



IEC 61508/11 FUNCTIONAL SAFETY

Datasheet

If you rely on an electrical, electronic or programmable electronic system for the safety of any part of your processing operation, there is a need to verify and demonstrate the performance and integrity of the system. IEC 61508 is a generic standard on which specific industry sector safety related standards are to be based. For the process sector IEC 61511 is in preparation and like IEC 61508 outlines a preferred lifecycle for any Safety Instrumented Systems. Its international adoption provides an accepted benchmark for determining the Safety Integrity Level, design requirements and test intervals for Safety Instrumented Systems.

IEC 61508

This standard is concerned with structuring the safety lifecycle for electrical, electronic or programmable electronic, (E/E/PES) technologies that are used to perform safety functions in operational activities. Essentially the standard covers the front end safety, detailed design stages, maintenance/test schedules and eventual decommissioning of safety instrumented systems.

The IEC 61508 Functional Safety methodology requires that you:-

- Define the Equipment Under Control (EUC) and its operating environment, sufficient to enable a detailed hazard identification and risk assessment to be undertaken relating to both people, the environment and in some cases the asset base.
- Ensure that the hazard identification and risk assessment identifies what is at risk, the likelihood of any hazardous event occurring and the sequence of events that leads up to it. Finally it should identify the consequences of the hazardous event.
- Determine the tolerable level of risk for each hazardous event and define any risk reduction measures required.
- Determine the Safety Integrity Level (SIL) required for each Safety Instrumented Function (SIF) used to reduce the risk.

LIFECYCLE REQUIREMENTS

For each EUC component and its Safety Instrumented System (SIS) you need to provide lifecycle documentation which includes a definition of the tolerable risk levels for each hazard, the results of each risk assessment and finally determination of the appropriate SIL. You should be able to demonstrate that the design, installation and proof testing of the equipment meets the desired SIL, and that Design Change Control procedures are in place with records of any changes made to the system. This should also take into account a review of the impact of change on the overall basis of safety of the EUC.

It is essential that a functional safety management system is used to ensure the requirements of the overall safety lifecycle are delivered. However, equally important is **verification** and **validation** of the SIS in terms of audits, analysis and testing to show the specification and requirements of each lifecycle phase have been met.

WHY IEC 61508?

IEC 61508 is a standard that can be methodically applied to both the end user and supply chain organisations. It covers the requirements of hazard identification, the E/E/PES design realisation and operations & maintenance aspects of the proposed safety related systems. Additionally the standard also promotes the use of quantitative or qualitative tools and techniques to identify the process risks and hazards.



IDENTIFICATION OF HAZARDOUS EVENTS

Fundamental to the overall safety lifecycle process is the identification of hazards. This covers the nature of materials used, the process itself including the operating conditions and also interaction with the legislative environment. Key to this are the principles of inherent safety relating to risk reduction, such as elimination, mitigation or separation. However once these have been applied there will still be hazards that remain within the operation.

It is identification of the remaining hazards that is crucial to ensuring that the correct level of risk reduction is applied. This will be achieved using an appropriate hazard and risk analysis technique which results in a series of measures being identified in order to prevent the hazardous event from occurring or mitigating its effects. These protective measures can either be in the form of safety instrumented systems, mechanical relief systems, bunding containment or emergency procedures combined to form protective layers.

IEC 61511

The process industry specific standard, IEC 61511, is similar in nature to IEC 61508 and utilises a simplified functional safety lifecycle and terminology more relevant to the Process Industries. IEC 61511 does not replace IEC 61508 but is seen as an essential additional safety standard.

Again core to the IEC 61511 lifecycle is the hazard and risk assessment process and allocation of safety functions. The standard concentrates on the detailed specification for E/E/PES system architectures, hardware and software configurations and associated operation, maintenance, verification and validation requirements.

It is seen as a standard that can be readily applied by the end user and engineering design system integrators. It provides additional guidance for the selection and integration of hardware and software designated SIS within the Process Industries.

HOW CAN CHILWORTH TECHNOLOGY HELP?

Chilworth Technology has nearly two decades of experience in providing hazard and risk assessment to the process industries. We can provide:-

- Front end hazard analysis.
- Inherent safety reviews.
- Impact and change hazard analysis.
- Safety allocation requirements for SIL's.
- Operation & modification of safety related systems.
- Functional safety management auditing.

In support of these activities, Chilworth can also draw upon our GLP compliant Process Safety Laboratories in the provision of safety test data, if it is not already available.

faxback

Please faxback to Marketing on +44 (0)23 8076 7866

Name:..... Job Title:.....

Company Name:.....

Address:

..... Postcode:..... Country:.....

Telephone: Fax:.....

Email:

My particular interests are:-

Inherent Safety and Applicable Legislation Incident Investigation / Expert Witness

Hazard Analysis and HAZOP Hazardous Area Classification.....

SIL Determination..... ATEX / DSEAR audits

Functional Safety Management & Assessment Chemical Reaction Hazards

Mechanical Relief Design (DIERS) Dust/Gas/Vapour Explosion Hazards.....

Training Electrostatic Hazards / Problems.....

I would like a FREE talk to a consultant about a process safety matter.....

I would like a FREE visit from a consultant next time one is in my area

For further information phone Chilworth Technology on +44 (0)23 8076 0722

Chilworth Technology Ltd., Beta House, Chilworth Science Park, Southampton SO16 7NS UK