APPROPRIATE AND PROPORTIONATE RISK ASSESSMENT

There are many tools available to determine risk, but the underlying methodology is identical in all cases, although the tool used needs to be appropriate and proportionate. If risks are significant, tools like HAZID, HAZOP, LOPA, QRA, etc. are used, but for simpler, lower risks, Checklists or What-if studies may be more appropriate.

Hazard Identification (HAZID) and Hazard & Operability (HAZOP) Studies

HAZOP is perhaps the most widely used method to identify both hazards and operational problems in design, with a broad application across many sectors of industry. Normally applied to a new process or design, it questions the design intent by applying simple guidewords (e.g., no, less, more, reverse) to process parameters (e.g., pressure, flow, temperature etc.) in a structured and systematic manner. The output from a HAZOP is a clear understanding of the hazards and operability issues around a design.

Our HAZOP study leaders have all followed recognised training programmes and are experienced in applying the technique across a wide range of industrial processes, at key stages in the project or plant lifecycle.

At SLR, we also use a formal HAZID technique for identifying hazards. This is much quicker and less resource intensive but is still recognised by Regulators as appropriate for review of existing processes and other operations. As with HAZOP, our tool applies guidewords, (e.g., overpressure, impact etc.) systematically to identify hazards and provides for risk assessment, since it considers the risks of the identified scenarios both before and after the installed risk reduction measures.

The output from the HAZID is a set of scenarios which are prioritised by risk, with the inherent safety, prevention, control and mitigation measures recorded to manage the risk in each case. This output can then be used to analyse scenarios and screen appropriately for potential further studies that may be required, for example, determination of the Representative Set of scenarios required in a COMAH safety report; determination of scenarios which rely on significant human intervention to manage risk and require further study using Task Analysis and Human Reliability Assessment (HRA); or determination of the required Safety Integrity Level (SIL) for a Safety Instrumented System (SIS) in a Layers of Protection Analysis (LOPA).

At the component level, we can also help you to carry out Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects, and Criticality Analysis (FMECA) studies to identify potential failures and assess the resulting effects on the rest of the system. The output is usually a set of actions focussed on design modification, or more generally on inspection, testing and preventive maintenance. Studies can be carried out using a range of templates, but we can provide our own FMEA/FMECA workbooks for recording results and actions.

All of the templates we provide can be used by you to maintain these studies as living documents to meet the expectations of the Regulators.

LOPA and SIL Determination
Layers of Protection Analysis (LOPA) is another risk assessment technique, more commonly used to determine the required Safety Integrity Level (SIL) for Safety Instrumented Systems (SIS) under specific standards (i.e., BS EN 61508 and BS EN 61511).

The methodology essentially differentiates between installed risk reduction measures. The outcome from most risk assessment techniques records all the risk reduction measures. These measures can include items of plant and equipment, human actions and procedures, etc. LOPA defines certain measures as special and calls them Independent Protection Layers (IPLs). IPLs are defined as measures which are:

- Independent – they act on their own
- Effective – they will prevent the hazardous scenario (if they work)
- Auditable – are capable of being formally tested

All the identified risk reduction measures are screened and non-IPLs removed, before deciding if the remaining IPLs reduce the level of risk to an acceptable Target Risk Level. The level of risk reduction achieved or credit for each identified IPL is determined using a LOPA Rule Book (which specifies how risk reduction credits can be awarded for various situations).

If, after assigning the risk credits for the installed IPLs, the Target Risk Level is not attained, then the standards assume that the remaining risk gap will be filled by the installation of a Safety Instrumented System (SIS). The size of the risk gap determines the Safety Integrity Level (SIL) of the SIS required.

We are actively involved in helping operators to determine whether or not proposed and existing safety related systems can provide the necessary level of risk reduction or SIL, consistent with the requirements of the standards.

We can help you:

- Specify appropriate IPLs
- Identify Safety Instrumented Functions (SIFs)
- Determine appropriate target SILs for SISs
- Validate proposed or existing designs for SISs to ensure the SILs can be achieved
- Prepare essential documentation for ongoing inspection, functional testing and maintenance of SISs

In addition, we can review existing practices and procedures within the Functional Safety Management system to assess compliance.

**Consideration of Human Factors**

The term Human Factors refers to the environmental, organisational and job factors, and human and individual characteristics, which influence behaviour at work. Human Factors studies provide an understanding of the factors that can affect human performance.
Performance can be affected by factors associated with the person (motivation, fatigue, etc.), the job itself (the working environment, having the correct tools and procedures, etc.) and the organisation (work pressures, culture, etc.). These factors are termed Performance Influencing Factors (PIF). For critical tasks, defined as tasks that must be performed correctly each time otherwise serious consequences may occur, we must ensure that these factors are considered in a robust and systematic manner. Tools used to assess the risks are Task Analysis and Human Reliability Analysis (HRA) which operate in a similar fashion to other risk assessments.

For COMAH sites the assessment of Human Factors is an essential part of the risk assessment process. You need to understand which activities are critical to safety and what can be done to optimise human performance to protect people and the environment.

Our highly skilled consultants can help you to tackle error reduction in a structured and proactive way, and make it an integral part of the Safety Management System.

