Abstract

Increasingly regulatory and competent authorities are looking to hazardous installation process operators to continually improve their compliance with IEC 61511 through the management of their safety instrumented systems, integration of that management system into their overall site-wide safety management system and carrying out reviews of existing safety instrumented systems and equipment suppliers for compliance with IEC 61511 with the long term view that only “high integrity” suppliers would be supplying and maintaining safety instrumented systems on hazardous installations.

For an organisation to provide a level of assurance that functional safety management is focused on IEC 61511 compliance and specific business needs a gap analysis should be undertaken to identify the areas of weakness within the organisation’s existing safety and maintenance management system, to set the benchmark for improvement against the performance guidance given in IEC 61511 and to provide a framework for the management of site-wide safety instrumented systems including the competency of persons who interact with and service the systems.

Using IEC 61511 clauses 5 and 7 as the targets of evaluation for the gap analysis and utilising the IEC 61511 lifecycle framework as the development tool for the management system this paper discusses a practical approach to carrying out the analysis and developing the management system by filling the gaps in the existing safety management system.

Background

Safety is best achieved by an inherently safe process design, but this approach is not always practicable and a Hazard Identification (HAZID) and/or a Hazard and Operability (HAZOP) study is necessary to systematically analyse the process design to identify any cause / consequences pairs that may lead to a potential hazard scenario and then assess the protective measures in place with respect to their ability to prevent or mitigate the potential hazard scenario identified. If the protective measure identified is a safety instrumented function then it will be required to operate to a defined performance standard set by the risk reduction contribution it is required to achieve and the integrity level band that the required risk reduction contribution sits within IEC 61511-3 [6]

Protective measures can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic). Safety Instrumented Systems (SIS) have been used for many years to provide preventative safeguards in the process industry. If process instrumentation systems are to be effectively used as a protective measure it is essential that
they achieve certain minimum standards and performance levels. IEC 61511 [6] addresses the application of SIS in the process industries; it requires that a process hazard and risk assessment be carried out to identify process hazards and to enable the identification and allocation of protection layers to prevent and / or mitigate the frequency or consequences of the hazard. Other passive safety measures, such venting, fireproofing, bunding, or active safety measures, such thermal or pressure relief, should be considered first so that their contribution can be taken into account in terms of risk reduction before considering the performance requirements for the Safety Instrumented Functions (SIF). The SIF must include all subsystem components necessary to carry out the safety function from sensor(s) to final element(s). IEC 61511-1 [6] is the process industry implementation of IEC 61508 [5], and states two concepts, which are fundamental to its application; safety lifecycle management and safety integrity levels and provides guidance on the application of safety life-cycle activities to achieve the performance standards and by following that guidance it is possible to provide evidence that a rational, consistent and auditable technical approach has been applied. The functional safety management (FSM) system must be based on this lifecycle approach.

**Purpose of Functional Safety Management Systems**

The purpose of the FSM system is to clearly describe the processes adopted by an organisation to assure the suitability and continuing functional integrity of safety instrumented systems essential to ensure the safety of hazardous processes (PSLG 47 [4]).

The FSM approach based on the IEC 61511-1 [6] lifecycle framework is considered to be one of the most effective means of recording how to generate, review, implement, verify and thereafter audit, revise and manage so as to achieve effective functional safety life-cycle operation of safety instrumented functions.

**Scope of Functional Safety Management Systems**

It is important not to confuse the FSM system with the Site Safety Management System (SMS) [1], the FSM supports the overall site safety performance and should therefore be an integral part of the site SMS and be considered in other business key performance indicators (KPI) such as competency profiling, training needs analysis, procurement procedures, supply chain management, reliability centred maintenance routines (RCM) and service level agreements (SLA).

The IEC 61511-1 [6] life cycle framework supports all of the above business requirements with respect to those safety-instrumented functions that have been determined by analysis to form a part of the hazardous Installation process operator’s safety instrumented systems. This support is further enhanced as the standard is the process industry sector implementation of IEC 61508 [5] and therefore equipment, software and management systems that comply with IEC 61508 will also comply with IEC 61511 simplifying project procurement and planning for obsolescence for legacy systems.

**Government guidance and the Process Safety Leadership Group Guidance**

Following the explosions at the Buncefield Oil Storage Depot on the 11th December 2005 the Major Incident Investigation Board carried out an extensive
investigation and has to date published eight reports providing findings and recommendations for use within the process industries. The report from the Process Safety Leadership Group [4] (PSLG) provides guidance on the application of functional safety management system within the process industries and complements the existing guidance on safety management systems already provided in the COMAH regulations. The guidance states that an FSM must be in place and contain for each phase in the SIS lifecycle the following:

- Safety planning, organisation and procedures;
- Identification of roles and responsibilities of persons;
- Competence of persons and accountability;
- Implementation and monitoring of activities;
- Procedures to evaluate system performance and validation including keeping of records;
- Procedures for operation, maintenance, testing and inspection;
- Functional safety assessment and auditing;
- Management of change;
- Documentation relating to risk assessment, design, manufacture, installation and commissioning;
- Management of software and system configuration

**Application of BS EN 61511 in the Process Industries**

As discussed above, it is important to understand that the application of IEC 61511 covers the complete lifecycle of a safety-instrumented function from identification and definition through to decommissioning. The application of the lifecycle can be sub divided into 8 general phases:

1. Business need for a new process plant / unit or modification to existing
   - Process and System Design
   - Operational and Technical requirements
   - Hazard Identification
   - Setting of safety targets

2. Safety Requirements Specification (Clauses 8, 9 and 10)
   - Safety Integrity Level Assessment (LOPA, Risk Graph, Fault Tree)
   - Definition of Safety Functions
   - Allocation of Safety Functions to protection layers
   - Definition of Safety Instrumented Functions
   - Allocation of Safety Integrity Level requirements

