C8 - Critical Systems Safety

Objectives

- Understand the challenges of system safety
- Explore methods of formal proofs
- Understand the development standards applicable
  - IEC 61508
  - DO-254
  - DO-178B and C
- Understand certification issues

Prerequisites

- Basic knowledge of embedded and real-time systems

Course Environment

- Theoretical course
  - PDF course material (in English) supplemented by a printed version.
  - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Course Outline

First Day

System Safety

- Risk Analysis
- Analysis Techniques
  - Analysing defects causes and effects
  - Fault Tree Analysis
- Safety Certification
- Technical failure prevention
  - Inherent system safety
  - Limiting the effect of failures
- Safety and reliability

Formal proofs

- Need for formal specification
- Formal specifications methods

Example:: Proofs using invariants, pre-and post-conditions

Software safety standards

- The IEC 61508 Standard
  - Integrity Levels (SIL 1 to 4)
  - Validation
- The DO-178 and DO-254 standards
  - System Safety Assessment
  - Software Levels (A to E)
  - Qualification tools
- Other Standards
- Other standards

Second Day

The DO-178 certification process

- Certification Authorities
  - FAA (Federal Aviation Administration)
  - EASA (European Aviation Safety Agency)
  - JAA (European Joint Aviation Authorities)
  - CAB (Japan Civil Aviation Bureau)
  - ...
- Certification Procedures
- Various types of certificates
  - Type Certificate (TC)
  - Supplemental Type Certificate
- The TSO (Technical Service Order)
- The DER (Designated Engineering Representatives)
  - Difference between the FAA and EASA
- The path to a successful certification

The DO-178B Standard

- The DO-178B development model
  - DO-178B and DO-254
  - The system development life cycle
  - The life cycle processes
  - Difference between verification and testing
- The software development process
  - Development Support
  - Development
  - Quality Assurance
  - Certification
- The audit framework
  - Reviews
  - Analysis
  - Tests
- Requirements traceability
  - Requirement-based tests
  - Test coverage
- DO-178B and off-the-shelf products

Third day

The DO-178C

- Why a new standard
  - Purpose of the DO-178C
  - Strategy definition
  - Structure of the DO-178C standard
- The differences with DO-178B
  - Clarifications of the standard
  - Changes in the document core
  - New items
- Supplements
  - DO-330: Tool Qualification
  - DO-331: Model Based Development
  - DO-332: Object Oriented Technology
  - DO-333: Formal Methods