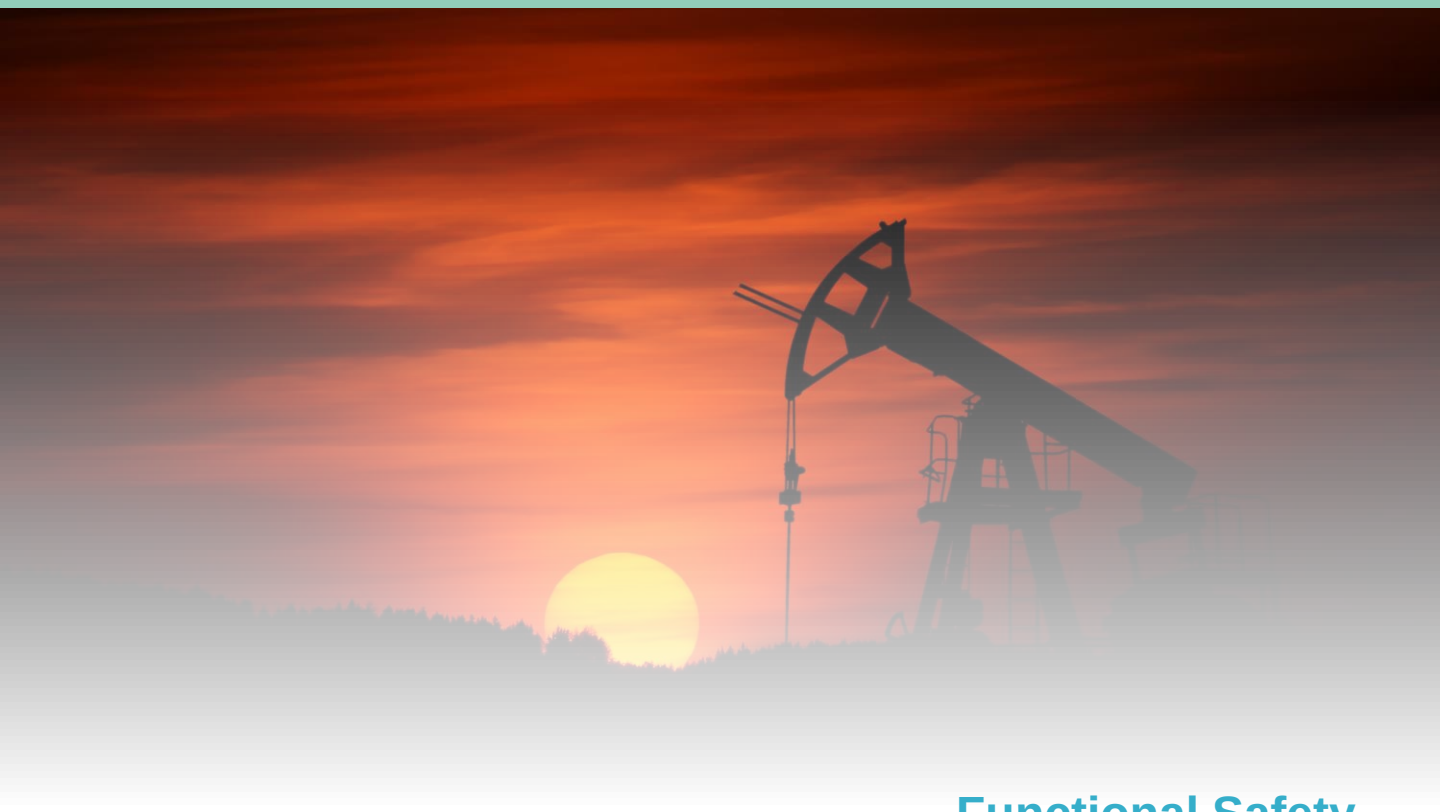
Engineering Safety Ltd.

