As of 20.05.2019

Functional Safety of Electronics and Software: Implementation Compliant with IEC 61508 and ISO 26262

Objectives

The Functional Safety Training covers the principles of safety for control electronics and software and deals with state of the art techniques.

You learn about the requirements for accomplishing electronic system and software safety as defined by corporate and project management.

You get an overview of the measures to be taken in an overall system, e.g. crane including crane control, or IoT systems, so as to assure electronics safety.

You understand the measures to be implemented in state-of-the-art projects to accomplish safe electronic systems and software for your work products, as well as the procedures to develop these work products.

You know how to apply the related international standards, perform risk and hazard analysis, differentiate between safety-critical faults and avoid them.

You learn about fault monitoring and handling techniques.

Your advantages:

You get an efficient and compact entry into the overall safety context

You can refresh and intensify your knowledge

You get a training certificate complying with the related standards

You benefit from efficient exam preparation

You can use the training documentation as compendium.

Participants

The functional safety training addresses development engineers and managers as well as project managers and engineers dealing with safety-related topics.

Requirements

Experience with control electronics (embedded systems)

Functional Safety of Electronics and Software: Implementation Compliant with IEC 61508 and ISO 26262

Content

Functional Safety: Basics and Introduction

- Functional safety definition
- International standardization
- How to handle threats and hazards
- Safety relevant functions and their integrity
- Exemplary systems
- Deriving risks
- Challenges of accomplishing functional safety
- Dangerous faults

- Functional safety of E/E/PE safety relevant systems
- Scope definition
- Relevant standards - overview
- Responsibilities and required conditions (practiced by means of discussion)
- Safety in a legal context

IEC 61508 as Basic Standard

- Objectives of the standard
- Defined system and hierarchies
- Documentation as main element of assessment
- Differentiation between security and safety

Safety Lifecycle

- Phases and their meanings
- E/E/PE system implementation
- Software implementation
- Hardware-software relation
- Requirements defined by the standard
- Using different lifecycle models or development models
- Verification
- Assessment
- Artefacts
- Required independence

How to Manage Functional Safety

- Persons involved
- Responsibilities
- Activities
- Planning documents
- Exercise: Prerequisites of a safety project

Risk Analysis and Risk Assessment

- Required input
- Relation between risk integrity and safety integrity
- Determination of SIL, modes of operation
- Risk reduction as a concept
- Common cause failures
- Multiple protection layers
- ALARP method
- Risk classification
- Risk graph
- Hazardous event severity matrix (qualitative)
- Layer of protection analysis
- Exercise: SIL determination

System Design

- Higher-level allocation of safety requirements
- E/E/PE system safety requirements specification
- E/E/EP safety-related system implementation
- E/E/PE system design requirements specification
- Functional requirements
- Integrity requirements
- E/E/PE system safety validation plan
- E/E/PE system design and development
- Systematic capability
- Architectural constraints
- Hardware fault tolerance (HFT)
- Types of components/elements/subsystems
- Safe failure fracion (SFF)
- Route 1H
- Serial combination of elements
- Parallel combination of elements
- Route 2H
- Data communication

- Fault reaction
- Fault tolerant time interval (FTTI)
- Failure analysis
- Fault types
- Failure types
- Quantifying the effect of random hardware failures
- Failure modes
- Failure rates
- Proof test interval (PTI)
- FMEDA
- Diagnostic coverage
- Mitigation systems
- Exercise: Assessment of knowledge

Software Safety Lifecycle

- Hardware/software interface (HSI)
- Additional requirements for the management of safety-relevant software
- Process adjustment
- Software safety requirements specification
- Software architecture design
- Support tools and programming languages
- Detailed design and development
- Code implementation
- Software module test
- Software integration test
- PE integration (hardware & software)
- Software operation and modification process
- Software aspects on system safety validation
- Software verification

Specific Aspects of ISO 26262

- Lifecycle and management
- ASIL determination
- Hardware design, development and assessment
- Software design, development and assessment

Example of a Microcontroller with Integrated Safety Functions

TOP 5 Dos and Don'ts

Note: An interactive and individual assessment of the learning progress is performed for each chapter; results are available at real-time and as pfd file.

Trainings

Date	Price *	Duration
21.10.2019 – 23.10.2019	1.800,00 €	3 days

* Price per attendee, in Euro plus applicable VAT.

Training code: E-SAFETY

Coaching

Unsere Coaching-Angebote bieten den großen Vorteil, dass unsere Experten ihr Wissen und ihre Erfahrungen direkt in Ihren Lösungsprozess einbringen und damit unmittelbar zu Ihrem Projekterfolg beitragen.

Für Ihre Anfrage oder weiterführende Informationen stehen wir Ihnen gern zur Verfügung.