

Sûreté de fonctionnement des systèmes embarqués

Présentation

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 (*systematiques 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.