services répartis
Conclusion

1 Introduction

1.1 Application des méthodes formelles

- Expression des spécifications :
  - Logique de Hoare.
  - Logiques modales.
- Développements formels de logiciels :
  - Raffinements.
  - Composition.
- Outils :
  - Preuve assistée.
  - Preuve automatique.

- Manque de cas d'étude.
- Passage à l'échelle.

1.2 Construction de systèmes

- Prise en compte de plusieurs aspects :
  - Accès concurrents aux ressources.
  - Localisation des ressources.
  - Fiabilité.
  - Configuration dynamique.
- Expériences de construction.
  - définition d'abstractions.
  - composition, architecture de services.
  - définition de langages dédiés.

- Formalisation et validation de l'expérience de construction.
- Utilisation effective des environnements de preuve.

1.3 Application des méthodes formelles pour la construction des systèmes

- maîtrise du processus de construction.
- définition de briques de base pour la formalisation et le développement des systèmes.
- mise à l'épreuve des méthodes formelles.

Les activités « système » considérées dans CORSS

- Services répartis :
  - définition et composition de services répartis.
  - algorithmique répartie.
- Services de téléphonie :
  - Définition de langages dédiés pour la construction de services de téléphonie.
- Systèmes de scheduling.
  - Définition d'une méthodologie de développement et d'intégration de schedulers.

2 Développement de schedulers

Problématique

– Correction de l'interaction avec le système.
– Correction de l'implantation de la politique d'ordonnancement.
– Satisfaction des contraintes du niveau applicatif.

Approche Bossa (OBASCO)

Etude noyaux existants.
- Etude des points d'interaction scheduler-noyau.
- Comportement abstrait d'un scheduler.

DSL (Domain Specific Language) pour la définition d'ordonnanceurs.
- Espace d'état dédié.
- Langage événementiel (description de transitions étiquetées).
- Analyse spécifique.

Intégration à des noyaux existants
- Vérification statique (raffinement).
- Génération de code pour un noyau existant.

Expérience MOSEL SVF

- Expression de la composition :
  - schémas de décomposition : B $\rightarrow$ B$\sharp$, TLA, ...
- Mécanisation de logiques de composition :
  - Owicky-Gries, Assume-Guarantee, ...
- Formalisation de politiques d'ordonnancement.
  - Réseaux de Petri temporisés.
  - Automates temporisés.

3 Services de téléphonie

Problématique

– Flot de contrôle implicite : programmation événementielle de base, exécution répartie de scripts.
– Interaction de services.
– Mécanismes de désignation.

Approche Compose

- Flot de contrôle explicite : langage call/C
- Compilation vers des langages de base.
- Enoncé des propriétés.
- Analyse statique.

Expérience MOSEL SVF

- Interaction de services.
- Expression de services répartis.
- Formalisation et validation de traductions.
- Outils de preuve automatique.

4 Composition de services répartis

Problématique

- partage des données, disponibilité des ressources,
- localisation des données,
- gestion de groupes,
- cohérence de données,
- reconfiguration.

Approche ARLES

aide au développement de services répartis composites

- gestion de l'échange et de la cohérence de données dans un contexte mobile.
- découverte de services.
- gestion de groupes dans un contexte mobile.
- sûreté de fonctionnement : WSCA.

Expérience MOSEL SVF

- Spécification de la répartition.
- Développement de la répartition.
- Formalismes de preuve pour les systèmes réactifs.
- Automatisation des preuves.

5 Conclusion

- Coopérations enrichissantes et prometteuses.
  - Etudes de cas intéressantes.
  - Meilleure capture du processus de développement.
  - Mécanismes de composition.
  - Définition d'un environnement de preuve dédié.
- ambitions - moyens.
  - Réunions pour enrichissement mutuel.
  - Stages pour études ciblées.