Functional Safety Management: As Easy As (SIL) 1, 2, 3

Abstract

This paper outlines the need for planning in functional safety management.

Recent events such as the Montara blowout and the Deepwater Horizon disaster are causing more emphasis to be placed on functional safety of control systems.

Functional safety seems to have been shrouded in mystery for many years – even the term itself is mysterious. In this context functional safety deals with the application of "safety instrumented systems" as part of a company's overall risk management strategy.

The standards for functional safety are relatively new. IEC 61508 was first released in 1998 followed by IEC 61511 in 2003. These standards are both very detailed and specific and yet they aim to establish generic frameworks that apply over a wide range of applications.

Some of the language used seems to be ambiguous and difficult to interpret. Users have found it challenging to interpret and to apply these standards.

The functional safety standards deal with managing the risk of both random failures and systematic failures. It is relatively straightforward to apply the mathematics of probability to characterise random failures. It has been significantly more difficult to manage the risk of systematic failures. This is primarily to do with how we apply engineering methods and techniques.

Engineering companies and operations companies that apply functional safety have struggled to reconcile their long established work practices with the relatively new standards. At best compliance has been "partial".

The good news is that it really is not that difficult to comply. There is nothing particularly new or onerous. The principles are essentially the same as in quality management and risk management.

The first step in achieving compliance is to prepare and to implement a "Functional Safety Management Plan".

Biography

Mirek Generowicz, the Engineering Manager at I&E Systems, has been working with functional safety systems since 1986. He gained certification as a Functional Safety Engineer with TÜV Rheinland in 2005.

In the mid 1990s Mirek contributed to the development of Worley Engineering's quality management system, certified to ISO 9001. Since then he played a key role in the development of ISO 9001 systems for Transfield Worley and for I&E Systems.

In 2004 Mirek began working in Functional Safety Assessment. This led to a better understanding of how to manage functional safety projects. From 2007 to 2010 he led the development of the TÜV certified functional safety management framework at I&E Systems.

I&E Systems Pty Ltd was the first non-vendor systems integration engineering consultancy in the world to achieve TÜV certification of a functional safety management system.

Introduction

There seem to have been widespread perceptions that Functional Safety Management is somehow difficult, mysterious and complicated. In some quarters it has met with active resistance on the grounds that it seems to be bureaucratic and expensive. It does not have to be that way.

There are simple steps that we can take to achieve functional safety efficiently and effectively:

- Planning
- Implementation
- Monitoring
- Assessment

History

Emergence of Standards for Programmable Systems

Programmable safety instrumented systems have been in use since the late 1970s.

Complex electronic and programmable systems are not inherently fail-safe. From the beginning duplex and triplex architectures have been used to reduce the probability of failure on demand.

Various codes of practice were developed for the engineering of shutdown systems and burner management systems. These were largely driven by the need to achieve a fail-safe solution.

At the same time software systems engineering practices have matured. Software systems projects are notoriously difficult to manage. There have been many high profile failures, so much so that the term “software death march” has become a common expression.

Software project management practices were defined in ANSI/IEEE 1058 (Software Management Plans) and ANSI/IEEE 730.1 (Software Quality Assurance) in the period 1987 to 1989.

Following this early work was done on functional safety by various parties including the ISA (standard S84.01 – 1996), the Health and Safety Executive in the UK and by companies such as Shell with their Design Engineering Practices.

The formal international standards for functional safety systems are relatively new. IEC 61508 was first released in 1998, followed by IEC 61511 in 2003 (similar to S84). These standards are both very detailed and specific and yet they aim to establish generic frameworks that apply over a wide range of applications.

Perceptions

Initially operating companies expected system vendors to comply with the standards but without appreciating their own responsibilities in achieving compliance.

Some of the language used seems to be ambiguous and difficult to interpret. Users have found it challenging to interpret and to apply these standards. The very specific and highly detailed nature of the standards obscures the simple principles behind them.

