



IEC 61508/11 AND COMAH / SEVESO II SAFETY MANAGEMENT

For high hazard sites, the Safety Instrumented System (SIS) is seen as a crucial layer to risk reduction and an important element of the Basis of Safety. Justification of the link between the major accident hazard and the risk reduction afforded by the Safety Integrity Level (SIL) of the intended system is an industry concern.

INTRODUCTION

Events such as the Buncefield storage depot incident highlight the need to ensure that dedicated Safety Instrumented Systems (SIS) have been correctly developed, designed and are regularly maintained.

Current UK legislation such as the Control of Major Accident Hazards (COMAH) Regulations calls for site operators to have a safety management system in place that can address the hazards and ensure an adequate Basis of Safety for plant and equipment. This should be in accordance with As Low As Reasonably Practicable (ALARP) principles and be delivered, maintained and improved as necessary.

Companies who must comply with COMAH / Seveso II have to develop a systematic approach to producing and demonstrating that a credible 'documented' operating Basis of Safety exists. As the majority of such sites utilise trips and alarms as risk reduction measures the HSE requires...

"That the company has a policy and strategy for achieving safety in its safety related control systems; that this policy is subject to evaluation; and that the policy is communicated throughout the organisation."

This HSE guidance goes on to identify that one method of assisting with the COMAH safety management system can be found within the functional safety lifecycle of the IEC 61508 generic standard and the Process Sector variant, IEC 61511.

IEC 61508 STANDARD

This risk based guidance standard (and its variants) is designed to cover the overall functional safety requirements for protective layers and provide the necessary hazard evaluation, design, operations and maintenance requirements for the dedicated trip and

alarm loops, termed as 'Safety Instrumented Systems' (SIS).

It should be appreciated that an instrumented control loop is deemed to be safety related in the context of IEC 61508/11 if it is called upon to undertake actions which significantly reduce the risk of a hazard occurring on the plant. It is generally required to contribute directly or towards putting the operating plant into a safe state i.e. shutdown in a controlled manner (and is consequently differentiated from a process interlock).

Regulatory authorities see IEC 61508/11 being used for determining whether a reasonably practicable level of safety has been achieved by the intended SIS. COMAH safety reports would benefit from the adoption of a risk based methodology as found in IEC61508/11 in order to aid demonstration of a safety management lifecycle approach to safety instrumented systems.



RISK BASED METHODOLOGY

IEC 61508/11 risk based methodology can apply to both existing and proposed new SIS. To align with industry best practise an operating site should

Safety Advice From The Experts in Process Safety

consider a review of its existing measures for managing the risks from safety instrumented systems. Typically for COMAH sites, a register of the most critical trips and alarms should exist, and general awareness and purpose of this register should be understood by both operational and engineering staff alike. Where this information is currently missing, it would be prudent to undertake a review to establish the existing trip and design architectures and proof test frequencies afforded when aligned with the equivalent IEC 61508/11 SIL levels. An appropriate Safety Integrity Level (SIL) determination method such as calibrated risk graphs, layer of protection analysis (LOPA) or full QRA fault trees should be used to establish the criticality of any intended SIS.

Should it be identified that ungraded or lower end SIL 1 systems are protecting against known high risk hazards then it may be that the current levels of protection are inadequate. Alternatively some systems may be found to be over designed against the risk and cost savings could be made, typically utilising longer proof test frequencies.

As part of this review a process hazard study of the operations will typically be necessary to establish the 'Required SIL' of the safety instrumented systems; this value then being compared to the 'Achieved SIL' for the SIS actually installed on site.

SIL determination is no longer the lonely domain of the Instrument Engineer, it is now recognised that comprehensive risk assessment can only take place by the use of a multidiscipline team comprising members of staff from Safety, Process, Plant Operations and Engineering.

For sites using non-IEC 61508/11 based standards a similar exercise should be undertaken on a sample of their SIS covering a number of known trip criticality ranges in order to establish how well the existing designs covering safety and environmental hazards compare with those required by IEC 61508/11.

The adoption of such 'Best Practice' SIL determination methodologies particularly for high hazard operations within a recognised functional safety framework will invariably assist with demonstrating regulatory compliance.

HOW CHILWORTH CAN HELP

Chilworth Technology has a wealth of knowledge from working within COMAH sites. Our services cover:

- Targeted hazard identification (e.g. HAZOP) and consequence reviews of new and existing installations.
- IEC 61508/11 SIL Determination, and Functional Safety Assessments for both new and legacy SIS.
- Process Safety Culture (PSC) reviews.
- Safety Management System technical audits.
- Identification of potential major accidents and associated consequence and impact modelling.
- COMAH health check as part of your 5 yearly submission review or following major changes to processes or systems.
- Occupied Buildings Risk Assessments.

For a hard or soft-copy of the datasheet above, please contact us on training@chilworth.co.uk