EC Logiciels sûrs

Composante
Sciences Fondamentales et Appliquées

Présentation

Description

L'UE Logiciels sûrs est une introduction à la vérification formelle de logiciels. La notion de preuve de propriétés d'un programme est introduite d'abord pour les programmes écrits dans le style fonctionnel ensuite pour ceux écrits dans le style impératif.

Différences entre validation et vérification, limites des techniques de tests, vérification par la preuve formelle de programmes. Périmètre de la vérification formelle.

Introduction à l'assistant de preuves Coq. Notion de preuve. Notions de logique (séquence, règles de la déduction naturelle). Rappels de programmation fonctionnelle. Preuves de propriétés de programmes fonctionnels.

Notions d'équivalence de programmes et de transformations de programmes. Logique de Hoare ; assertions, triplets de Hoare, décoration de programmes, invariants de boucles, précondition la plus faible. Mise en oeuvre dans Coq.

(* Cette partie est optionnelle *)

Sémantique opérationnelle à petits pas, systèmes de typage.

Objectifs

Initiation à la vérification formelle de programmes : comprendre les notions de base, savoir les mettre en oeuvre et être autonome dans cette mise en oeuvre.

Heures d'enseignement

Logiciels sûrs - CM	CM	10h
Logiciels sûrs - TP	TP	15h

Pré-requis nécessaires

Notions d'algorithmique fonctionnelle et programmation fonctionnelle de niveau licence d'Informatique.

Compétences visées

Capacité à décrire formellement un programme, savoir exprimer une propriété dans un formalisme logique, maîtriser les outils logiques de manipulation d'une preuve de programme, maîtriser le développement d'une preuve de programme dans un assistant de preuve.