Managers have been slow to commit to standards that seem hard to interpret. The perception of complexity and bureaucracy has hampered the acceptance of these standards.

Engineering companies and operations companies that apply functional safety have struggled to reconcile their long established work practices with the relatively new standards. At best compliance has been “partial”. There has been a reluctance to change work practices.

Development of Quality and Risk Management

In the 1980s industry experienced similar difficulties in understanding and adopting quality management. The ideas behind managing quality are quite abstract.

Quality is primarily about understanding and satisfying a customer's expectations. This includes implicit expectations as well as explicit expectations. The techniques of specification, inspection and testing only make sense in that wider context.

Formal risk management developed in the late 1980s and throughout the 1990s. Risk management principles are now widely understood and applied.

Functional safety management simply applies quality management to systems that are designed to control risk.

Quality

In the early days of quality management the focus seemed to be on "Quality Control" or "Quality Assurance". Emphasis was placed on inspection and testing. Quality was about conformance to specification. Non-Conformance Reports were seen as representative of quality control.

Our understanding of quality management has evolved. Quality management principles are now better understood.

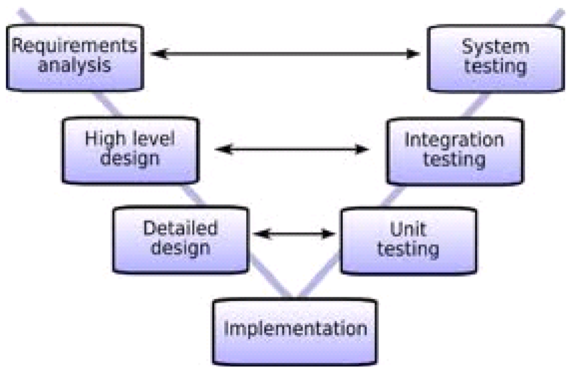
Quality begins with executive management taking overall responsibility, setting policies and implementing strategies.

Quality management principles include:

- Resource management (including competence, training and awareness)
- Management of product realisation
- Measurement, analysis & improvement
- Monitoring
- Documentation

The core of quality management is in "Product Realisation". It includes these main elements:

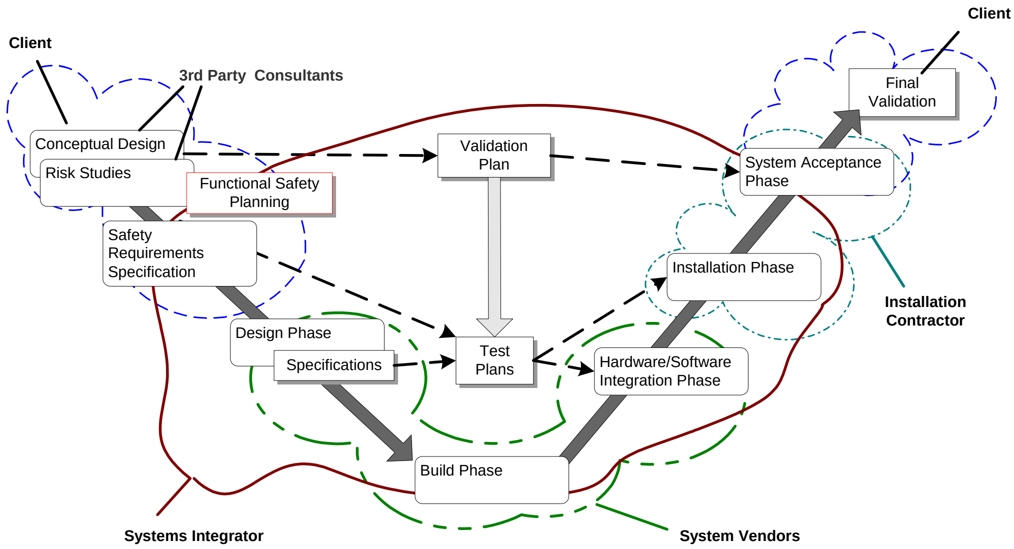
- Establishment & review of requirements
- Design and development
  - inputs
  - outputs
  - review
  - verification
  - validation
- Change control
- Purchasing



These same elements form the core of functional safety management.

