UNDERSTANDING FUNCTIONAL SAFETY

AN OVERVIEW OF THE IEC 61508 STANDARD AND ITS APPLICATION AND BENEFITS

As the integration of automated safety systems expands globally across diverse industries – including process, household and commercial products, medical, nuclear, automotive, railway and avionics – the importance of functional safety evaluation and certification has become recognized internationally. Today functional safety certification is widely considered to be an essential tool to control and mitigate risk, particularly in those cases where a failure could lead to serious injury or death.

Those unfamiliar with the concept of functional safety may find the subject difficult to understand and place within the context of traditional safety and reliability assessments. However, designers who understand and embrace the concept of functional safety – and who demonstrate that products or systems conform to the requirements of recognized functional safety standards – are equipped to better manage risk while also capture increased share of market among the growing ranks of customers who also seek to meet the requirements of functional safety standards.

This paper provides an overview of functional safety concepts, standards requirements and methods of compliance. It is intended to help readers understand the importance of functional safety and the advantages of obtaining formal evaluation and certification services performed by an independent third-party.

Why Functional Safety?

IEC 61508 is the international standard for safety related systems associated with electrical, electronic and software-based technologies. The principles of the standard can also be extended to assess mechanical elements if they are used in the safety function.

IEC 61508 is an umbrella (generic) standard, intended to form a basis for sector-specific standards, including:

- IEC 61511 **process** industry
- IEC 61513 **nuclear** industry
- IEC 62061 & ISO 13849 **machinery** industry
- EN 50402 **gas detector systems**
- EN 50126 **rail** industry

Evaluation and certification of systems and products to confirm that the functional safety requirements of IEC 61508 have been met is just one of the methods of dealing with hazards control. An appropriate initial hazard analysis must be implemented to define the level of risk and determine if functional safety is necessary to ensure adequate safety protection.

The IEC 61508 standard defines requirements for determining the level of risks and describes the lifecycle process for ensuring that systems are designed, validated, verified, operated and maintained to perform a specific function or functions to ensure risk is kept at an acceptable level. IEC 61508 defines four SILs according to the risks involved in a safety related system application, with SIL4 used to protect against the highest risks.

Safety function requirements are defined though a hazard analysis while safety integrity requirements are derived from an assessment of acceptable risk. IEC 61508 may cover both determining the SIL level of a product and verifying the manufacturer specified safety integrity level (SIL) level. The higher the SIL assigned to the safety system or component, the lower the likelihood of dangerous failure. Instruments covered by these requirements might include sensors, detectors, signal conditioners, logic controllers, monitors, alarms, actuators, valves and motors.

Demonstrating Functional Safety

In a highly complex, safety-related system where functional safety is required, equipment suppliers should identify an accredited approval body (third body) that can evaluate and certify compliance with the IEC 61508 or applicable industry-specific standard. Accreditation means that the third-party agency has an internationally recognized approval that qualifies it for functional safety conformity assessment.

The agency should demonstrate its experience and expertise in functional safety with a highly knowledgeable staff capable of carefully performing conformity assessment requirements while providing levels of service that help clients optimize their businesses. Agencies should be independent third parties subject to annual audits by the accrediting body. Qualifying agencies must provide annual compliance evidence to the accreditation agency as proof of full conformance with the requirements of IEC 61508.