We can help you by:

- Employing both qualitative and quantitative Human Reliability Assessments, sometimes known as Human HAZOPs
- Feeding the results of assessments into traditional engineering risk assessment tools and methodologies such as Event Trees and Fault Trees
- Developing Standard Operating Procedures (SOPs) for safety critical operations

By applying proven Human Factors techniques, grounded in the principles of human and organisational psychology, we can help you to manage the risk to your business and ensure compliance with regulatory requirements at every level, from site management to operational personnel.

Cybersecurity Risk Assessment

Applying Risk Assessment to Cybersecurity requires a fundamental shift in how the process industries approach the subject of risk. A significant difference between process and cyber risks, are that the latter involve threats that are permanently present and often deliberate. Traditional hazard identification and risk assessment techniques, such as HAZID, HAZOP and LOPA are therefore not appropriate.

Assessment of risk from cyber-attacks starts with understanding the Instrumentation, Automation and Control System (IACS) network and then separating it into zones and identifying which zones have major accident potential. Information is then presented on a network drawing and forms the basis of the risk assessment. This requires the combined skills of IT, computer and risk specialists. The HSE’s operational guidance, OG86, provides an example network drawing.

One fundamental difference between process safety and cybersecurity risk assessment is that the latter is conducted upon the network zones rather than items of equipment and processes. However, the consequences associated with each network zone are based upon the outputs of traditional process safety risks assessments. Consequently, the starting point for cybersecurity risk assessment is an assessment of criticality of each zone, based upon sound process safety knowledge. Once the
criticality of each zone is understood, threat assessments are carried out and appropriate and proportionate counter measures are identified as present or required to be introduced.

Quantified Risk Assessment

Quantified Risk Assessment (QRA) is a form of risk evaluation/analysis where both the consequences and likelihoods of hazardous scenarios are determined numerically. There are varying levels of QRA that can range from simple (largely qualitative) approaches, through semi-quantitative to full parts count QRA, which should be selected to provide a proportionate approach to the level of risk posed by the facility. The output is often in the form of individual and societal risk frequencies, which are used to determine the tolerability of risk. Individual risk is often presented using risk contours, which depict the individual risk for people located in a particular place, from all hazardous scenarios on a site which can impact them, whilst societal risk is often developed using FN curves.

QRA is often used for Land Use Planning issues by the Regulators – determining whether a new development should go ahead or not. Its use for depicting the risks to on-site personnel or members of the public off-site within COMAH safety reports is not generally required.

We can advise on the need for QRA and use the recognised tools and techniques to carry out a full and detailed assessment at a proportionate level.

Occupied Buildings Risk Assessment

Under the COMAH Regulations, operators must demonstrate that the risks to employees in offices and other workplaces on site are ALARP.

Many major incidents that have occurred on sites have resulted in serious harm to people in buildings, e.g. due to partial building collapse, or the generation of missiles or glass fragments. In many cases, the effects have been more severe than if the people were located in the open air and involved populations that did not necessarily need to be within such a close proximity to process equipment.

Occupied Buildings Risk Assessment (OBRA) is the tool used to assess the risks to people located in buildings on site. The approach requires knowledge of the actual hazard impact on a specific building and of building performance (different types of building provide differing performance).

We have completed a large number of OBRA’s of various types (including the use of exceedance curves for complex sites) for many operating companies throughout the process industries, and we have a well-developed methodology which incorporates the requirements of the Chemical Industries Association (CIA) and HSE. In fact, our experience in this area is such that we were involved in writing the latest CIA guidance on Occupied Buildings.

We can help you by:

- Carrying out OBRA’s according to the CIA guidance
- Reviewing existing building design and identifying remedial measures to increase protection
- Developing toxic gas and flammable/explosion refuges for people
Developing emergency response plans

Fire Risk Assessments

Whatever your type of business, you need to assess your fire hazards and general fire precautions and put in place the necessary measures to prevent and protect against a fire. This means ensuring that your current fire precautions are fully compliant and that your staff can raise the alarm and evacuate safely in the event of a fire.

We routinely undertake Fire Risk Assessments on behalf of our many and varied clients and can assist you in:

- Assessing how combustible materials are stored and used
- Assessing the general fire precautions i.e., means of escape, fire-fighting equipment, etc.
- Determining if fixed firefighting installations are adequate and fit for purpose
- Liaising with your local fire authority
- Assessing and developing procedures and training of personnel

ALARP Demonstration

If your risk analyses or evaluations show that the risks on your site are intolerable the law requires you to take immediate further action to lower risk. Even when the risks are deemed tolerable or broadly acceptable, you may still need to do more to demonstrate that the risks posed are ‘as low as reasonably practicable’ (ALARP) e.g., as required under COMAH.

In most circumstances, demonstration of ALARP can be achieved by considering additional potential risk reduction measures to see if implementation is reasonably practicable, which may include the use of Cost Benefit Analysis (CBA). In CBA, where the cost of an additional measure is deemed ‘grossly disproportionate’ in comparison with the level of risk reduction achieved then there is no requirement to install it; note, however, that the opposite is also true.

At SLR we have recognised tools and techniques for dealing with all of these issues, delivering reliable results that have proved acceptable to the Regulators over many years.