Functional safety management can be seen as a specific application of quality management.

Functional safety management follows the same classic systems engineering “V-model” which is central to quality management:



Risk

In the 1980s it was not easy to answer the question of “*what should we do to improve safety?*”

It was an admirable goal but it seemed like such a vague question. It was difficult to formulate objective and specific activities without resorting to ‘motherhood statements’ such as “*safety is our number 1 priority*”.

In the 1990s the adoption of ideas like “Safety SAM” made the message easy to understand:

Spot the hazard

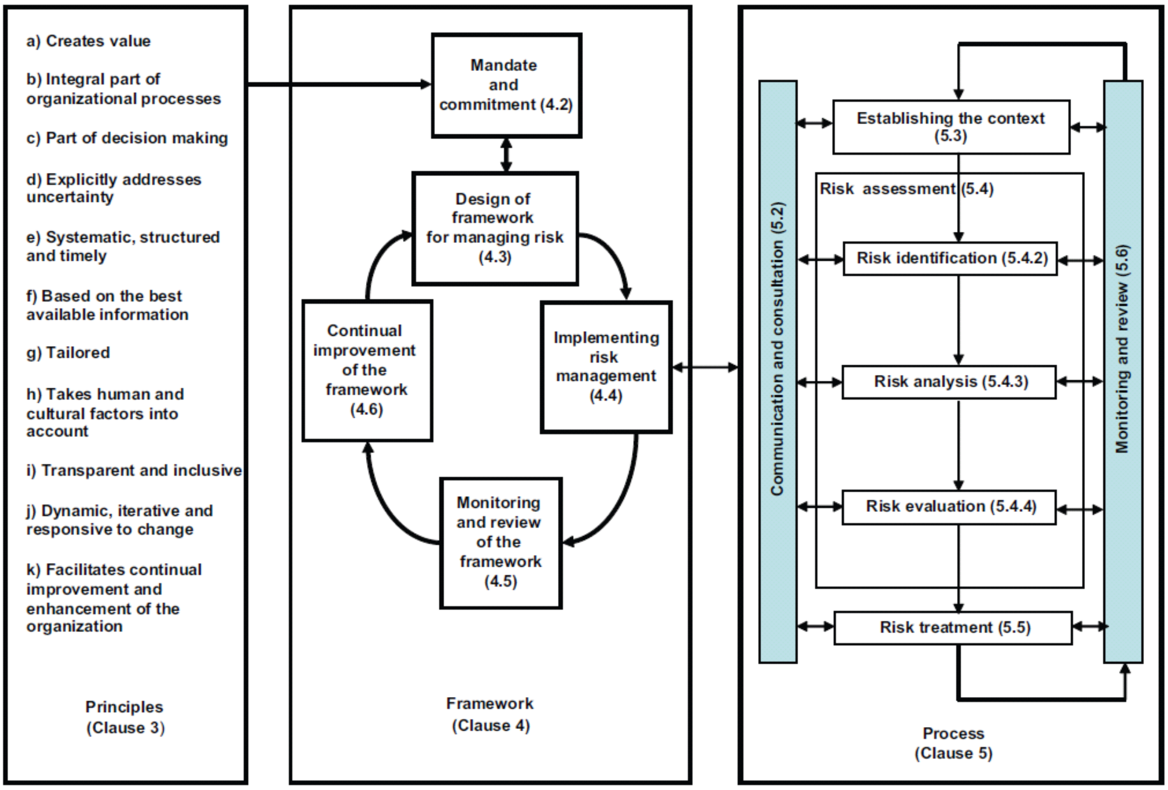
Assess the risk

Manage the hazard

Australia and New Zealand together published the world’s first risk management standard (AS/NZS 4360: 1995, revised in 1999 and now superseded in 2009 by AS/NZS ISO 31000).