International Provider of Functional Safety, Engineering Safety and Inspection Consultancy

Functional Safety Services

Engineering Safety Ltd, (ES) is an international provider of Functional Safety Consultancy, Engineering Safety and Inspection Consultancy Services

ES are competent in providing practical solutions that emphasise the application of the appropriate level of rigour for various industries and applications. Our solutions and services are tried and tested, implemented by major operators in the process industry and accepted by regulating bodies.



Functional Safety

Compliance to the international Standards such as IEC 61508 and IEC 61511 are imperative to meeting the Functional Safety requirements for many processes and have formed part of the quality management systems of many companies. Provision of Functional Safety Services in line with the Phases and Activities detailed in the Functional Safety Life-cycle is an area in which our consultants have demonstrated vast experience and expertise.

Functional Safety Services

- Management of Functional Safety for control and minimisation of Systematic Errors.
- Reliability Assessment in terms of Random Hardware Failures.
- Architectural Assessment and requirements for Hardware Fault Tolerance.

Input of expert consultancy services in Front End Engineering or Detailed Design stages are key in achieving Functional Safety. Support in procurement, design and implementation of Safety Instrumented Systems are imperative in meeting the safety requirements of a project. ES can provide the required functional safety consultancy support in meeting the project and industry needs.

Process Hazard Analysis

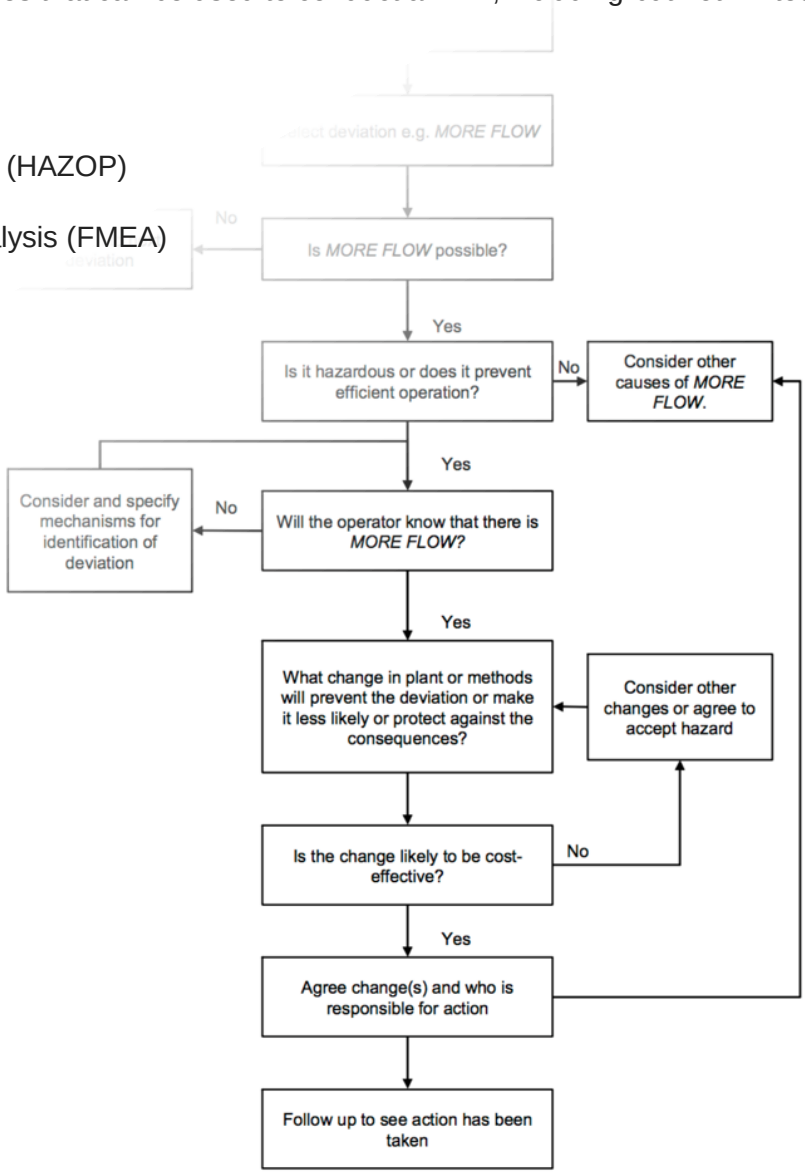
Process Hazard Assessment (PHA) is a set of organised and systematic assessments of the potential hazards associated with an industrial process. A PHA can provide information intended to assist in making decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. A PHA is often directed towards analysing potential causes and consequences of undesirable events and focuses on equipment, instrumentation, utilities, human actions, and external factors that might impact the process.

