DATASHEET

IEC 61508/61511 - Safety Integrity Level (SIL) Assessment

In many applications dedicated instrumented trip and alarm systems are essential for plant safety. In order to establish a plant's appropriate basis of safety, it is necessary to determine and record the functionality and reliability requirements of these instrumented safety systems. This can be done most effectively by using the safety lifecycle strategy described in IEC 61508/61511.

Introduction

Plants handling hazardous materials are expected to comply with stringent regulations that call for a basis of safety to be developed. Such regulations often refer to utilizing several 'layers' of prevention or mitigation systems, one of which is the dedicated instrumented trip system. The benchmark standard IEC 61508 and its process sector variant, IEC 61511 (current industry best practice) provides a recognized methodology for the design and maintenance of such instrumented systems.

The IEC 61508/61511 safety lifecycle calls for the identification of risk reduction measures associated with plant processes and operating equipment. A SIL (Safety Integrity Level) determination exercise is a method for identifying the required risk reduction factors.

SIL Methodology

A common misconception of the SIL determination process is that the instrument engineer alone carries it out in conjunction with relevant hazard studies. In fact, detailed input is required from a study team comprised of plant process engineers, operations staff, safety management and engineering personnel to specify the 'target SIL' of a given Safety Instrumented Function (SIF) adequately. This

team uses an appropriate method (i.e. risk graph, **Layer of Protection Analysis (LOPA)** or full Quantitative Risk Assessment (QRA)) for SIL determination to identify and document the following before any hardware or software design is considered:

- Description of each hazardous event – normally highlighted within earlier hazard studies.
- Description of the consequences and likelihood of each hazardous event.
- Details of all existing or proposed risk reduction or mitigation measures (e.g. relief systems or other process protection, control systems, fire and gas detection systems, deluge systems, alarms, emergency procedures, etc.).
- Management and operational actions taken to reduce or eliminate the hazards as far as reasonably practicable.
- A description of the key assumptions made during the SIL assessment, including the expected interfaces with the plant operating teams.
- A description of the required trip functionality and associated safety reliability requirements.

The first part of any assessment is to ascertain the tolerable risks associated with an operation or specific plant area. For this, in-house risk/consequence matrices are usually employed to calibrate the intended **SIL** determination method e.g. a risk graph covering safety, environmental and potential asset loss.

The SIL determination process benefits from the design and operational knowledge of the study team and can be harnessed to identify the required level of risk reduction for any given SIF, which at this stage, is often expressed as the 'target' safety integrity level. The SIF can also be specified in terms of the reliability required of the instrumented safety equipment. This is expressed as the average Probability of Failure on Demand (PFDavg). The required risk reduction or required PFDavg figure can be inserted into one of four risk reduction levels (SIL 1 to SIL 4) described in IEC 61508/61511. This value can then be used to ensure the correct design of the instrumented architecture, so that both the performance and reliability targets specified during the SIL determination process are met.

SIL Determination Issues

Flaws in the SIL determination process can cause risk reduction measures to be overly specific or inadequately designed. Such errors result in increased expenditures for unnecessary equipment, or deficiencies in the overall basis of safety stemming from underrated instrumented systems. Expert SIL determination keeps the focus on what is important for safety whilst optimizing costs.

How DEKRA Process Safety Can Help

DEKRA Process Safety can offer quality SIL determination in accordance with the functional safety requirements of the IEC61508/61511 lifecycle phases, including:

- Development of risk matrices to ensure risk reduction values meet ALARP principles.
- SIL determination studies and supporting documentation.
- Development of the overall basis of safety including contribution from other layers of protection e.g. mechanical relief.
- Technical reviews of proposed new instrumented architectures and proof test frequencies.
- Functional safety assessments and/or verification of basis of safety assumptions.

For existing plants:

- Review of the current operating basis of safety.
- Identification of PFDavg values for existing trip and alarm loops.
- Verification between existing risk reduction measures and corresponding analysis of existing hazards expressed as a required SIL for the existing trip systems.
- Re-design or improvements to meet necessary levels of risk reduction covering all layers of protection, i.e. trips, relief valves, bunding and emergency procedures.

DEKRA Process Safety and Chemical Safety

The breadth and depth of expertise in process safety makes us globally recognised specialists and trusted advisors. We help our clients to understand and evaluate their risks, and work together to develop pragmatic solutions. Our value-adding and practical approach integrates specialist process safety management, engineering and testing. We seek to educate and grow client competence to provide sustainable performance improvement. Partnering with our clients we combine technical expertise with a passion for life preservation, harm reduction and asset protection. As a part of the world's leading expert organisation DEKRA, we are the global partner for a safe world.

Process Safety Management (PSM) Programmes

- Design and creation of relevant PSM Programmes
- Support the implementation, monitoring, and sustainability of PSM Programmes
- Audit existing PSM Programmes, comparing with best practices around the world
- Correct and improve deficient Programmes

Process Safety Information/Data (Laboratory Testing)

- Flammability/combustibility properties of dusts, gases, vapours, mists, and hybrid atmospheres
- Chemical reaction hazards and chemical process optimisation (reaction and adiabatic calorimetry RC1, ARC, VSP, Dewar)
- Thermal instability (DSC, DTA, and powder specific tests)
- Energetic materials, explosives, propellants, pyrotechnics to DOT, UN, etc. protocols
- Regulatory testing: REACH, UN, CLP, ADR, OSHA, DOT
- Electrostatic testing for powders, liquids, process equipment, liners, shoes, FIBCs

Specialist Consulting (Technical/Engineering)

- Dust, gas, and vapour flash fire and explosion hazards
- Electrostatic hazards, problems, and applications
- Reactive chemical, self-heating, and thermal instability hazards
- Hazardous area classification
- Mechanical equipment ignition risk assessment
- Transport & classification of dangerous goods

We have offices throughout North America, Europe, and Asia.
For more information, visit **www.dekra.com/process-safety**
To contact us: **process-safety@dekra.com**

Would you like more information? Contact Us

DEKRA