Risk management principles are now well understood worldwide:

- Establish context
- Identify
- Analyse
- Evaluate
- Treat



AS/NZS ISO 31000 Figure 1
Relationships between the risk management principles, framework and process

Most operating companies now have established risk management frameworks.

The concepts of risk ownership, risk assessment and risk management are well defined and understood.

Functional Safety – Using Quality to Manage Risk

Functional safety refers to “Safety Instrumented Systems” that implement “Safety Instrumented Functions” (SIFs) as part of a company’s overall risk management strategy.

A Safety Instrumented Function is designed to respond to a specific hazardous event. It implements an action that will achieve or maintain a safe state for the equipment under control.

Functional safety must always be seen within the wider context of company risk management. It cannot be seen in isolation, it makes no sense without that broader basis.

Functional safety is just one element in a range of risk treatments. A company’s risk managers may use Safety Instrumented Functions together with a number of other risk reduction measures to control risk exposure.

The target level of risk reduction for each SIF is determined to ensure that the overall risk to personnel is as low as reasonably practicable.

Each SIF is defined with a Safety Integrity Level (1,2 or 3) according to the Risk Reduction Level that is required from that function (10^{-1}, 10^{-2}, 10^{-3}).

A Safety Instrumented System is composed of a combination of

- Sensors
- A logic solver
- Final elements such as actuators and valves

The functional safety standards provide a very specific quality management system to implement one part of an overall risk management strategy.

OHSE Context

Responsibility for managing Occupational Health, Safety and Environmental hazards is shared.

Occupational Health, Safety legislation throughout Australia requires the owners, designers, builders and operators of a facility to manage hazards. We must prevent people from being exposed to an unreasonably high level of hazard.

Clearly, we all want to avoid killing and hurting people but we are obliged to take positive action to prevent harm.

Under Common Law our Duty of Care requires us to:

- Identify appropriate standards
- Take reasonable steps to apply the standards
- Monitor compliance
- ***Demonstrate*** compliance

Ultimately the CEO of a company is accountable. The CEO needs to have evidence that “reasonable steps” have been taken to prevent harm.

Systematic Integrity

The functional safety standards deal with managing both random and systematic failures.

Management of the risks associated with **random failures** has been relatively easy to understand. Random failures can be characterised by failure rate and/or Mean Time Between Failures (MTBF).

Safety instrumentation is characterised by its "Probability of Failure on Demand" (PFD) and "Safety Integrity Level" (SIL).

The mathematics underlying failure rates, MTBF, PFD and SIL are well defined.

It is a simple process to characterise and quantify risks through estimating their **likelihood** and **consequence.**

Each Safety Instrumented Function is designed to deliver a specific Risk Reduction Factor, and that gives it a target Probability of Failure on Demand

The biggest challenge here perhaps is that we need to be comfortable in dealing with uncertainty and ambiguity.

These probabilities are evaluated in orders of magnitude. Engineers who are used to dealing with 3 or more significant figures in precision sometimes find it difficult to think in orders of magnitude.

It has been significantly more difficult to embrace the management of **systematic failures**. This is primarily to do with how we manage our engineering methods and techniques. It deals with avoiding errors and failures due to the design and implementation of the systems.

It is just as important to achieve ***systematic integrity*** as to achieve the ***safety integrity*** levels that we quantify through probabilities of failure.

The good news is that it really is not that difficult to comply. There is nothing particularly new or onerous. The principles are essentially the same as in quality management and risk management.

Functional Safety Management Planning

There is no law that specifically requires us to comply with IEC 61508 or IEC 61511.

However it is very clear that these are the appropriate standards for managing functional safety in the process industries.

A company that chooses to use Safety Instrumented Functions in managing risk needs to demonstrate that it has taken reasonable steps to comply with these standards.

