Reliability of embedded systems

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

In brief

- **Ametys Code:** M34HPPYB
- **Open to exchange students:** Yes

Presentation

Objectives

By the end of this course, students will be able to:
- Understand the fundamental principles of functional safety and its importance in critical systems.
- Identify and analyze different categories of failures (systematic and random) and the associated fault models.
- Master risk management approaches applied to embedded systems, particularly in the automotive field.
- Understand the ISO 26262 standard and its requirements for functional safety.
- Perform safety analyses at the system and hardware component levels.
- Implement design strategies to achieve the safety objectives defined by ASIL integrity levels.
- Perform specific safety analyses such as FTA (Fault Tree Analysis), FMEDA (Failure Modes, Effects and Diagnostic Analysis) and DFA (Dependent Failure Analysis).

Description

1- Introduction to functional safety
Definition and importance of functional safety.
History and evolution of safety standards.
General approach to risk management and classification of failures (systematic vs. random).

Risk management in the automotive industry.
Concepts of safety goals and safety integrity levels (ASIL).
Introduction to ISO 26262.
2 - Awareness of functional safety
Overview of ISO 26262 and structure of the standard.
Conceptual phase
Definition of items.
Risk analysis and HARA (Hazard Analysis and Risk Assessment).
Development of the Functional Safety Concept (FSC).
System-level development
Definition of the Technical Safety Concept (TSC).
ASIL decomposition and design decisions.
System-level safety analysis methods.
Testing and integration into the development cycle.
3- Hardware development and safety analyses
Hardware life cycle and specific safety requirements.
Development of the Hardware Safety Concept and associated safety mechanisms.
Hardware safety analysis techniques:
FTA (Fault Tree Analysis): fault tree.
DFA (Dependent Failure Analysis): analysis of dependent faults.
Calculation of failure rate. FMEDA (Failure Modes, Effects, and Diagnostic Analysis): study of failure modes and diagnostic coverage.
Specific constraints for semiconductors in the automotive industry.