Université de Bretagne Occidentale

Faculté des Sciences & Techniques

MASTER INFORMATIQUE

## PARCOURS LOGICIELS POUR SYSTÈMES EMBARQUÉS

**Semestre 9**

# S9 LSE Sûreté et sécurité des systèmes

## Présentation

Ce cours aborde le problème de la validation des applications embarquées en proposant des méthodes/techniques pour vérifier les propriétés temps-réel, pour évaluer la fiabilité du système et pour mettre en place des mécanismes de sécurité.

**4 crédits ECTS**

Volume horaire

Travaux Pratiques : 16h
Travaux Dirigés : 16h
Cours Magistral : 16h

## Objectifs

Etre sensibilisé à certaines bonnes pratiques, à certaines propriétés fondamentales de la cryptographie appliquée, à l'utilisation des bibliothèques cryptographiques, à l'analyse des protocoles de sécurisation d'une communication.

Comprendre les techniques et mécanismes pour mettre en place des modules fiables au sein d'un système embarqué.

Savoir modéliser l'architecture du système avec un standard (ex AADL),

Comprendre les problèmes de contraintes de temps dans le cadre du temps réel et savoir réaliser la vérification de ces contraintes.

## Pré-requis nécessaires

Systèmes temps-réel

## Descriptif

Ce cours est constitué de trois parties:

partie I: vérification de propriétés, application au temps réel, modélisation AADL

Pour cette première partie, nous regarderons comment décrire l'architecture du système, tant du point de vue du logiciel que de la plateforme d'exécution. Le langage employé pour ce faire sera AADL, un exemple de standard appliqué par les acteurs du domaine dans le cadre de systèmes embarqués critiques temps réel. Puis, nous regardons comment réaliser la vérification des contraintes de temps (analyse d'ordonnancement temps réel) pour des architectures monoprocesseurs et multiprocesseur).

partie II: Modèles pour l'analyse de fiabilité et techniques de tolérance aux fautes

Dans cette partie, on s'intéresse au monitoring du système et à l'analyse de sa fiabilité. Des techniques de tolérance aux fautes sont abordées pour rendre les architectures matérielles plus robustes (ECC, TMR). Des exemples d'application de ces techniques sont développés.

partie III: Sécurité des systèmes embarqués

Dans cette dernière partie, nous allons étudier certains aspects de la sécurité informatique dans le cadre des systèmes embarqués. Nous reviendrons sur les propriétés de base de la sécurité, puis nous nous intéresserons à la cryptographie utilisée dans ce contexte (en particulier en présentant des attaques spécifiques à l'embarqué, et les protections pour les contrecarrer). Enfin il sera présenté un exemple d'application bien connu, le standard EMV, utilisé lors des paiements via carte à puce.

## Modalités de contrôle des connaissances

### Session 1 ou session unique - Contrôle de connaissances

| Nature de l'enseignement | Modalité | Nature | Durée (min.) | Coefficient | Remarques |
|---|---|---|---|---|---|
| | CC | Travaux Pratiques | | 1/3 | |
| | CT | Ecrit - devoir surveillé | 120 | 2/3 | |

### Session 2 : Contrôle de connaissances

| Nature de l'enseignement | Modalité | Nature | Durée (min.) | Coefficient | Remarques |
|---|---|---|---|---|---|
| | CT | Ecrit - devoir surveillé | 120 | 100% | |

## Langue d'enseignement

Français avec aide ponctuelle en anglais