There should be a deliberate process to plan how the standards will be applied. Without a plan compliance will be ad-hoc and difficult to demonstrate.

In exactly the same way that a company will have a Quality Plan, an OHSE Plan or a Risk Management Plan it should also have a **Functional Safety Management Plan.**

The need for Functional Safety Management Planning (FSMP) applies to all of the parties involved in engineering and operating a functional safety system:

- Owners
- Engineers
- Suppliers
- Operators
- Maintainers

Functional Safety Management Planning helps us to ensure that we achieve the required ***systematic integrity*** as well as achieving the required ***safety integrity.***

Planning Objectives

Both IEC 61508 or IEC 61511 outline requirements for "Management of functional safety"

The objectives in planning are to:

- Define the Lifecycle Model, i.e. which parts within the overall lifecycle are relevant
- Define responsibilities
- Specify management and technical activities
- Establish the documentation framework
- Facilitate and demonstrate compliance to the standards
- Plan the verification, validation and assessment activities
- Provide a “live” planning document that can be maintained throughout the lifecycle
- Obtain acceptance of the plan from the risk owners

Plan Outline

A typical outline for a Functional Safety Management Plan might include these headings:

- Context
- Responsibilities
- Document / lifecycle plan
- Verification Plan
- Validation Plan
- Quality Planning

The plan must always fit within the context of a company’s wider framework of risk management. It cannot be seen in isolation. Functional safety systems implement risk reduction factors that contribute to an overall risk management strategy.

Levels of Planning

It may be useful to have several levels of functional safety management planning:

- An overall company-wide plan
- A plan for an individual operating facility
- A project plan for a specific project
- The system vendors may have plans covering only their scope

This is similar to the way that quality is managed. A company that has a quality plan will usually prepare separate project execution plans for individual projects.

Document / Lifecycle Plan

The document/lifecycle plan identifies which stages of the lifecycle apply for the scope of work being planned:

- Conceptual design & requirements development
- System design & engineering

- Testing
- Installation & commissioning
- Operations, maintenance & ongoing modifications

Figure 8 in IEC 61511 illustrates the lifecycle:

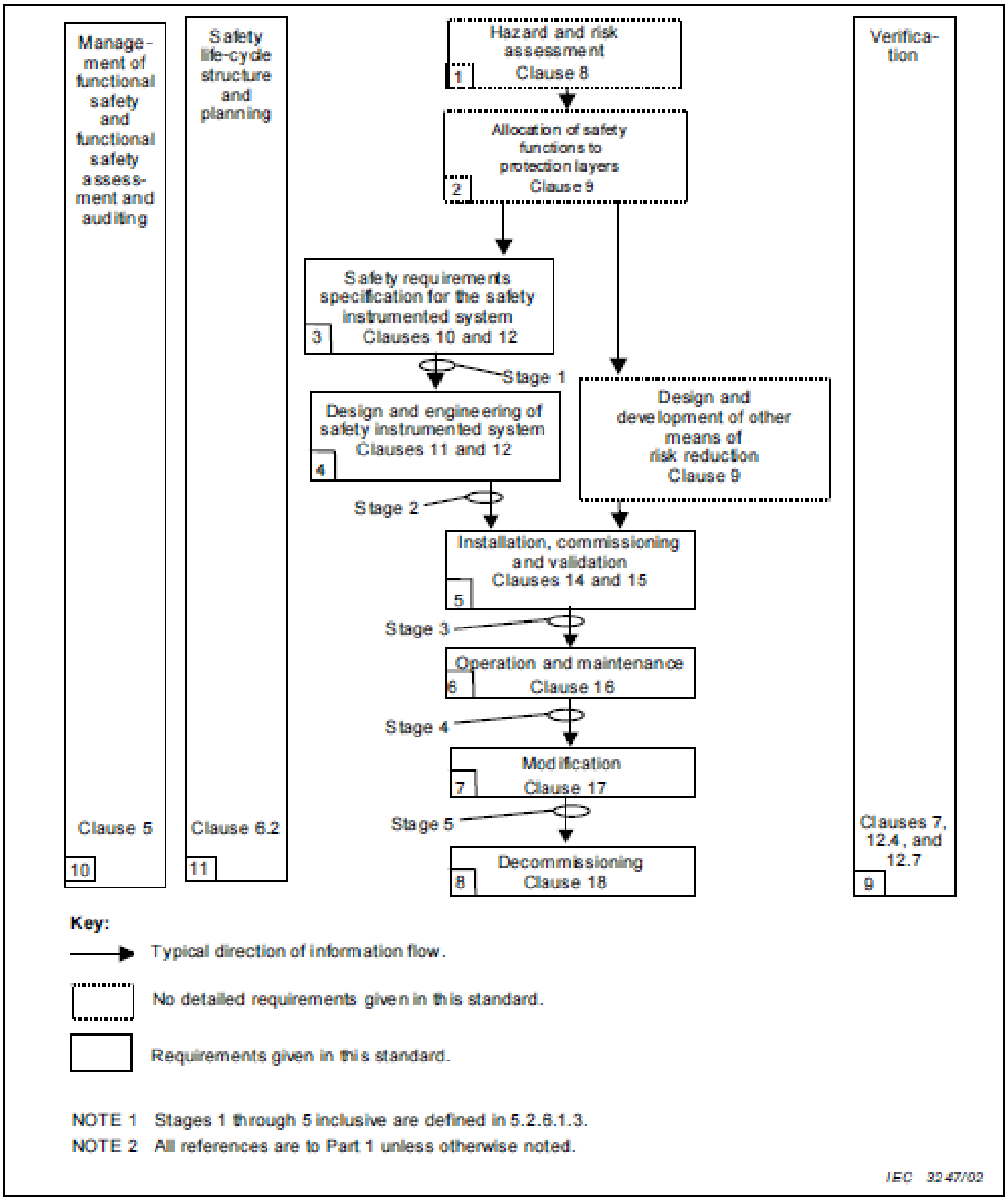


Figure 8 – SIS safety life-cycle phases and functional safety assessment stages

In practice the lifecycle phases seem to overlap. It can be hard to tell when one phase finishes and another starts.

There are key documents that are produced in each phase. It may be easier to think of these phases in terms of the status of its documents.

Different companies have different document structures. The document structures have evolved over many decades and are firmly established by tradition in each company.

To make matters worse the titles of the documents vary enormously between companies. It can be difficult to understand how the documents and the lifecycle phases are related.

It is important to help project members to understand the document structure and to identify the key documents.

Despite the many variations the key documents are simple and easy to define. The core of the structure includes:

- Risk analysis
- Requirements specification
- Detailed design specifications
- Test specifications

Requirements

The **Safety Requirements Specification** (SRS) is a collation of many elements:

- Control & Safeguarding Philosophy
- SIS Architecture Specification
- HAZOP Reports
- SIL Determination Report
- Cause & Effect Charts
- Functional Specifications
- SIF Narratives
- Ranges, Alarm and Trip Settings Schedule
- Overrides

The SRS has to be seen as a single, cohesive entity. It is the fundamental document that sets the basis for the detailed design of the system.

It must be issued formally as a "baseline" document before ***detailed*** design can start. Formal change control must be strictly applied to any changes that affect the safety requirements.

The distinction between conceptual or architectural design and detailed design is often blurred. Preliminary work on the detailed design specifications often starts before the requirements are finalised.

When the requirements are not clearly defined and controlled the design will inevitably be subject to many changes. The cost and schedule will blow out.

Detailed Design Specifications

There are many different ways of specifying detail, depending on the nature of the work. The common elements in detailed design are:

- Hardware fabrication specifications and drawings
- Software architecture

- Software standards
- Detailed ***functional*** requirements
- Detailed ***non-functional*** requirements

One of the fundamental principles in functional safety management is that the detailed design should be clearly traceable to the requirements. Just as there is no “correct” way of specifying the detail, there is no “correct” way of achieving traceability.

