Functional Safety for Leaders and Managers

Training Course Outline

The functional safety standards IEC 61508-1 and IEC 61511-1 both make it clear that the first priority in functional safety is to provide effective management and leadership.

Leaders and managers need to provide context, direction and a framework so that the engineering teams can work effectively.

Management of functional safety is more difficult than the practice of functional safety engineering because it is more abstract in nature. It is often poorly understood and not well defined.

Leaders and managers need to be competent to fulfil their responsibilities. They need training to support them in developing competency.

The fundamentals of functional safety management are taught in a 2-day course:

<table>
<thead>
<tr>
<th>Session 1</th>
<th>Day 1</th>
<th>Day 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Introduction - what is Functional Safety?</td>
<td>Human Factors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 2</td>
<td>Risk Management</td>
<td>Techniques and measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 3</td>
<td>Standards and the Safety Life-cycle</td>
<td>Managing Competence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 4</td>
<td>Functional Safety Management - Introduction</td>
<td>Planning and Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 5</td>
<td>Risk Studies, RRF, SIL, SC</td>
<td>Documentary Evidence, Assessment and Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 6</td>
<td>Failure Modes</td>
<td>Modification and Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 7</td>
<td>Safety Requirements Specification</td>
<td>Operations and Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session 8</td>
<td>Quantification of Failure Rates</td>
<td>Planning Exercise</td>
</tr>
</tbody>
</table>

The first 4 sessions provide an ‘executive summary’ for top level managers who do not have the time to attend a 2-day course.

The course materials include exercises for self-guided assessment. An optional on-line assessment test is available for candidates who would like to obtain a certificate of attainment.
**Course Outcomes**

The ultimate aim of the course is for candidates to develop the following abilities:

- Understand enough about functional safety in order to supervise and direct the technologists who implement it.
- Prepare a functional safety management plan for a project or for a department within the context of a corporate risk management framework, company policy and the applicable legislation and regulations.
- Lead and coordinate a team in implementing a functional safety management plan to achieve a safety system that delivers the required levels of risk reduction with an appropriate level of systematic integrity.
- Ensure that all participants have a clear understanding of their responsibilities and accountabilities and are competent to carry out the necessary activities.
- Understand the limitations and practicalities of SIL determination, appreciate the uncertainties in failure rate data and in the calculation of probability of failure.
- Monitor records, issues, performance and compliance to ensure that the management plan is effective and to demonstrate that functional safety is achieved and maintained.

**Course Cost**

The cost per candidate for the 2 day training course is AUD 2,500 +GST. The additional cost for the optional on line assessment and certificate is AUD 300 +GST.

**Course Schedule**

Courses are arranged on demand for classes of at least 4 students.

**Registration**

To register for this course please contact training@iesystems.com.au

**Presenter**

Mirek Generowicz is the Engineering Manager at I&E Systems Pty Ltd, a company that specialises in control and safeguarding systems for the process industries. He first started working with functional safety systems in 1986. Mirek has worked in engineering management roles since 1992, focusing particularly on design integrity and quality issues. Mirek specialises in independent functional safety assessment and audit for end-users. Since 2004 he has carried out more than 30 functional safety audits and/or assessments. He was accredited by TÜV Rheinland as a Functional Safety Engineer in 2005, as a Functional Safety Expert in 2012.
1. Introduction

Context: Risk management

Functional Safety refers to “Safety Instrumented Systems” that implement “Safety Instrumented Functions” (SIFs) as part of a company’s overall risk management strategy. Managers need to understand that the purpose of functional safety is to deliver specified levels of risk reduction with integrity.

Context: Law

Occupational Health & Safety obligations under Statute Law and Common Law.

‘Duty of care’

Concepts: Systematic and Random Failures

The difference between systematic and random failures, systematic integrity and hardware integrity.