PHA methods are qualitative in nature. The selection of a methodology to use depends on several factors, including the complexity of the process, the length of time a process has been in operation and if a PHA has been conducted on the process before, and if the process is unique, or industrially common.

Methods of Process Hazard Analysis (PHA)

There are a variety of methodologies that can be used to conduct a PHA, including but not limited to:

- Checklist
- What if?
- Hazard and Operability Study (HAZOP)
- Hazard Identification (HAZID)
- Failure Mode and Effects Analysis (FMEA)



SIL Classification

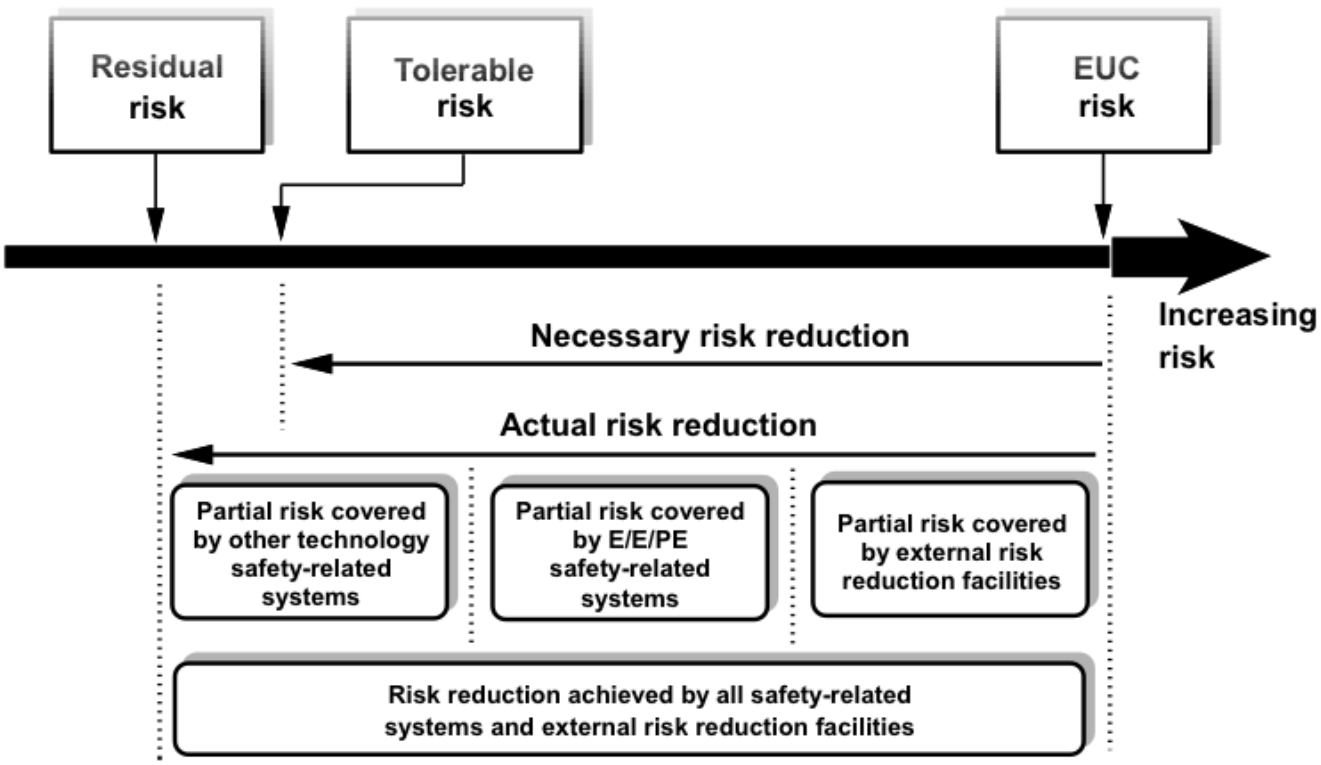
The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency of the hazardous event and its specific consequences.