The objective is to:

- demonstrate that the requirements are satisfied
- allow the impact of changes through the documents to be managed.

A typical way of managing traceability is to assign unique numbers to identify each SIF and each trip group and to use these numbers throughout the suite of documents.

Verification & Validation

It is easy to confuse verification and validation because they seem to overlap.

The principles of verification and validation in functional safety are exactly the same as in ISO 9001 quality management.

Verification applies to the deliverable documents and software.

Verification is against specific and objective requirements.

Companies need to keep evidence demonstrating what was verified. The verification records should show what was actually checked, how it was checked and against what basis. Random review and checking is not enough, verification needs to be planned deliberately.

Validation is the process of showing that the commissioned system satisfies the requirements, independently of how the system was designed and built. Validation takes into account the whole hierarchy of tests starting from individual unit tests right through to final commissioning.

The whole suite of tests needs to be considered together within the context of the requirements.

Each set of tests should be defined in a detailed test specification that is traceable to the design specifications and the requirements specifications.

Multiple parties are involved in validation, the responsibilities are shared.

As validation is such a wide process it needs to be planned so that people can readily understand how it will be achieved and who is responsible for each part.

A simple Inspection and Test Plan format can make an effective validation plan.

Quality

Under the heading “Quality planning” other key issues that need to be considered include:

- Competency Management
- Procedures
- Techniques & Measures
- Supplier Quality
- Sub-Contractors & 3rd Party Contractors

- Change management
- Requirements Tracking & Traceability
- Configuration Management
- Issues Management
- Incidents & Performance Analysis
- Functional Safety Audits & Assessments

IEC 61508 provides very detailed guidance on the techniques and measures that are necessary to achieve specified systematic integrity throughout the engineering design process.

Functional Safety Audit & Assessment

Audit and assessment are easily confused, but they are distinctly different.

Audit is a review of compliance against the procedures. It reviews whether ***the process*** is being followed as planned. It provides feedback to the project team on whether the procedures and work practices are functioning effectively. Functional safety audits follow the same principle as quality audits.

The objective of functional safety ***assessments*** is to enable a judgement to be made as to the functional safety and safety integrity achieved by a safety instrumented system. The assessor recommends for acceptance, qualified acceptance or rejection of the systems assessed.

An assessment reviews whether ***the product*** system meets the requirements. An assessment will often make use of audits in order to make a judgement but it is more than an audit. It is independent assessment of whether the required risk reduction has been achieved.

Summary

Deliberate Planning

A Functional Safety Management Plan is an essential tool in achieving systematic integrity. It facilitates and demonstrates compliance to the standards. The plan:

- Provides context
- Defines the key documents
- Outlines management practices
- Clarifies responsibilities

A Functional Safety Management Plan is similar to a Quality Plan. Functional safety management must always be seen in the context of the operating company's overall risk management framework.

Different parties and different phases might have different (complementary) plans.

Structured Documents

The documents for controlling the implementation should be clearly structured and easy to follow. The core documents are:

- Risk analysis
- Requirements specification
- Detailed design specifications
- Test specifications

The Safety Requirements Specification provides a firm basis for the system.

The detailed design documents must be traceable to the requirements.

Verification records must be kept for the deliverable documents and software. They should show what was actually checked, how it was checked and against what basis.

Validation is the process of showing that the final system satisfies the requirements. An overall Inspection & Test Plan is essential for validation planning. Complete test & validation records must be kept.

Formal change control must be applied for any change that impacts on the requirements.

Audit & Assessment

When a plan has been established it is a simple matter to monitor implementation against the plan.

Functional safety audits provide an effective tool for monitoring compliance. These are similar to standard quality audits.

The standards require an independent functional safety assessment of the functional safety and safety integrity achieved by the completed safety instrumented system.