The Benefits of Functional Safety

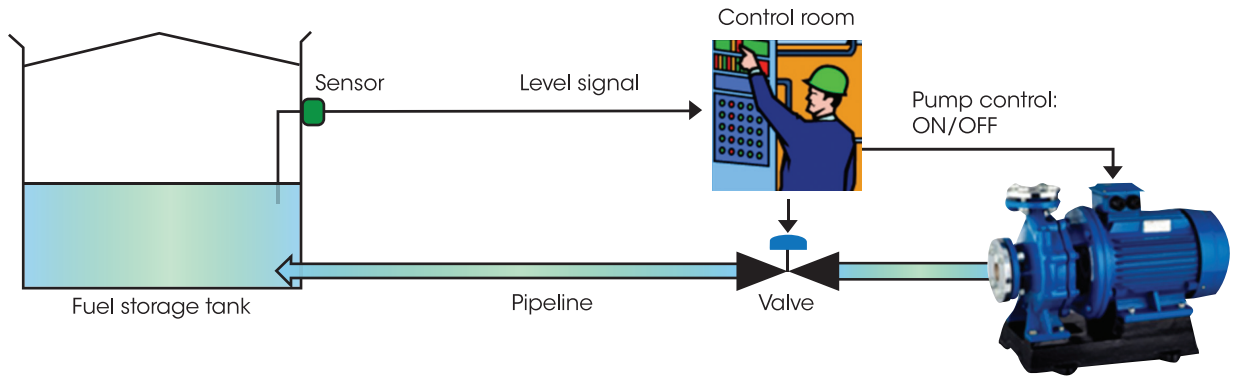
Evaluation of systems and components, and certification that they meet the requirements of the applicable functional safety standards, provides designers, owners, operators and other stakeholders with increased confidence that processes operate safely, products meet regulations and industry requirements, risk has been appropriately managed, and the potential for costly litigation has been minimized.

Equipment suppliers can also leverage their functional safety certifications to gain market advantage, access new markets and achieve sales growth among customers who require products that meet a given SIL for use in their safety related applications or systems. This "product-of-choice" status is reinforced by subsequent positive assessment reports from customers whose products and systems are also certified, further demonstrating full compliance with functional safety requirements.

Organizations that provide a safety related service, or operation involving safety systems, can be approved for the technical and management processes that govern their functional safety activities (e.g., plant operators, systems integrators, contract designers, product suppliers etc). This type of approval covers the organization's generic processes as well as the competency of its staff. This approval can be very useful in earning new business, or in satisfying ongoing contractual or regulatory requirements.

Example of Functional Safety

The following example explains the basic principles of functional safety. The diagram below shows a relatively simple operation from the process industry: filling a bulk storage fuel tank. Questions that must be answered initially include: What hazards are associated with this application? What can go wrong in the process? What are the risks? How safe is the application? How safe does it need to be? Other questions may also apply.



In this illustration, tank overfill is clearly one of the main hazards that must be addressed.

That might sound basic, but consider what can happen if an overflow occurs…

Oil storage depot, Buncefield, UK, December 2005

Miraculously, no-one was killed in this incident (it was 6:00 am on a Sunday morning), but dozens of surrounding businesses were devastated. Several companies were prosecuted and found guilty in criminal and civil courts – including the owner/operator, the control system supplier and one of the instrument suppliers. The incident could have been prevented if the hazard and risk had been correctly identified and an appropriate target SIL established, resulting in the implementation of an appropriate overfill protection system and an operational functional safety management system.

In a scenario like this, specifying a "safety-related system," usually called a *"Safety Instrumented System"* (SIS) in the process industry, can reduce risk to a target SIL deemed acceptable based on assessment of the hazard. Depending on the target SIL, risk level can be reduced by at least…

- SIL1 by ≥10 times
- SIL2 by ≥100 times
- SIL3 by ≥1,000 times
- SIL4 by ≥10,000 times

