

Safety

TUV SUD Functional Safety Certification

General Information

Course Code: SCT-TUVFSE1A
Length: 3.5 Days

Audience

This course is for

- Application engineers and system integrators with some experience in Functional Safety
- Project and safety managers
- Designers and safety specialists working in machinery applications.

Prerequisites

- MS Windows Expertise
- Basics of Functional Safety according to IEC 61508 (SIL) and ISO 13849 (PL)
- Basic exposure to machine safety concepts

Profile

The objective of this course is to relate the safety concept of IEC 61508 and cover the main principles for Functional Safety. ISO 13849 and IEC 62061 are covered by demonstrating safety principles according to these standards and how they relate to IEC 61508.

Software development of safety related control systems is covered in day three followed by a fourth day question and answer session with resulting final exam.

The exam is closed book containing 60 multiple choice and 25 open questions. Certification requires a 75% passing grade.

Objectives

Upon completion of this course, the student shall be able to:

- Analyze the main requirements of IEC 61508 (SIL) and ISO 13849 (PL) for the design of safety related parts.
- Identify risk analysis and selection of protective devices to achieve required risk reduction.
- Review the documentation requirements for machine safety applications
- Examine typical safety circuits, schematics.
- Identify safety validation requirements.
- Review the software related to safety related control systems.

Topics

1. IEC 61508 Safety Concepts
 - a. Introduction to safety and overview on standards
 - b. Risk and hazard analysis
 - c. Safety functions and the safety performance
 - d. Life cycle
 - e. Functional safety management
 - f. Modification process
 - g. Required documentation
 - h. Basic architectures
 - i. Measures to avoid and control failures, diagnostics
 - j. FMEDA on system and component level
 - k. SIL, HFT, PFD, PFH, DC and SFF calculation
 - l. Verification and validation activities
2. Safety Principles relating to ISO 13849 & IEC 62061
 - a. Safety concept of ISO 13849
 - b. Risk analysis according ISO 13849 and IEC 62061
 - c. Determination of PL (Categories, MTTFd, DC and CCF)
 - d. Safety concept of ISO 62061
 - e. Determination of SIL (SIL CL, PFH, β -factor)
 - f. Examples and exercises for IEC 62061 and ISO 13849-1
3. Software Development of Safety Related Control Systems
 - a. Software lifecycle
 - b. V-Model
 - c. Measures to avoid systematic failures
 - d. Software architecture
 - e. Self-tests (RAM-, ROM- and CPU-tests)
 - f. Program sequence monitoring
 - g. Data communication
 - h. Coding-rules (MISRA)
 - i. Software criticality analysis (SWCA)
 - j. Differences to ISO 13849 and IEC 62061
4. Final Exam
 - a. Q&A
 - b. Exam