USRS2D - Sécurité et sûreté de fonctionnement pour l'embarqué - mobile

Mis à jour le 18-05-2017

Code : USRS2D

Unité spécifique de type cours

5 crédits

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

Systèmes enfouis et embarqués

2D4P40, 33.1.13, 2 rue Conté
75003 Paris
01 40 27 26 81
Meriem Bouabdellah
meriem.bouabdellah@cnam.fr

Présentation

Objectifs pédagogiques

L'objectif de cette UE est de donner une introduction approfondie aux besoins et techniques de la sûreté de fonctionnement et de la sécurité des systèmes informatiques embarqués.

Programme

Contenu

De nos jours les problèmes de sécurité des données et des systèmes informatiques ainsi que
la sûreté de fonctionnement ne peuvent plus être ignorés et la prise en compte de ces questions doit être envisagée très tôt dans le processus de développement. Dans le cadre des systèmes embarqués et enfouis qui sont souvent moins sujet au contrôle direct ou indirect d'opérateurs humains avertis ou de
systèmes de supervision, la question de la sécurité et de la sûreté de fonctionnement se pose de façon plus aigüe.
Concernant la sécurité, nous aborderons la mise en place de politiques de sécurité et les normes souvent rencontrées et/ou imposées dans différents domaines d'application des systèmes embarqués.
Nous introduirons également les concepts fondamentaux de la cryptographie et des protocoles réseau pour obtenir des propriétés de sécurité désirées.
Des intervenants extérieurs évoluant dans le domaine de la carte à puce présenteront la cryptographie réellement déployée dans leur monde. Mais apporteront aussi un éclairage particulier sur les vulnérabilité des systèmes embarqués par des illustrations d'attaques détournées (attaques physiques,
. . .) et les contre-mesures (DPA, exploration du circuit au microscope électronique, ...) et plus généralement toute exploitation de canaux cachés.
Concernant la sûreté de fonctionnement nous aborderons les domaines suivants :
- Concepts et moyens de la sûreté de fonctionnement : diagnostic, redondance, codes détecteurs et correcteurs, reconfiguration
- Validation d'architectures : spécification de propriétés, modélisation d'architectures, vérification des propriétés
- Evaluation prévisionnelle : composantes de la SDF, diagrammes de fiabilité, arbres de défaillance et calcul de coupes minimales, méthodes markoviennes, méthodes de simulation.
- Les outils de la sûreté de fonctionnement : outils de modélisation comportementale et temporelle, outils fondés sur l'analyse des événements redoutés (AER, AMDEC, Coupes minimales), outils d'évaluation quantitative (processus markoviens et semi markoviens, réseaux de Petri stochastiques,
méthode Monte Carlo, etc.), outils d'analyse statique de code, outils de suivi des tests.

Description des modalités de validation

Contrôle continu sous la forme d'exposés thématiques (50%) + examen (50%).