

# HMIN229 : Preuves de programmes

Systèmes critiques : système dont la panne peut avoir des conséquences dramatiques (morts, dégâts matériels importants, conséquences graves pour l'environnement).

Domaines d'application critiques : transports, production d'énergie, santé, système financier, domaine militaire.

Logiciels sûrs (sans bugs, zéro défaut) : utilisation de méthodes rigoureuses de développement ; méthodes très particulières et qui reposent sur un certain nombre de fondements théoriques.

# De quoi allons-nous parler dans cette UE ?

- ❶ Introduction aux méthodes formelles de développement logiciel :
  - ▶ Typage des langages de programmation ;
  - ▶ Vérification déductive (preuves) ;
  - ▶ Model-checking (états du système) ;
  - ▶ Analyse statique par interprétation abstraite.
- ❷ Preuves formelles :
  - ▶ Langage support : outil d'aide à la preuve Coq ;
  - ▶ Langage de programmation (fonctionnel) ;
  - ▶ Langage de spécification (types inductifs, etc.) ;
  - ▶ Langage de preuve (utilisation et écriture de tactiques).
- ❸ Sémantiques formelles et preuve de programmes
  - ▶ Modélisations en utilisant Coq ;
  - ▶ Sémantiques opérationnelles (naturelle, structurée) ;
  - ▶ Preuves de propriétés (correction du typage, etc.) ;
  - ▶ Preuves de programmes (fonctionnels et impératifs).

MCC : 2/3 examen écrit + 1/3 projet (Coq).