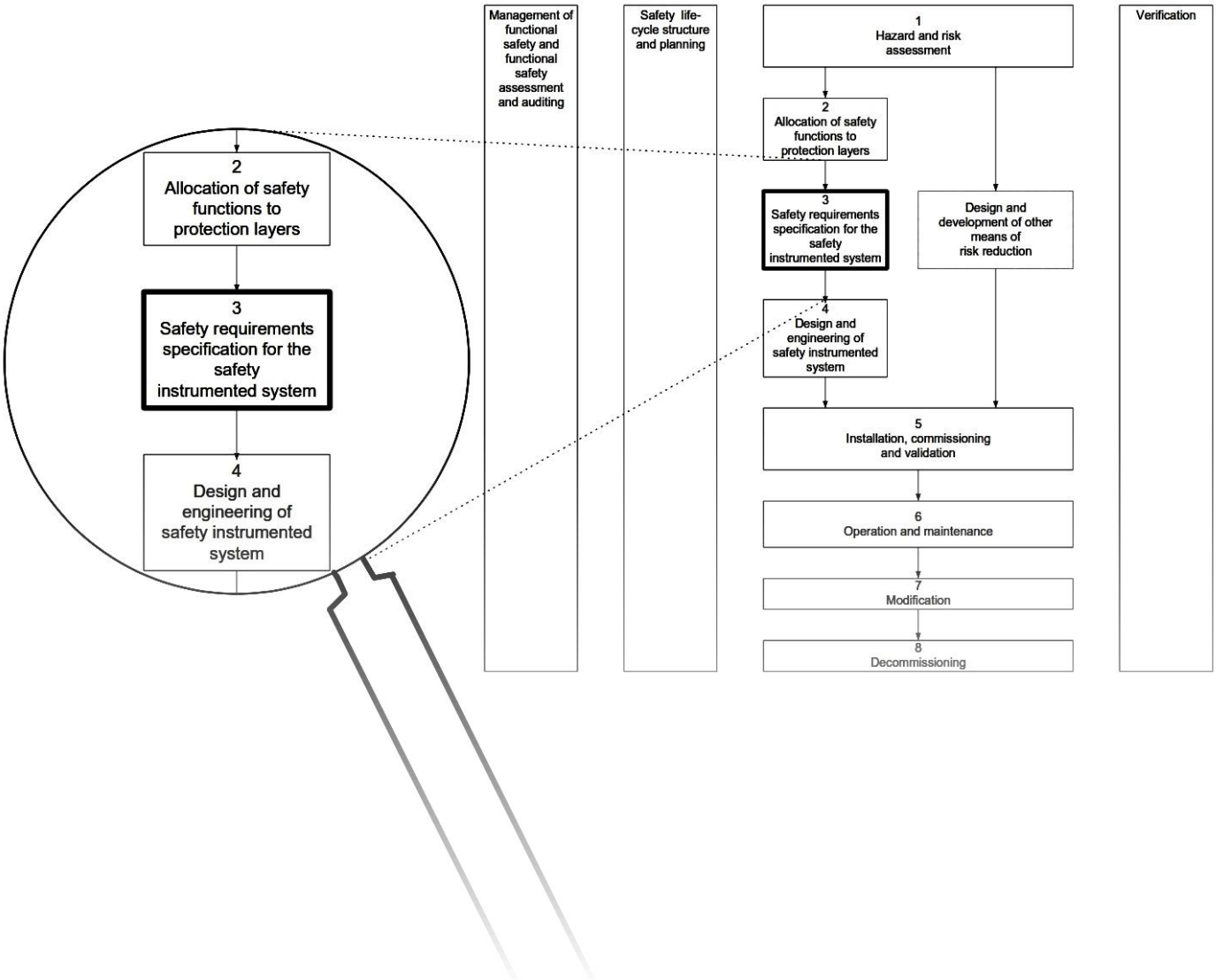
The tolerable risk will depend on many factors. For example, the severity of the consequences or injury, the number of people exposed to danger, the frequency and the duration of the exposure. Important factors will be the perception and views of those exposed to the hazardous event. Risk reduction is achieved by a combination of all the safety protective features, including any associated Safety Instrumented Function (SIF). The necessary risk reduction to achieve the specified tolerable risk, from a starting point of the risk presented by the Equipment Under Control (EUC), is shown below.