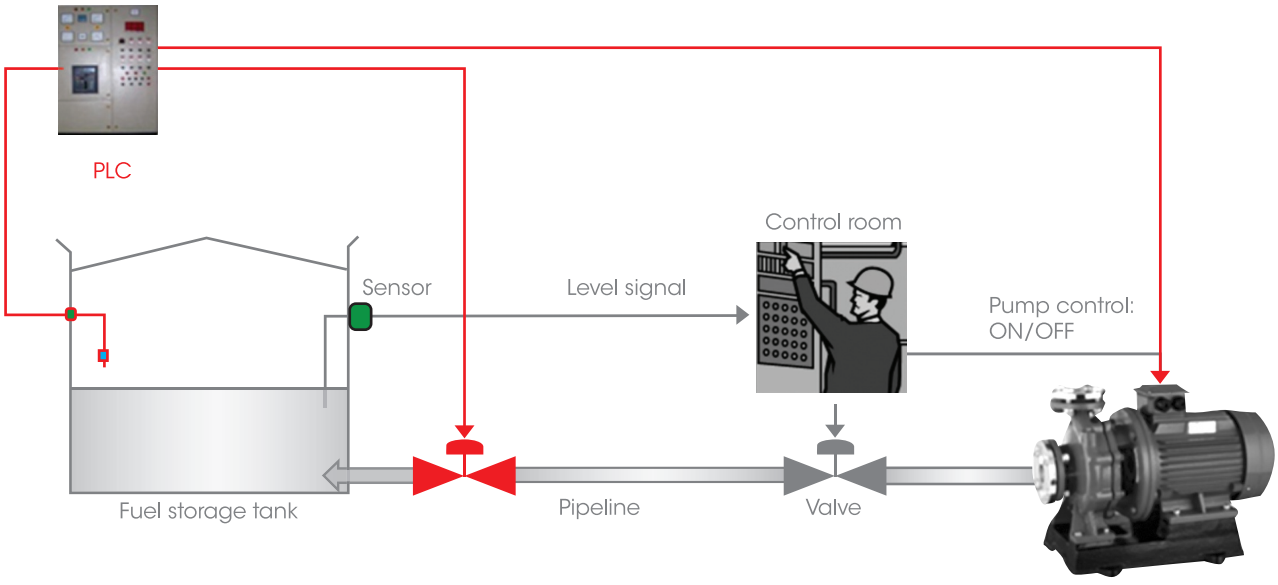
SIS Implementation

With the hazard and risks identified, safety requirements can be assessed and an acceptable target SIL established, resulting in the design of a safety related protection system – an SIS loop – implemented as shown below.

The SIS (in red) in this example might be specified as follows:

Safety Function: To close the emergency shut off valve and switch off the pump in the event that the high-high level switch contacts are opened

Safety Integrity: To perform the safety function to SIL2 (that's a probability of the independent safety function failing to work of less than 1 in 100 trips)



Basic Steps in Achieving Functional Safety

1) SIL Determination

Once the hazards and risks have been identified, using "HAZOP" analysis, a *SIL Determination* study can be prepared (normally arranged by the plant/machine operator) to establish the *Safety Function(s)* and the amount of risk reduction required of the safety system, which then defines its SIL. The IEC 61508 standard shows the requirements for failure data which are expressed either as a ***probability of failure on demand*** (PFD) for a "trip" safety system or as a ***failure rate*** (for a safety system that has to respond more frequently or even continuously).

Each SIL has its own range, with an "order of magnitude" between end points. If the demand from the process on the safety function is predicted to be less frequent than once a year, it is classed as a *low demand* system; if the demand is more frequent than once a year, it is a *high demand* system. (A continuous mode safety function is where safety is achieved by continuous or linear control of the plant/machine). It is important to get the distinction between high and low demand right as the mathematics used to derive the requirements are different. Once the safety instrumented system is in operation, all demands (whether "nuisance" or valid) should be logged, investigated and compared with what was predicted at SIL determination.

2) Safety Requirements Specification

Once the target safety functions and safety integrity have been determined, the Safety Requirements Specification (SRS) should be prepared, as it is one of the most important phases in the lifecycle. Functional safety standards emphasize the importance of capturing functional requirements, deriving more detailed design requirements (right down to low level hardware and software) and tracing these through the design and development stages, integration and testing process, and through to final validation (assessment to the product lifecycle). At the end of every stage of the product lifecycle, a verification process must be followed to capture any details not fully addressed that can affect compliance. This supports avoidance of systematic failures. For complex or high-integrity safety systems, capture of formal requirements and associated testing require trusted automated tools. The safety system (including all instruments) should then be designed and realized to achieve the numerical SIL requirements identified for the safety function.

