FUNCTIONAL SAFETY MANAGEMENT

In the UK, operators of hazardous installations have a legal obligation to demonstrate that the risks they present to people and the environment are being managed and are as low as reasonably practicable (ALARP). Such hazards and risks are typically regulated through the Control of Major Accidents Hazards Regulations 2015 (COMAH), although operational sites which fall outside of COMAH still have this legal obligation. A key aspect of demonstrating ALARP is to understand what risks are present, what more you could do to reduce the risks and to show compliance with accepted good practice.

Functional safety is a part of overall safety, relating to the process and the basic process control system (BCPS), which depends on the correct functioning of the Safety Instrumented Systems (SIS) and other protection layers. Functional safety work provides an assurance that a SIS gives sufficient risk reduction to meet its required integrity level and offers the necessary protection from an identified hazardous scenario. Consequently, achieving functional safety is an important aspect of the plant's overall basis of safety and a key requirement of making an ALARP demonstration.

Functional safety is achieved by adopting a lifecycle approach which details all activities pertaining to functional safety, from initial identification of hazards through to specification, design, installation, commissioning, operation, maintenance and change / decommissioning. The accepted good practice for functional safety is detailed in the British Standards BS EN 61508 (Functional Safety of E / E / PE Safety related systems) and BS EN 61511 (Functional Safety – Safety Instrumented Systems for the Process Industry Sector); each describe the safety lifecycle in detail. In 2017 these documents were updated and included the following key changes:

- Mandatory requirement for competency assessment
- Functional Safety Assessment (FSA) Stage 4 and 5 now mandated
- On-going performance of the SIS to be monitored
- Introduction of Systematic Capability
- Requirement for an independent person to perform a Functional Safety Audit
- Requirement for an impact assessment upon modification of a SIS
- Requirements for a Security Risk Assessment to be conducted on the SIS

Through the COMAH Regulations and review of associated COMAH Safety Reports, the UK Health and Safety Executive will assess the performance of operational sites with respect to functional safety and compliance with accepted good practice. We can assist clients in all aspects of the SIS safety lifecycle from the development of management systems and assessment of risk through to the design, operation and maintenance phases. By offering an independent view, we can help ensure that sites correctly apply the accepted good practice to engineer plant and processes to a standard which is appropriate for the levels of risk present.

Management of Functional Safety

Key to ensuring that functional safety is achieved is the implementation of management systems which are aligned to functional safety standards such as BS EN 61508 and BS EN 61511. A Safety Instrumented System (SIS) is only as reliable as the process used to develop it. Functional safety

management should be integrated within the existing safety management system which touches upon all aspects of the business from design, engineering, operations, maintenance, modification, and procurement.

Do you know if your existing management systems adequately cover functional safety?
Do you know if they are being implemented?

Functional Safety Gap Analysis

A Functional Safety Gap Analysis is a review of the management systems to ensure compliance with functional safety standards. By identifying gaps in the system, additional work can be performed to upgrade systems and ensure suitability. A gap analysis differs from activities such as auditing since it challenges the underlying management systems to establish if they are suitable for the purpose of managing functional safety.

We can review existing management systems and standards and compare them with the requirements of the functional safety standards (BS EN 61508 and BS EN 61511). Having identified the gaps, actions can be set, prioritised and presented for agreement to enable forward planning of resolution activities.

Functional Safety Planning

Safety Lifecycle Planning is a mandatory requirement of the functional safety standards and ensures that all activities required by the standards are performed. Plans can be aligned to a plant, organisation or single project and are used to verify activities associated with achieving functional safety.

Our Functional Safety Consultants can assist in the generation of Safety Life Cycle Plans to ensure that the defined safety lifecycle activities are performed from design through to operation, maintenance and modification of the Safety Instrumented Systems. Plans will identify the procedures used to ensure that the SIF achieves its safety requirements along with roles and responsibilities for each activity.