Safety integrity applies to the Electrical / Electronic / Programmable Electronic (E/E/PE) SIFs, other technology safety instrumented systems and external risk reduction facilities and is a measure of the likelihood of those systems satisfactorily achieving the necessary risk reduction. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the SIFs can be allocated in terms of the PFD.

Methods of SIL Determination

There are various methods in achieving SIL targets qualitatively by Risk Graphs, semi-quantitatively by Layer of Protection Analysis (LOPA) or fully quantitatively by Fault Tree Analysis (FTA).





Safety Requirement Specification (SRS)

Compliance to the international Standards such as IEC 61508 and IEC 61511 are imperative to meeting the Functional Safety requirements for many processes and have formed part of the quality management systems of many companies. ES have vast experience in the provision of Functional Safety Services in line with the phases and activities detailed in the Functional Safety Life-cycle.

SIS Conceptual Design

Selecting the correct equipment and architecture are key requirements to ensure Functional Safety and reliability targets are achieved. Selecting the best equipment is often preferred during the conceptual design change to minimise the cost and time impact later during the life of the project.

SIL Verification

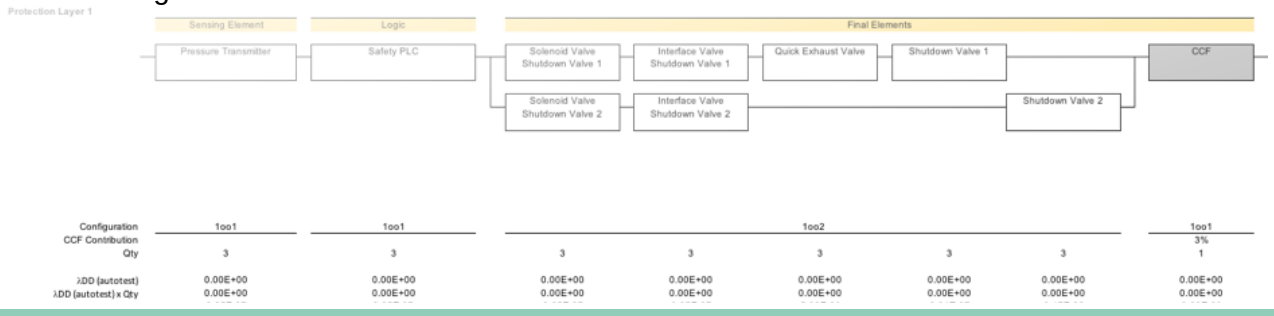
Safety Integrity Level; or SIL Verification demonstrates the capability of a Safety Instrumented Function (SIF) in accordance with IEC 61508 and IEC 61511 against the following requirements:

- Quantifying the effect of random hardware failures (Probability of Failure on Demand (PFD) or the Average Frequency of Dangerous Failures (PFH)).
- Hardware safety integrity architectural constraints (Safe Failure Fraction (SFF), Hardware Fault Tolerance (HFT), Element Type A or B).
- Systematic capability.
- Common Cause Failure (CCF).

