

Functional Safety Engineer – Level 01 (IEC 61508 & IEC 61511)

Learn to apply IEC 61508 and IEC 61511 to determine SIL,
design safety instrumented systems, and manage their lifecycle.

4 Days

DURATION

19

MODULES

73

TOPICS

COURSE OVERVIEW

This course covers the foundations of functional safety, including the structure of IEC 61508 and IEC 61511, functional safety management, and the conceptual phase of identifying safety instrumented functions. It then addresses hazard and risk analysis techniques such as HAZOP, LOPA, FTA and ETA, methods for determining the Safety Integrity Level, the safety requirements specification, and SIS design and architecture principles including reliability engineering basics. It continues with system realization and integration, factory and site acceptance testing, installation, commissioning and validation, operations and maintenance, and management of modifications. It concludes with functional safety assessment, the safety lifecycle in practice, cybersecurity considerations for functional safety systems, and common industry mistakes and best practices.

WHO THIS COURSE IS FOR

Functional Safety Engineers

Process Safety Engineers

Instrumentation Engineers

SIS Design Engineers

Safety Assessors

Control Systems Engineers

LEARNING OBJECTIVES

- Explain the concept and lifecycle of functional safety
- Describe the structure and relationship of IEC 61508 and IEC 61511
- Apply hazard and risk analysis techniques such as HAZOP and LOPA
- Determine the Safety Integrity Level for a safety function
- Develop a functional safety requirements specification
- Analyse SIS design and architecture principles, including redundancy
- Assess operations, maintenance and modification management practices
- Evaluate functional safety assessment and cybersecurity considerations

19 Modules, 73 Topics

DAY 1 Foundations of Functional Safety and Risk Understanding

01

Course Introduction

TOPICS

Purpose and scope of the course · TÜV SÜD certification process · Examination overview and expectations

02

Introduction to Functional Safety

TOPICS

- Definition of functional safety
- Historical background (e.g., Bhopal, Texas Refinery incidents)
- Need for risk reduction in process industry
- **Comparison:** Occupational Safety vs. Functional Safety

03

Introduction to IEC 61508 and IEC 61511

TOPICS

- Overview of standard structure
- Relationship between IEC 61508 (generic) and IEC 61511 (process sector)
- Applicability and relevance to E/E/PE systems
- Key terminology (SIF, SIL, SIS, PFDavg, SFF, HFT)

04

Functional Safety Management (FSM)

TOPICS

Lifecycle concept of functional safety · FSM planning and documentation requirements · Roles and responsibilities in FSM · Competency management for personnel

05

Conceptual Phase

TOPICS

- Defining the process and operating environment
- High-level risk analysis and hazard identification
- Process Safety Time (PST) concept
- Identification of Safety Instrumented Functions (SIFs)

DAY 2

SIL Determination and SIS Design Architecture

06

Hazard and Risk Analysis Techniques

TOPICS

- **HAZOP:** Structured hazard identification
- **Layer of Protection Analysis (LOPA):** Quantitative assessment
- Fault Tree Analysis (FTA) and Event Tree Analysis (ETA)
- Risk graph and risk matrix approach

07

Determining the Safety Integrity Level (SIL)

TOPICS

- What is SIL?
- **Methods for SIL assignment:** Risk graph, LOPA, qualitative/quantitative models
- **Example:** SIL Determination using LOPA
- Allocation of safety functions

08

Functional Safety Requirements Specification (SRS)

TOPICS

- Structure and content of SRS
- Functional requirements vs. safety integrity requirements
- Input/output specification, process conditions
- Human-machine interface (HMI) considerations

09

SIS Design and Architecture Principles

TOPICS

- **SIS elements:** Sensors, logic solvers, final elements
- Diversity and redundancy (1oo2, 2oo3, etc.)
- Diagnostic coverage and safe failure fraction (SFF)
- Hardware Fault Tolerance (HFT) and architectural constraints
- Voting logic and failure modes

10

Reliability Engineering Basics

TOPICS

- PFDavg (Probability of Failure on Demand – average)
- PFH (Probability of Failure per Hour) for continuous modes
- Failure Modes and Diagnostic Coverage (FMDC)
- Mean Time to Failure (MTTF) and mission time

DAY 3

Realization, Validation and Lifecycle Maintenance

11

System Realization and Integration

TOPICS

- Hardware and software development lifecycle
- Software safety lifecycle phases (per IEC 61508-3)
- Application software vs. embedded software
- Use of certified and proven-in-use components

12

Factory Acceptance Test (FAT) and Site Acceptance Test (SAT)

TOPICS

Purpose, procedures, and documentation · Traceability to the SRS · Test case development and evaluation criteria

13

Installation, Commissioning & Validation

TOPICS

- Verification of installed equipment
- Installation inspection and loop checking
- Validation vs. verification
- Validation plan, criteria, and test documentation

14

Operations and Maintenance (O&M) Phase

TOPICS

- Maintaining SIL during operation
- Proof testing and maintenance procedures
- Test coverage, intervals, and impact on PFDavg
- Managing bypasses and overrides

15

Management of Modifications

TOPICS

Change management process · Impact assessment for functional safety · Revalidation requirements after changes

DAY 4

Functional Safety Assessment (FSA), Practical Cases & Exam

16

Functional Safety Assessment (FSA)

TOPICS

FSA stages and purpose (Stage 1 to Stage 5) · Independence requirements for FSA · Documentation review and audit evidence · Competence and independence of assessors

17

Safety Lifecycle in Practice

TOPICS

- Integration of functional safety with overall safety lifecycle
- Interface with Basic Process Control Systems (BPCS)
- Examples of safety lifecycle failures

18

Cybersecurity in Functional Safety Systems

TOPICS

IEC 62443 overview · Asset inventory, vulnerability assessment · Secure architecture for SIS · Impact of cyber threats on functional safety

19

Common Industry Mistakes & Best Practices

TOPICS

- Case studies of failures due to poor SIS design
- Lessons learned from incidents
- Human error vs. system error
- Pitfalls in SIL determination and testing

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com