Auditing Functional Safety Management Systems

Auditing is an activity designed to establish if the Functional Safety Management Systems are being followed, that this is evidenced and provides an assurance to senior leaders that functional safety is being managed adequately. Unlike a Functional Safety Gap Analysis or Functional Safety Assessment, which comment on adequacy of the standards or work performed, the audit focuses only on compliance with the standards. Our Functional Safety Consultants can assist in performing audits, developing audit programmes or integrating functional safety related audit programmes into existing audit schedules.

Linking closely with auditing are performance metrics such as Process Safety Performance Indicators (PSPIs) which can be aligned to include functional safety elements as a part of the site overall strategy for managing process safety.

Cybersecurity Management Systems

Of specific importance to the UK Health and Safety Executive is the emerging field of Cybersecurity, and how such threats and vulnerabilities impact upon site with Major Accident Hazard potential. The impact of this on how Functional Safety is managed is detailed under Cybersecurity below.

Hazard Identification and Risk Assessment

Hazard identification and risk assessment is used to determine all reasonably foreseeable hazardous events within the process and its associated plant items and to identify the current safeguards. A HAZOP study is a structured brainstorming session to identify potential undesirable scenarios which might cause hazards or operability problems. By understanding the cause/consequence pairs and the measures in place to prevent such hazards, risk reduction requirements can be identified which could include the requirement for a Safety Instrumented System (SIS). This information is used in future lifecycle stages e.g., the allocation of safety functions to protective layers and in the generation of a Safety Requirement Specification (SRS).

We have gained significant experience of using recognised industry methods such as Hazard Identification Studies (HAZID) and Hazard and Operability Studies (HAZOP).

SIL Determination

Once cause/consequence pairs have been identified, the functional safety standards require allocation of safety functions to protective layers and to establish any Safety Integrity Level (SIL) requirements for Safety Instrumented Functions (SIFs). This process involves:

- Establishing a risk tolerability target
- Determining the consequence and frequency of a specific hazard
- Identifying the layers of protection present and determining the risk reduction provided
- Assessing for the presence of a protection gap and assigning a required SIL rating if instrumented systems are used to close the protection gap

We can provide experienced Functional Safety Engineers to conduct SIL determination studies such as Layer of Protection Analysis (LOPA), Risk Graph or Fault Tree Analysis. By providing an independent view, proposed designs are subject to the required scrutiny while avoiding the need for costly over-engineering. Additionally, SLR can assist by peer reviewing client LOPAs, reviewing or developing LOPA procedures and providing training in SIL determination techniques such as LOPA.

Safety Requirement Specification (SRS)

The Safety Requirements Specification (SRS) is a key document which is required for both the design and validation of the Safety Instrumented System (SIS). The SRS specifies the safety integrity and functional requirements for each Safety Instrument Function (SIF) and should link directly back to the hazard identification and risk assessment stages of the safety lifecycle. The SRS is an essential source of information for all aspects of the SIF and is required throughout the lifecycle until the SIF is decommissioned. All maintenance procedures and proof testing should establish if the SIF is performing as per the SRS while modifications to the SIF must be reflected by an updated SRS.

We have standard SRS templates, which are aligned with the functional safety standards, BS EN 61508 and BS EN 61511, and can provide Functional Safety Consultants to assist in the specification of new equipment or retrospective specifications. SLR can also assist in the generation of proof testing and inspection procedures specifically aligned to the SRS.

Legacy Equipment

Legacy equipment can present many challenges to operating sites with common problems being the designation of equipment as a 'SIL device' without any basis for doing so, or utilising equipment which pre-dates the functional safety standards BS EN 61508 and BS EN 61511. Under such circumstances equipment should not just be 'ripped out' and new equipment installed when all that operational sites are required to do is provide a demonstration of the suitability of the current equipment. A reassessment of the hazards and risks of the process through techniques such as HAZOP and LOPA can be performed to establish if the Safety Instrumented System (SIS) is really required to be SIL rated. Should SIL rated equipment be required, SLR's Functional Safety Consultants can guide organisations through the requirements to see if a 'prior use' argument for legacy equipment is appropriate. The requirements for such demonstrations are challenging although worthwhile to avoid retrospectively re-engineering the process.