3) Random Hardware Failures

Systems fail due to random hardware failures and systematic failures. Random hardware failures typically stem from the components used in assembly and the design architecture. The *probability* that the safety system will fail to perform its designed safety function must be estimated using numerical and analytical techniques. A quantitative assessment is performed to ensure the specified figure is achieved.

A theoretical model of the equipment's reliability must be constructed, decomposing the design into functional blocks to form a *"Reliability Block Diagram"* (RBD). Other methods such as Fault Tree Analysis can also be used. Modelling is particularly required for more complex designs.

Common Functional Safety Terms and Concepts

- *Functional Safety* is when safety relies on:
  - **Safety function(s)** – what the equipment *does*, and
  - **Safety integrity** – *how reliably* the equipment does it
- It is aimed at systems, typically formed from discrete instruments such as:
  - Sensors (to detect for unsafe process/machine conditions)
  - Logic solvers (decision making or controlling devices)
  - Output elements (devices that physically interrupt or halt the process/machine to make the situation safe)
- It is concerned with *how* the systems/ instruments can *fail*: **failure modes**
- How *likely* will the system/instrument failure mode occur: **failure data**
- The SIS is used to reduce the risk(s) to an "acceptable level" (a figure generally accepted by society and legislators)

Continued on next page

Each "block" down to component level must be analyzed, using methods such as *Failure Modes and Effects Analysis* (FMEA). During this analysis, it is necessary to determine how the failure of each component affects the equipment's safety function. Failures can be a combination of safe and dangerous depending on the definition of the safety function.

The outcome of the FMEA for each block is a sum of the different types of failures (safe and/or dangerous). Using the Reliability Block Diagram, the different failure rates can be grouped into categories, such as safe failures or dangerous (detected or undetected); the probability of failure on demand (PFD) can be then calculated for the equipment.

In addition to meeting the PFD requirement, it is necessary for the equipment to meet certain *architectural constraints* such as the safe failure fraction (SFF) and the hardware fault tolerance (HFT) outlined in the standard.

This analysis can be performed using information from circuit diagrams, mechanical assembly drawings, parts lists, and other sources, and therefore can be undertaken *following* design. It requires a detailed knowledge of component failure rates, their various failure modes and how these can affect the functionality of the instrument used in the safety function. The analysis is a specialist area and should only be undertaken by analysts with the appropriate tools, competence and access to the appropriate failure rate data in order to yield a statistical prediction of the random hardware failure.

4) Systematic Failures

The second reason for system failure is weaknesses in the processes used in the specification, design, test, installation, use, modification and repair of the safety system (known as the *"lifecycle"*). These *systematic failures* cannot be modelled and determined statistically. Instead they must be avoided by using processes and techniques of sufficient rigor for the SIL involved. These are prescribed in the IEC 61508 standard.

The verification of systematic failures (hardware or software) require a qualitative assessment of the evidence of using the prescribed lifecycle, although the actual processes and work activities used will depend on the technologies in the design and type of safety equipment in question. For equipment developers, evidence of using these methods must be gathered *during* the design and made available for assessment.

5) Software

Software requires special attention from the developer if it is involved in performing the safety function. Software defects are a specific type of systematic failure and a full discussion is beyond the scope of this paper. However, these points should be noted:

- Ensure requirements are *fully captured* and *traceable* through the development lifecycle
- Remember the linkage between hardware and software – FMEA is a rich source of generating software requirements to achieve hardware diagnostic coverage
- Develop a *software review culture* (and keep evidence; informal log books are fine)
- Modifications must include an *impact analysis* and proof of the implementation process
- Configuration *management* is critical, including versions of test and development tools
- *SOUP* (software of unknown provenance) and *COTS* (commercial-off-the-shelf) are best avoided, or extreme care should be taken in their use
- Invest in and maximize the use of *automated test tools* – anything repetitive or requiring manual effort to generate test cases or logging results will lend itself to such tools
- *Static analysis tools* – some are very affordable and offer great benefit; the deeper and wider the analysis the better
- *Coding standards* – this is an essential requirement to ensure correct and safe constructs and a safe language sub-set are used
- Use recommended (*Misra C and approved development tools*) to facilitate the structure of the safety software compliance
- For systems integrators, achieving compliance to *IEC 61511* is relatively straightforward

