



Functional Safety – A General Overview

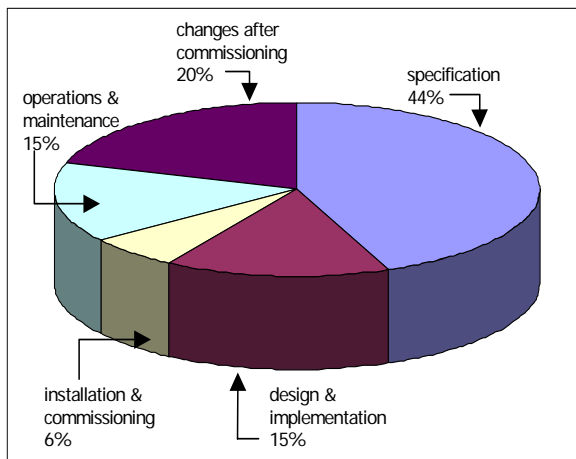
Challenges faced by industry today include unremitting pressure to reduce costs coupled with shorter product life-cycles, a need for ever shorter time to market, and pressure to maximise the use of the asset base. Industry continually strives to improve performance and profitability while maintaining and improving safety. In addition, there are regulatory and social requirements for safety and reliability, and for protecting the environment.

Against this background industry is experiencing a revolution in rapidly evolving safety technologies, all which have an increasing reliance on computer-based control and safety solutions.

It is important to exploit this modern technology so as to facilitate improvements in both safety and economic performance. But this must be done within an overall safety framework which maintains an appropriate level of safety and which provides confidence that this is being achieved.

Where do most Hazards Occur?

Studies carried out by HSE of incidents involving process control systems show that the majority stem from relatively few causes.



(From 'Out of Control' A compilation of incidents involving control systems, by the UK HSE)

In addition, computer control and embedded software were becoming more commonplace, thereby increasing concerns about the possibility of 'hidden' risks buried within complex coding.

Due Diligence

In the UK, the Consumer Protection Act requires that goods supplied into the market are 'of marketable quality', expecting suppliers to exhibit due diligence to ensure this. Similar legislation exists in other countries. Where national or international standards exist for this purpose, any supplier not applying them would have difficulty pleading 'due diligence'.

What is the HSE Position?

It is recognised by the UK Regulators, the Health and Safety Executive (HSE), that good practice such as that laid down in the functional safety standards can help to achieve good health and safety performance. The HSE may use IEC 61508 and related industry-specific standards as a reference for determining whether a reasonably practical level of safety has been achieved.

So what is Functional Safety?

Functional Safety is concerned with equipment whose failure could have an impact on the safety of persons and/or the environment. The relevant standards which are now widely accepted are:

IEC 61508 - the *generic standard*. It provides a firm basis for the specification, design and operation of electrical or electronic (including software controlled) safety systems and allows the potential of this technology to be realised fully and safely. It also forms the basis for the following related industry-sector standards.

IEC 61511 - Functional safety of safety instrumented systems for the process industry.

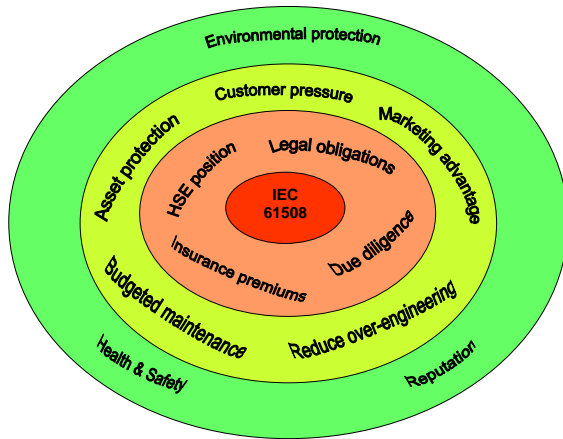
IEC 61513 - Nuclear power plants: Instrumentation and control for systems important to safety.

IEC 62061 - Safety of machinery: Functional safety of safety-related E/E/PE control systems.



Other Benefits

By following best practice for managing plant safety as set out in these standards, not only can insurance premiums be reduced, but also health and safety inspections may be more easily progressed.



What is the Scope of Functional Safety?

The approach used covers all the activities described in the HSE pie chart described overleaf, from entire systems down to components contributing to safety, including hardware, software and procedures.

Safety Integrity Level (SIL)

Four levels (SILs) of safety performance are specified for a safety function: SIL 1 being the lowest and SIL 4 the highest, according to the degree of risk that must be reduced. The SIL is an indication of the probability of failure of the safety function. Safety functions with higher SILs require more rigour in terms of the design, testing and methods used in the development.

Note: The SIL relates to the overall safety function being performed **not** to the individual component parts of the system. Any use of the term 'SIL' in relation to components must be treated with extreme caution and looked at in the context of their application.

Organisation and Competence of Personnel

An important aspect which is assessed is the ability of an organisation to manage any of it's

activities that could have an impact on functional safety, such as it's quality process and the competence of it's staff.

What Else Does it Cover?

Being generic, the principles in the standard can also be applied to other technologies such as mechanical, hydraulic or pneumatic which are used, for example, in pipeline emergency shut-down systems.

Studies have shown that perhaps 50% of problems in the field are the result of valves, actuators and/or solenoids failing to respond, often because they remain in one position for long periods, making them difficult to operate when needed. IEC 61508 provides a framework to define the reliability of such devices using whatever technology. Analysis of historical reliability data for these elements can determine the component's suitability for use in a safety function with a given SIL.

Protection of Environment and Assets

An identified hazard may not be one that affects the safety of individuals directly, but one which compromises the integrity of the **environment** or of costly **assets**. Again the strategy of the standard is valid, and the only difference is in the choice of criteria for quantifying the hazards and the integrity levels for the risk reduction factors.

How can Sira Help?

Sira provides a range of services to enable you to benefit from the advantages of functional safety.

- Technical advice & Training.**
- Product certification.**
- Company certification.**
- Independent third party assessments.**
- Staff competence.**

More Information

For further information please contact Sira:

Tel: +44 (0) 1244 670 900
Email: functionalsafety@siracertification.com
Web: www.siracertification.com