Even if instrumented systems have been specified and designed in accordance with the functional safety standards, Edition 2 of the standards have introduced the requirement to evaluate the actual performance of the equipment used within a SIS and Safety Instrumented Functions (SIFs). Mandatory requirements now include the need for periodic Functional Safety Assessments (FSA stage 4) and the collection of demand rates and failure data to support the claims made in earlier lifecycle stages and to link into the sites Process Safety Performance Indicators (PSPIs).

Maintenance and Proof Testing

Once a Safety Instrumented System (SIS) is installed, its ability to continue to operate as required by the Safety Requirements Specifications (SRS) is dependent upon the quality of inspection, maintenance and proof testing. All SIS require operating, inspection and proof testing procedures to be developed which must be aligned to the SRS and any likely failure modes.

The purpose of a proof test is to reveal what would be otherwise un-revealed dangerous failures in the system to prove that the entire safety system (sensor, logic solver and final element) operates as per the SRS. Results from the proof tests should be recorded and reviewed to look for trends. This information is essential in making a demonstration that the assumptions used in earlier lifecycle stages are valid, for substantiating prior use arguments and an important feed into FSA stage 4 assessments.

Inspection differs from proof testing and is a more frequent activity which aims to pick up early signs of deterioration, damage or alterations to the installed SIS in between its proof tests. Any maintenance activity on a SIS is likely to be considered as a Safety Critical Task which should be subject to techniques such as Human Reliability Analysis (HRA).

SLR can assist in the review or development of proof testing and inspection procedures to ensure that equipment is inspected and maintained in accordance with the SRS. We can also train

operations and maintenance personnel in SIL Awareness as part of compliance with functional safety competence requirements and to upskill staff to play a leading role in shaping company standards and procedures. Our proof test and inspection procedures provide the relevant information for on-going performance measurement of the Safety Instrumented Function and to conduct Human Reliability Analysis on identified Safety Critical Tasks.

Functional Safety Assessment

Functional Safety Assessment (FSA) is a 5-stage review which acts to assess the adequacy of the work performed at key stages of the safety lifecycle:

- FSA1 - after development of the Safety Requirements Specification (SRS)
- FSA2 - after design of the Safety Instrumented Function (SIF)
- FSA3 - after installation and commissioning prior to hazards being introduced
- FSA4 - after operating and maintaining the SIF for a period of time
- FSA5 - after modification or decommissioning

The FSA is a comprehensive review which requires the assessor's experience and judgement to establish if the SIF in question is adequate for the intended duty and will ensure functional safety. SLR's Functional Safety Engineers can provide the required competence and independence to utilise standard templates and check sheets to conduct a documented review against set criteria depending upon which FSA stage is being performed. Assessment could be on any aspect of compliance with the BS EN 61508 and BS EN 61511 standards and examples include linkage to hazard identification and risk assessment, adequacy of the SRS, that validation documentation is complete, and that the design is adequate and meets the specification.

Functional Safety Training

Training and competence in functional safety is a mandatory requirement for all those who perform safety lifecycle activities, and this includes both employees and third-party contractors. Competence is a broader topic than training and involves ensuring that all individuals who perform Functional Safety Lifecycle activities have the relevant skills, knowledge, experience, behaviours and attitudes to conduct the tasks required of them. SLR can assist in the review or creation of competence profiles and competence management systems relevant to functional safety.