2. Risk

Concept of tolerable risk

ALARP principle

Concept of layers of protection

Independence of layers

Common cause failures

3. Standards

Duty of care depends on standards and established work practices

IEC 61508 and IEC 61511: History, relationship, structure

Comparison with risk management and quality management


Systematic problems are controlled through active functional safety management:

- Risk management together with
- Quality management

Safety management starts with planning

Planning starts with context: corporate policies and values. Needs clear leadership, values and expectations

Functional safety management

- Defines responsibilities
- Crosses boundaries
- Plans are layered in scope and time
- Defines lifecycle phases and phase transitions
- Defines the document plan
- Defines how quality will be achieved

5. Risk Studies

Risk assessment, risk reduction factors

SIL determination - overview

SIF allocation
Planning for SIL studies
SIL determination methods
Exercises
  - Calibrated Risk Graph
  - LOPA

6. Failure Modes
   Concepts: SIS, SIF, SIL, PFD, HFT
   Failure modes: covert, overt, random, systematic
   Why is hardware fault tolerance so important?
   Variability and reliability of failure rate data
   Diagnostics and safe failure fraction
   Proof test intervals, fractional dead time
   Why is proof testing so important?

7. Safety Requirements Specification
   Requirements development
     - Functional requirements
     - Non-functional, performance requirements
     - Architectural design
   What needs to be defined?
   Who owns the requirements?
   The difference between requirements and design specifications
   Systems architecture in the context of failure modes
   Separation
   Fault tolerance

8. Quantification of Failure Rates
   What to expect and what to look for in SIF Compliance Assurance:
     - PFD quantification
     - Architecture
     - Proof testing
     - Fault tree analysis
     - Diagnostic coverage
     - Common cause failures
     - Repair times
     - Communications failures
     - Human response
     - EMC
     - Climatic and mechanical conditions

9. Human Factors
   History of systematic problems leading to major accident events
   Human factors need to be understood and managed
   Factors affecting response times:
1. Clarity and availability of information
2. Stress
3. Training and practice
4. Team support

Safety management starts with corporate policies and values, setting standards for expected behaviour

Competency development and training
Fitness for work
Operability of equipment

10. **Techniques and measures**
Planning for Quality
Controlling Change
Configuration Management
Issues Management
Document Control
Competency Management
Supplier Quality

11. **Managing Competence**
Systematic management of abilities
Evidence of skill as well as understanding
Competence must match accountability
Applying competency based assessment

12. **Planning and Monitoring**
The need for planning ("Why, Who, What, When and How")
- Context
- Responsibilities
- Competence
- Lifecycle Phase and Document Planning
- Quality Planning

Similarities with project plans and operations plans
Achieving traceability
- To the standards
- To the requirements

Lifecycle phase transitions, baselines and change management
Importance of information being accessible, understandable, current

Managing issues
Managing performance
Supplier Quality

13. **Evidence, Assessment and Audit**
Evidence – the what?
- Lifetime records
Verification versus Validation
Audit
Assessment

... and the why?
Demonstrating compliance
Closing the management loop

Verification objectives
Validation objectives
Constructive feedback for management
Audits: Do the procedures work in practice?
Assessments: Does the SIS meet requirements?

Audits review compliance against the procedures
Assessments make a judgement about whether the required functional safety and safety integrity have been achieved

Planning audits and assessments
Degree of independence

14. Managing Modification and Configuration
Modification management
- Identification and registration of changes
- Review, impact assessment and approval

Configuration management
- For hardware, software and design
- Preventing unauthorised items from entering service.

15. Operation and Maintenance
Functional safety management planning is needed for the operations and maintenance phase, including:
- Procedures
- Training
- Discrepancies and issues
- Proof testing and inspection
- Modifications
- Documentation
- Demonstrating compliance

16. Planning Exercise
Outlining a functional safety management plan for your area of responsibility
Considering the wider context, what corporate frameworks exist?
What interfaces will you have with other departments and organisations?
What aspects are already well defined?
What are the areas where you need to develop new procedures and processes?