An introductory course in managing functional safety

Should I worry about functional safety management?

How would you answer the following questions?

- Does my business involve the risk of harm or damage associated with chemical processes, fuel fired heaters or with hazardous machinery?
- Do we rely on automated safety systems to reduce the risks associated with the hazards?
- Am I accountable for the effectiveness of automated safety systems in some way, and do my decisions affect other people's safety?
- How can I demonstrate that I have done enough to fulfil my duty of care?

If you answer 'yes' to the first three questions and are not completely sure about the last question then this course will be relevant to you.

An introductory course in managing functional safety

Overview

Functional safety is about applying automated safety functions to implement risk reduction for hazardous scenarios.

In practice most problems in achieving functional safety are not technical, they stem from uncertainty in roles, responsibilities and interfaces within and between organisations.

Functional safety needs good management just like any other engineering activity. Imagine a project without project management.

Teams working on functional safety need to have a clear understanding of their responsibilities and objectives. They need simple, efficient and robust work processes. This course provides the basic knowledge and understanding that leaders need in order to be effective in managing functional safety.

Objective

The ultimate objective of this course is to enable managers to demonstrate due diligence in their duty of care. This means that they need to show that they have taken reasonable steps in applying appropriate standards and practices in managing hazards in the workplace.

Half-day or full-day course option

This one-day course is structured as two separate half-day courses. The first half is a stand-alone four hour introduction into what is meant by 'functional safety', why it might be necessary, and the vital role of managers in achieving safety. The second half of the course concentrates on how effective risk reduction can be reliably achieved by applying functional safety.

Target audience

The course is designed for professional engineers, managers and team leaders who rely in some way on automated safety systems to reduce the risks associated with process hazards.

Typical applications include automated emergency shutdown of chemical processes, fuel fired heaters or of hazardous machinery.

An introductory course in managing functional safety

Course cost

This course is presented as a private in-house course on demand. In the Perth metropolitan region the cost is $3,000 + GST irrespective of class size. The course can also be presented on-line.

Contact training@iesystems.com.au to register or for further details.

Presenter

Mirek Generowicz is the Principal Consultant at I&E Systems, a company that specialises in control and safeguarding systems for the process industries. He first started working with functional safety systems in 1986. Mirek worked in engineering management roles from 1992 to 2018, focusing particularly on design integrity and quality management.

Mirek specialises in independent assessment and audit of functional safety. He has carried out more than 40 functional safety audits and/or assessments for a wide variety of automated safety systems around the world, including some of the largest LNG plants in the world. He is a chartered professional engineer and is accredited by TÜV Rheinland as a Functional Safety Expert.

I&E Systems

I&E Systems has specialised in engineering functional safety systems for process safeguarding since its inception in 1991. We have a thorough understanding of IEC 61508, IEC 61511 and IEC 62061. We apply these standards in a simple and effective manner.

I&E Systems was the first engineering consultancy in the world to achieve TÜV Rheinland FSM certification for functional safety management in safety related systems integration.


Certificate

Functional Safety Management

FS Management (TÜV Rheinland)
IEC 61511-1:2016 - SIS Integration (Phase 4)
FSM 125

Certificate No. 968/FSM 125.06/17

DAY 1 – The Functional Safety Framework

Session 1: Context – Why Functional Safety Needs Management

- Why might we need functional safety?
- The legal requirements for application of functional safety
- Due diligence and duty of care in managing hazards
- What is functional safety?
- What is a safety function?
- Automated safety functions: Safety instrumented functions (SIFs) and safety-related control functions (SRCFs), demand mode functions and continuous mode functions
- What makes functional safety difficult?
- Multiple systematic failures as a common factor in the causes of all major accident events
- What is the purpose of management, and why is it vital in functional safety?

