Sûreté de fonctionnement des systèmes embarqués

Composante
École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications

En bref

- **Code Ametys:** M34HPPYB
- **Ouvert aux étudiants en échange:** Oui

Présentation

Objectifs

À l'issue de ce cours, les étudiants seront capables de :

- Comprendre les principes fondamentaux de la sûreté de fonctionnement et son importance dans les systèmes critiques.
- Identifier et analyser les différentes catégories de pannes (*systématiques* et *aléatoires*) ainsi que les modèles de fautes associés.
- Maîtriser les approches de gestion des risques appliquées aux systèmes embarqués, notamment dans le domaine de l'automobile.
- Appréhender la norme **ISO 26262** et ses exigences en matière de sûreté de fonctionnement.
- Effectuer des analyses de sûreté au niveau **système** et **composant matériel** (*hardware*).
- Mettre en œuvre des stratégies de conception permettant d'atteindre les objectifs de sûreté définis par les niveaux d'intégrité ASIL.
- Réaliser des analyses de sûreté spécifiques telles que **FTA (Fault Tree Analysis), FMEDA (Failure Modes, Effects and Diagnostic Analysis)** et **DFA (Dependent Failure Analysis)**.

Description

1- Introduction à la sûreté de fonctionnement

- Définition et importance de la **sûreté de fonctionnement** (*Functional Safety*).
- Historique et évolution des **normes de sûreté**.
- Approche générale de la **gestion des risques** et classification des pannes (*systématiques vs aléatoires*).
- Gestion du risque dans l'industrie automobile.
- Concepts de **safety goals** et **safety integrity levels (ASIL)**.
- Introduction à la norme **ISO 26262**.

2 - Sensibilisation à la sûreté de fonctionnement

- **Vue d'ensemble de la norme ISO 26262** et structure du standard.
- **Phase conceptuelle**
  - Définition des **items**.
  - Analyse des risques et **HARA (Hazard Analysis and Risk Assessment)**.
  - Développement du **Functional Safety Concept (FSC)**.
- **Développement au niveau système**
  - Définition du **Technical Safety Concept (TSC)**.
  - Décomposition ASIL et décisions de conception.
  - Méthodes d'analyse de sûreté à l'échelle du système.
  - **Tests et intégration** dans le cycle de développement.

3- Développement matériel et analyses de sûreté

- Cycle de vie du **hardware** et exigences spécifiques en sûreté.
- Élaboration du **Hardware Safety Concept** et des mécanismes de sûreté associés.
- Techniques d'analyse de sûreté matérielle :
  - **FTA (Fault Tree Analysis)** : arbre de défaillances.
  - **DFA (Dependent Failure Analysis)** : analyse des fautes dépendantes.
  - **Calcul du taux de défaillance**.
  - **FMEDA (Failure Modes, Effects and Diagnostic Analysis)** : étude des modes de défaillance et de la couverture diagnostique.
- Contraintes spécifiques aux **semi-conducteurs** dans l'industrie automobile.