Common Functional Safety Terms and Concepts *Continued*

- The level of risk reduction required from the SIS will define its Safety Integrity Level ("SIL"). The SIL places:
  - Limits on the probability of random hardware failure, and
  - Requirements on the systematic failure during the development process known as the "lifecycle" used during the product realization phase
- Note that before a SIS is specified, risk control is already reduced as much as possible by conventional measures such as good (safe) process/machine design, the basic control system, alarms, trips, relief systems, procedural measures, etc.

6) Functional Safety Assessment

All safety systems must undergo an independent *functional safety assessment* (FSA) covering the hardware and software as well as all the related processes used in the realization of the instrument/system. The FSA applies to all activities in the life-cycle of the safety system or instrument.

Requirements for the FSA are defined in IEC 61508-1 section 8. The accredited certification process is defined by the international standard for certification ISO/IEC 17065, which was published in September 2012 and replaces EN 45011 and ISO Guide 65. This change dictated the need for changes within Certification Body (CB) management systems and processes in order to maintain UKAS accreditation in. ISO 17065 covers many of the requirements with respect of the assessment body. The requirements for the assessment, including the methods and techniques prescribed, increase in rigour with higher SIL. There is a minimum level of independence between the assessment team and the work being assessed, which depends on the SIL and the lifecycle activities being evaluated.

7) Management of Functional Safety

IEC 61508 makes it clear that all organizations that deal with safety instrumented systems should operate a functional safety management (FSM) process. This could be a company-wide process, typically part of the company's Quality Management System, and should include the additional elements required for functional safety. Alternatively, it could be implemented as an overarching plan that covers a specific project and details how functional safety will be achieved. Either way, FSM is indispensible to avoid systematic failures and for creating a safety culture. No product, system or operation can claim to conform to the IEC 61508 standard without this critical assessment, which should govern all safety-related work activities from concept to decommissioning.

An important part of the FSM is the development structure, deployment and assessment of the *competence* of all staff that have any roles or responsibilities associated with safety systems. For companies starting a functional safety project for the first time, FSM is a good place to begin as it establishes the procedural infrastructure in advance.

Conclusion

History (past and recent) shows there is a great need for industry to provide evidence of the reliability of automated safety systems to ensure the safety of people, the environment and corporate assets. *IEC 61508* (and related standards) provides the systematic lifecycle approach necessary to achieve functional safety. Around the world, new and existing plants are being measured against the criteria of this standard and market requirements for instruments that are suitable for SIL-rated systems are now commonplace. This enables instrument suppliers to benefit commercially from functional safety certification, increasing their market advantage by earning "product-of-choice" status among current and future customers.

About CSA Group

CSA Group was the first certification body in the world to be accredited to issue functional safety certification to IEC 61508 by UKAS for both products and companies (FSM). It has undertaken more than 300 functional safety projects for clients worldwide in the past five years. These projects have been as diverse as simple electro-mechanical switches, actuators, and valves, to highly complex programmable protection devices and embedded real-time operating systems, up to SIL3 compliance. CSA Group's team of functional safety specialists has experience in a wide range of industry sectors and applications, including safety of machinery.

CSA Group offers a wide range of functional safety compliance assessment services – from household equipment, software evaluation, FSM and product certification, to services for wide sectors in the process industries. CSA Group's functional safety program offers a full-service global solution to manufacturers of equipment used in hazardous locations and in critical applications.

The ***CSA Certified***® advantage: helping manufacturers get the market access they need for over 95 years.

Contact CSA Group to obtain more information about our global functional safety evaluation and certifications services:

Call 1.866.463.1785 or
visit **www.csagroup.org** or
email us at **certinfo@csagroup.org**