Methods of SIL Verification

SIL Verification can be carried out using various modelling techniques including Reliability Block Diagrams (RBDs), Fault tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA). Where the SIF fails to achieve the target failure measure or SIL, a sensitivity analysis can be carried out to demonstrate the effect of modifying certain factors. This includes the following factors:

- Maintenance strategy (repair time and proof test frequency);
- System architecture;
- Implementing diagnostic mechanisms;
- Minimising CCF.



Installation, Commissioning & Site Support

ES can provide a host of services in support of Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) requirements. ES can also act as inspectors or auditors for the clients during FATs and SATs. ES can carry out review studies and provide consultancy to ensure Functional Safety requirements are maintained during Operation and Maintenance. Such studies include proof testing, management of overrides, recording failures and demands and management of change.

Functional Safety Training

ES provide various courses from Introduction to Functional Safety, to the development of client specific or custom courses, in order to provide the knowledge and knowhow for tackling everyday Functional Safety challenges.

We currently provide the following courses:

- Introduction to IEC 61508 and Sector specific standards.
- Introduction to IEC 61511 the Process Sector derivative of IEC 61508.
- Allocation of Safety Functions to Protection Layers using the Layer Of Protection Analysis technique.
- Specifying and Achieving Functional Safety.
- Quantitative Risk Assessment in order to specify High Integrity / Complex SIF requirements.
- IEC 61511 Functional Safety Life-cycle and how to apply it.

Prior User & Proven In Use

IEC 61511 requires devices that make up a Safety Instrumented Function (SIF) to be either, assessed against the requirements of IEC 61508 or against the requirements of “Prior-Use”. Many facilities utilise equipment that is used in both Safety and Control functions and the operator has gained experience and confidence in these devices. In these circumstances, Prior Use may be considered a more suitable (and logical) alternative to replacing these devices for IEC 61508 assessed items of which the operator has no experience.

Functional Safety Assessment

A Functional Safety Assessment is defined as; systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives.

Compliance

Defines compliance with the standard as: “to conform to this standard it shall be demonstrated that all the relevant requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or sub-clause, all the objectives have been met.”

Why conduct FSA

FSA is the process of performing independent reviews and audits at predefined stages of the Safety Life-cycle. FSA is the activity of ensuring the quality of execution is adequate and as per the requirements of international standards such as IEC 61508 and IEC 61511.

FSAs may be conducted at the following time:

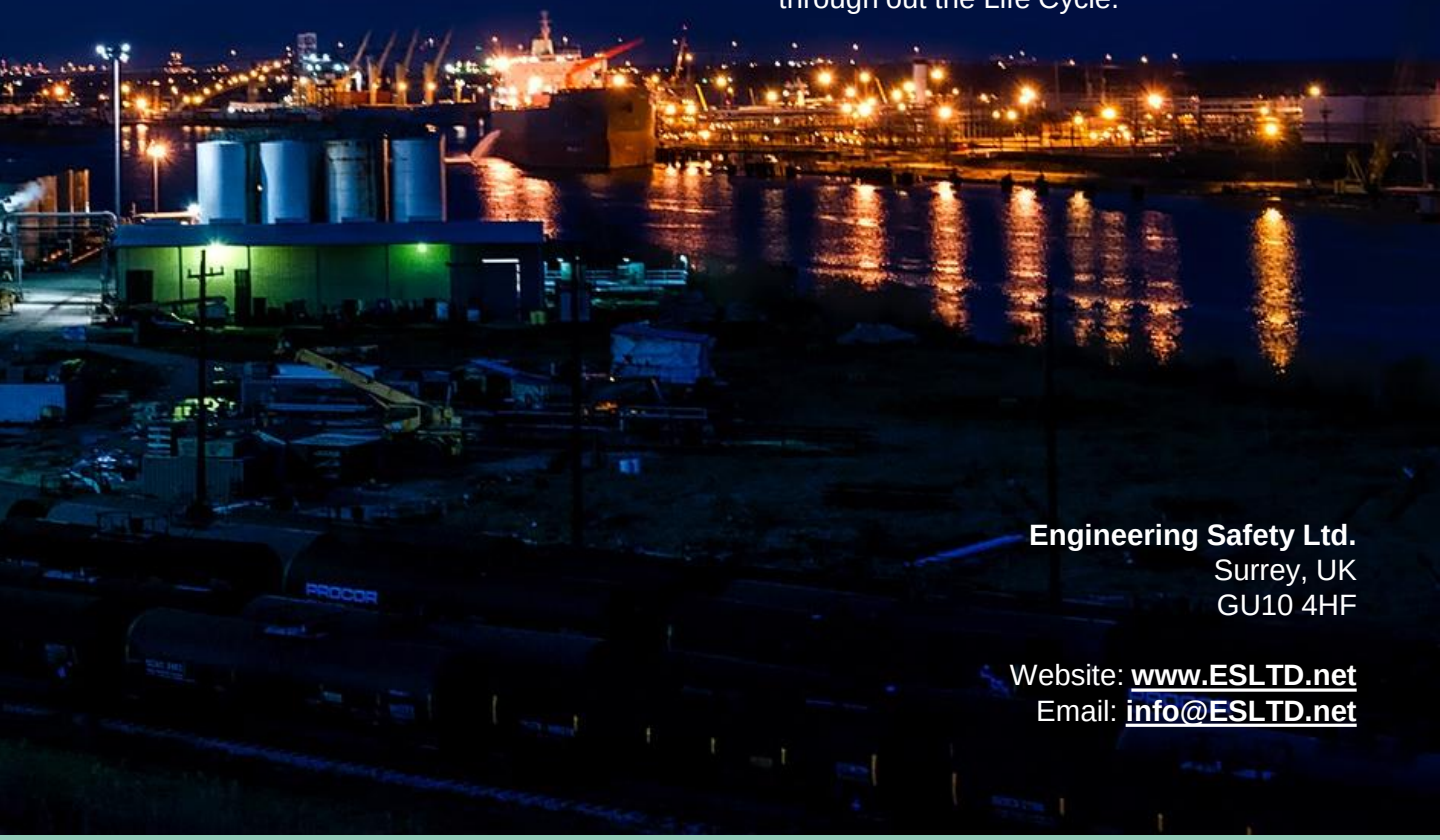
- After the hazard and risk assessment has been carried out, the required protection layers have been identified and the Safety Requirement Specification (SRS) has been developed.
- After the Safety Instrumented System (SIS) has been designed.
- After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed.
- After gaining experience in operation and maintenance.
- After modification and prior to decommissioning of a SIS.

Functional Safety Lifecycle & Management

The Functional Safety Lifecycle is one of the two concepts of IEC 61508 and IEC 61511 (the other being Safety Integrity Levels (SILs)). This is a key requirement demonstrating how Functional Safety is to be implemented and achieved. Functional Safety Management relates to how Functional Safety requirements and procedures are implemented throughout the lifecycle of a project.

Our Consultants
We work across the world with engineering organisations, equipment manufacturers and end-users providing services across all industries in every aspect of functional safety for systems, inspection and testing. Our consultants are TUV Functional Safety Engineers and NDT PCN level 3 certified, Quality focused through ISO 9001 Management Systems.

Our Pledge
Feasibility study, conceptional or detailed design, installation, modification, operation, maintenance through to decommissioning, Engineering Safety have the experience, expertise and in depth knowledge of the international standards as well as the practical knowledge as to how they should be applied so you can be assured that your installations or projects are compliant and remain compliant with all required aspects through out the Life Cycle.



Engineering Safety Ltd.
Surrey, UK
GU10 4HF

Website: **www.ESLTD.net**
Email: **info@ESLTD.net**