Session 2: Risk Management

- Risk management principles (referring to ISO 31000 and ISO 12100):
- The difference between process safety and personal safety
- Acceptable risk and tolerable risk
- ALARP: Risk reduced to 'As Low As Reasonably Practicable'
- Disproportionate cost
- Calculus of negligence
- Implied cost to avert a fatality
- Layers of protection and hierarchy of risk controls

Session 3: Standards and the Safety Life-cycle

- Modern safeguarding systems are complex and can have hidden, latent faults. Systematic failures are much harder to manage than random hardware failures.
- Functional safety standards were developed over decades in response to increasing complexity in systems and in response to the many major accidents caused by multiple systematic failures.
    - HSE Guidelines
    - ISA S84 and IEC 61511
    - IEC 61508
    - AS 4024
    - ISO 13849
    - IEC 62061

- What does integrity mean in the context of functional safety?
- How could we quantify integrity?
- Achieving integrity using quality management and risk management
- The safety life-cycle as a basis for quality and integrity
- Lifecycle phases can best be understood in terms of the main outputs of each phase:
- Each phase needs to be defined by:
  - Inputs
  - Outputs (information, hardware, software)
  - Verification and records
  - Activities and responsibilities
- There are at least four different standards for machine safety, which one should we choose?
- The standards come from two different sources: ISO and IEC
- The ISO approach is simpler and easier, it relies on a limited choice of circuit architectures
- The IEC approach allows any architectures, but it imposes a more formal and systematic approach to design and development
- The different standards can be used in combination
- The ISO standards have categories, designated architectures and performance levels
- The IEC standards have safety integrity levels and functional safety management
- Conveyor safeguarding
- Mine winders

Session 4: Managing Functional Safety

- Functional safety starts with clear communication of corporate policies and strategies for achieving safety. Functional safety only makes sense within a wider, corporate framework for managing risk.
- Learned helplessness and wilful blindness
- Where problems always start: Interfaces, boundaries and responsibility gaps
- Who is responsible for functional safety management planning?
- Accountability as distinct from responsibility
- Outlining a functional safety management plan
- Planning is usually nested in several layers because of boundaries and interfaces
- Project managers must play a key role in managing functional safety by planning and integrating efforts across boundaries and interfaces
- Managing competence systematically
- Unknown unknowns and Kruger-Dunning
- Supplier competence
- Supplier quality

- What is the difference between verification and validation?
- Managing changes and modifications
- Configuration management
- What is the difference between audit and assessment?
- Follow up and closeout of action items and recommendations
- Measuring performance
- Managing information and documentation

DAY 2 – Achieving and Maintaining Functional Safety

Session 5: Risk Studies

- Hazards identification and analysis comes before SIFs or SRCFS
- Evaluation of risk reduction requirements
- The risk bow-tie, fault trees and event trees
- Prevention versus mitigation
- LOPA
- Machine safety evaluation methods
- Common difficulties in risk evaluation: uncertainties in orders of magnitude
- Developing and specifying safety requirements

Session 6: Achieving Risk Reduction by Design

- Distinguishing random failures from systematic failures
- What proportion of failures is random in practice?
- Estimating probability of failure from failure rates
- Adding redundancy to reduce probability of failure
- Suitability of devices, well tried components
- What is hardware fault tolerance, and why is it necessary?
- Where do the failure rates come from? Why do they vary so widely?
- How can we achieve confidence in failure rate data?

Session 7: Maintaining Risk Reduction in Operation

- The handover gap
- Procedures for operation and maintenance
- Controlling bypasses
- Operator and maintainer training

- Measuring performance and the importance of leading indicators
- Assessing demand rate
- Analysing discrepancies
- Analysing failures and measuring failure rates
- Detecting incipient failures
- Proof test planning
- Facilitating inspection and test
- Keeping records
- Managing modifications

Session 8: Systematic Integrity

- Identifying and preventing systematic failures
- Humans make errors
- Factors affecting human reliability
- How can systematic failures be avoided or controlled?
- Techniques and measures for systematic capability
- Systematic capability
- Avoidance and control of systematic failures
- Choosing techniques and measures
- Effectiveness of techniques and measures
- Systematic integrity starts with management