Training is one part of the overall competence demonstration, and SLR provides functional safety training which includes:

- Functional Safety Management Awareness (Site Leaders and Managers)
- Functional Safety Management Awareness (Site Engineers)
- SIL Determination Training
- SIL Awareness for Operations and Maintenance Personnel

Training packages utilise generic industry examples and workshops to teach the key concepts of functional safety at the level required for the audience. Bespoke company training packages or e-learning options are available upon request.

Functional Safety Competence

A recent change to BS EN 61511 (Edition 2) has led to the introduction of a mandatory requirement for the demonstration of competence when performing Functional Safety Lifecycle Activities. Organisations tend to believe that the demonstration of competence is merely presenting certification, however the Functional Safety Standards neither require certificated people or certificated equipment.

Certification and training are just one part of an overall competence demonstration. The subject of Functional Safety touches all levels within the organisation and therefore there is a requirement for the consideration of the competence of individuals at all levels. Functional Safety Lifecycle planning is key to this activity, to ensure that roles and responsibilities, along with inputs and outputs of a given lifecycle stage, clearly define the knowledge, skills, experience and personal qualities required to demonstrate such competence.

SLR can assist in the development of competence matrices and programmes which align roles within the organisation with the Safety Lifecycle activities required to ensure Functional Safety is achieved; furthermore, our Functional Safety Engineers and Risk Consultants can provide standard or bespoke training programmes to assist your organisations in the demonstration of competence, along with on-going verification assessments.

Are you a:

- Senior Executive / Director who needs to understand that the subject of Functional Safety is adequately covered to protect your assets?
- Engineering Manager / Project Engineer / Design Engineer or Site Manager who needs to understand aspects of Risk Assessment, Design and Compliance?
- Operator or Maintenance Technician who needs to understand the criticality of inspection and proof testing, and how this links to SIL?
- An employee working in support functions such as Human Resources or Procurement, who needs to understand how Functional Safety impacts upon your role?

If so, then Functional Safety training at a level of detail which is appropriate for your role will be required. Training can be face to face or through our blended learning platform.

Cyber Security

As business advances technologically, new threats and vulnerabilities develop; one such threat is of a cyber-attack. Although the term cyber-attack creates a vision of state sponsored attacks, or the theft of personal information, the subject is relevant to Industrial Automation and Control Systems (IACS) used in high hazard industries.

The UK's Health and Safety Executive (HSE) is in the process of inspecting sites with high hazard potential, after performing initial trial inspections. Early indications are that while organisations do manage cybersecurity, this is generally from the perspective of data / financial protection; sites are therefore weak at applying cybersecurity principles to the control of major accidents. Operators of sites regulated under COMAH have a legal requirement to demonstrate that risks are managed to As

Low and Reasonably Practicable (ALARP), and therefore improvement in Cybersecurity will be required throughout the industry.

An easy misconception would be to assume that this work is for IT and computer specialists However, such assumptions could not be further from the truth. While appropriate (i.e., functional) protection against Cyber-attacks requires computer specialists, protection also needs to be sufficient (i.e., proportionate) to the risk. Good cybersecurity performance is, therefore, based on effective Cybersecurity Management Systems which bring together the skills of the computer specialists and risk specialists to:

- Identify vulnerabilities and assess the risks from the perspective of Major Accident potential
- Identify existing countermeasures and ensure that they are both appropriate and proportionate
- Maintain the counter measures and assure effectiveness through audit, monitoring and review processes

The approach that the HSE are expecting to see is set out within operational guidance OG86 Edition 2, Appendix 1, Figure 1.

As specialists in the field of COMAH, Risk Assessment and Risk Management, SLR are well positioned to assist the industry with understanding how to manage cybersecurity in a proportionate manner for sites with major accident potential. Our services include:

- GAP analysis and Audits of Cybersecurity Management Systems
- Development of Cybersecurity Management Systems
- Assisting in the definition of IACS boundaries which are linked to Major Accident Potential
- Cybersecurity Risk Assessments
- Assistance in proportionality considerations for ALARP demonstrations