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

Duration: 4 Days | Mode: Instructor-Led |

DAY 1: Foundations of Functional Safety and Risk Understanding

Course Introduction

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

Introduction to Functional Safety

- 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

Introduction to IEC 61508 and IEC 61511

- 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)

Functional Safety Management (FSM)

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

Conceptual Phase

- 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

Hazard and Risk Analysis Techniques

- 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

Determining the Safety Integrity Level (SIL)

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

Functional Safety Requirements Specification (SRS)

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

SIS Design and Architecture Principles

- 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

Reliability Engineering Basics

- 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

System Realization and Integration

- 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

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

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

Installation, Commissioning & Validation

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

Operations and Maintenance (O&M) Phase

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

Management of Modifications

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

DAY 4: Functional Safety Assessment (FSA), Practical Cases & Exam

Functional Safety Assessment (FSA)

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

Safety Lifecycle in Practice

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

Cybersecurity in Functional Safety Systems

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

Common Industry Mistakes & Best Practices

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