

# Méthode de conception de logiciel système critique couplée à une démarche de vérification formelle

## Mots clés :

- **Directeur de thèse** : Kamel Barkaoui
- **Co-encadrant(s)** :
- **Unité de recherche** : Centre d'Étude et de Recherche en Informatique et Communications
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

## Résumé du projet de recherche (Langue 1)

En raison de l'évolution rapide des technologies, la complexité des systèmes et des logiciels critiques s'accroît de plus en plus. Ces derniers doivent offrir une garantie de sécurité et de sûreté de fonctionnement. Afin d'assurer une meilleure maîtrise des systèmes critiques, il est intéressant d'utiliser des outils de méthodes formelles. Ces outils présentent de nombreux avantages pour l'industrie grâce à leurs capacités à fournir des garanties mathématiques permettant de prouver l'absence de certains défauts. Néanmoins, l'application de ces outils à du code système se heurte à plusieurs difficultés d'ordre pratique et théorique. Ces outils se concentrent généralement sur la validation de modèles ou d'algorithmes de haut-niveau. Pour un code système comme le noyau de système d'exploitation, la prise en compte des contraintes bas niveau est essentielle. L'objectif est donc d'une part, de mettre en place une méthode et des outils adaptés à ce type d'ingénierie et d'autre part de combattre le problème de l'explosion combinatoire de l'espace d'états du système rencontré lors de la vérification algorithmique.