Functional Safety Course

Roxby Training Solutions Ltd, Unit 4 John Clarke Centre, Dockside Road, Middlesbrough
TS6 6UZ
Telephone: 01642 438700
Fax: 01642 466879
j.dean@roxby.com or r.mellor@roxby.com

Aim: To give an appreciation of Functional Safety

This course is an opportunity for Operating, Process, HSE and Maintenance personnel to gain an insight into aspects of Functional Safety.

This appreciation course is intended to demonstrate the fundamentals of Functional Safety Lifecycle i.e. how a Functional Safety Engineer would:-

1. reduce risks
2. satisfy legal and regulatory requirements
3. meet the organisation's business objectives
4. enable the organisation to meet regulatory/contractual commitments

By understanding:

- The principles and concepts of the internationally agreed standards IEC 61508 and IEC 61511 for safety instrumented systems (SIS)
- Hazard identification and the hazard and operability (HAZOP) process including understanding cause / consequence pairs and the sequence of events leading to the hazard
- Risk, the setting of tolerable risk targets for safety, asset and the environment and methods to achieve these targets by reducing risks to as low as reasonably possible (ALARP)
- The concepts and differences between qualitative, semi quantitative and quantitative risk assessment methods and when and how to apply them
- The principles of risk modelling, event tree analysis (ETA) and fault tree analysis (FTA) and how to model protective systems using these techniques
- How to set up, use and apply the most popular safety integrity level (SIL) risk assessment methods such as risk graphs, risk matrices and layers of protection analysis (LOPA)
- SIL determination for preventative and mitigation systems including Fire and Gas systems (e.g. detector coverage and mitigation capability)
- Correctly developing the Safety Requirements Specification (SRS) to ensure the requirements are auditable, testable and written for ease of understanding
- How to design safety-instrumented systems for protecting against process related hazards using the techniques and measures in IEC 61508 and IEC 61511 including developing lifecycle procedures (e.g. maintenance, inspection and testing)
- The technical information required on all system components including extracting reliability data for the application from manufacturer's certificates, reports, FMEA and applying confidence levels to the data
- SIL demonstration calculations such as probability of failure on demand (PFD), safe failure fractions, hardware fault tolerance and proof test interval determination
- How to identify and calculate the impact of common cause failures (Beta factor) on the reliability of protective systems
- Requirements for proven in use evidence for existing installed equipment
- Requirements for validation documentation to demonstrate that systems, (including application software and software and hardware integration) have been fully tested checked and approved against the safety requirements specification
- Introduction to the latest software tools for risk assessment and designing safety instrumented systems and integrating them with other technologies

Course Objectives

The course will give participants an appreciation of the application, principles and requirements of IEC 61508 — Functional safety of electrical/electronic/programmable electronic safety systems and IEC 61511 — Functional Safety: Safety Instrumented Systems for the Process Sector.

The course will provide three days of classroom tuition and practical guidance, mixed with practical exercises based on real life examples.

Day 1 Agenda

Will provide an introduction to the functional safety standards, the underpinning legislation and the concept of the functional safety lifecycle. Phases 1, 2, 3, 10 and 11 - process hazard analysis, risk assessment, allocation of safety functions and functional safety and competency management will be discussed in depth and participants will be introduced to the concepts of the international standards that cover this area of risk assessment and risk reduction.

The topics covered will be:

- IEC 61508 and IEC 61511 background
- Functional Safety Management and the application of the FS lifecycle
- Competency Management and Assessment
- Hazards, Risk and ALARP principles
- Failure Modes and Effects Analysis (FMEA)
- Risk Reduction
- SIL Determination by Risk Model
- Event Tree Analysis
- SIL Determination using Event Tree Analysis
- Fault Tree Analysis (FTA)
- SIL Determination using Fault Tree Analysis
- Quantified Risk Assessment
- Practical Exercises
- Case Studies with typical findings and issues

Day 2 Agenda

Covers phases 3 and 4 in depth from determining the target SIL, developing the Safety Requirements Specification (SRS) and how to undertake appropriate cost effective designs for Safety Instrumented Functions (SIF). Participants will be introduced to the concepts of Probability of Failure on Demand (PFD), safe failure fraction, hardware fault tolerance, proven in use, failure modes, reliability, diversity, separation and the influence of common cause.
The topics covered are:

- Risk Graph Calibration
- SIL Determination by risk graphs qualitative & Semi Quantitative
- SIL Determination Exercises
- Layers Of Protection Analysis (LOPA)
- SIL determination using LOPA
- LOPA Exercise

- SIL determination for Fire and Gas

- SIS Safety Requirements Specification
- Selection of Components and Subsystems
- Proven in use
- Failures and failure modes
- Demand Modes
- Probability of Failure on Demand (PFD)
- SIF Implementation (Low demand mode)
- Importance of Testing and Maintenance
- Common cause failures and influence on reliability
- Safe Failure Fraction and Hardware Fault Tolerance
- Practical Exercises
- Case Studies with typical findings and issues

Day 3 Agenda

Covers phase 4 - application software requirements for safety-instrumented systems (SIS) and the relationships between hardware and software architecture. In depth instruction in phase 9 requirements for verification explaining methods for calculating the Probability of Failure on Demand (PFD), safe failure fraction and hardware fault tolerance, the concepts of failure modes, reliability and the influence of common cause failures will also be covered in more depth.

The topics covered are:

- Understanding Failures and failure modes
- Understanding technical information / certificates and reports
- Reliability data and interpreting failure data
- Using Confidence levels
- PFD Exercises including diagnostics & Common cause influence on Integrity
- Partial Closure Testing
- Application Software Requirements Specification & Validation Planning
- Requirements for Support Tools, User Manuals and Application Language
- Requirements for Application Software Development & Module Testing
- Integration of Application Software with SIS Subsystems
- Operations & Maintenance - Installation & Commissioning
- Proof testing strategies and the impact of testing
- Validation Planning and reporting
- Operation and Override procedures
- Inspection and maintenance management
- Modification, Change management and Impact Analysis
- Practical Exercises
- Case Studies with typical findings and issues

Dates available on request