3. Design and Development (Clauses 11 and 12)
   - SIF Identification Reference
   - Detailed design drawings (Schematics, Loops, Hook Ups)
Technical Information on all sub system components (Reliability Data)
Manufacturers Information (Safety Manual / Proven In Use / FMEDA)
SIL hardware verification calculations
Determination of optimum Proof Test Interval
Lifecycle documentation for Application software development
Certification of Source / embedded code
Maintenance, Inspection and Testing Procedures

4. Installation, Commissioning and Validation (Clauses 13, 14 and 15)
   Factory Acceptance Test (When Applicable)
   Site Acceptance Test
   Mechanical Inspection and completion certificate
   Electrical Inspection and completion certificate
   Function Testing and completion certificate
   Commissioning Procedure (Aligned to SRS)
   Validation documentation and report

5. System Operation and Maintenance (Clause 16)
   Competency Management System - Training and Assessment
   Proof test procedures and Schedule
   Inspection procedures and Schedule
   Management of overrides procedure
   Schedule for periodic review of procedures by competent person

6. System Modification (Clause 17)
   Management of Change Procedure
   Impact Assessment and levels of authorization
   Document control and archive procedures

7. System Decommissioning (Clause 18)
   Impact Assessment and levels of authorization
   Decommissioning procedure
   Document control and archive procedures

8. Management of Functional Safety (Clauses 5 and 7)
   Policy and Procedures
   Responsibilities
   Competency Management System
   Planning
   Verification
   Audit and Review
Not every phase or every process within a phase is applicable to an organization’s business needs, for example a systems integrator would not normally develop the safety requirements specification phase as this would be driven by the end user of the safety instrumented system. Similarly, in general, an end user would subcontract the design and development phase to a third party. Each organization should therefore identify the phases applicable to their business needs and develop a FSM that addresses those lifecycle phases. This identification process is best achieved by the use of a simple tool first proposed for the application of FSM systems based on IEC 61508 by the Conformity Assessment for Safety Systems (CASS) committee [13] and is based on a set of targets of evaluation. This concept has been further developed and adapted for use with IEC 61511 and the adapted targets of evaluation are shown in table 1 below.
IEC 61511 Functional Safety Capability Gap Analysis

Based on a typical set of the targets of evaluation (TOES) such as those in table 1 below, the objective of the functional safety capability gap analysis is to review the organisations existing plans, procedures and work instructions and map them to the IEC 61511 version of the TOES. The adapted TOES are based on the requirements of IEC 61511 [clause 5 “Management of Functional safety and the recommendations of the Conformity Assessment for Safety Systems (CASS) Guide [13]. This process assesses an organisations existing Functional Safety Capability and identifies any gaps between the requirements of the standard and the existing systems and where necessary provides recommendations for additional plans, procedures and work instructions to fill the gap between existing management activities and IEC 61511 requirements.

<table>
<thead>
<tr>
<th>T.O.E. Number / Description</th>
<th>Procedures and Controls Required to Comply</th>
<th>IEC61511 Refs. (Clause. Para)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General Requirements</td>
<td>FSM System</td>
<td>5.2.1</td>
</tr>
<tr>
<td>2.</td>
<td>FS Policy Statement</td>
<td>5.2.1.1</td>
</tr>
<tr>
<td>3. Organization &amp; Responsibilities</td>
<td>Applied FS Lifecycle Phases – Procedures</td>
<td>5.2.2.1</td>
</tr>
<tr>
<td>4</td>
<td>Competency Assessment Policy</td>
<td>5.2.2.2</td>
</tr>
<tr>
<td></td>
<td>Personnel Competency Procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Competency Assessment Report</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Training and Development Policy</td>
<td>5.2.2.2</td>
</tr>
<tr>
<td></td>
<td>Training &amp; Education Records</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance Appraisal Form</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Risk evaluation and Risk management</td>
<td>5.2.3 &amp; 8</td>
</tr>
<tr>
<td></td>
<td>HRA procedure including the requirement to identify the overall safety requirements and allocation of safety requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Procedures for maintaining information on hazards with respect to all safety related systems (Assessment &amp; Auditing)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Post Incident / Accident activities</td>
<td></td>
</tr>
<tr>
<td>7. Planning</td>
<td>Functional Safety Planning</td>
<td>5.2.4 &amp; 6</td>
</tr>
<tr>
<td>8. Implementation</td>
<td>SRS - Procedure / Checklist</td>
<td>5.2.5, 10, 11 &amp; 12</td>
</tr>
</tbody>
</table>
### Table 1 - Functional Safety Management System – Mapping Tables

<table>
<thead>
<tr>
<th>T.O.E. Number / Description</th>
<th>Procedures and Controls Required to Comply</th>
<th>IEC61511 Refs. (Clause. Para)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 and Monitoring</td>
<td>Validation &amp; Verification Planning</td>
<td>5.2.5, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>10</td>
<td>Supplier Auditing &amp; Assessment process</td>
<td>5.2.5.2</td>
</tr>
<tr>
<td>11</td>
<td>SIS Verification Procedure</td>
<td>5.2.5, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>12</td>
<td>SIL Conformance Assessment</td>
<td>5.2.5.3, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>13</td>
<td>Production Control &amp; Issue of SIS Docs</td>
<td>5.2.5, 5.2.6, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>14</td>
<td>SIS Project Checklists Procedure</td>
<td>5.2.5, 5.2.6, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>15</td>
<td>SIS Change Control Procedure for modification process of SIS SIS Fault &amp; Review</td>
<td>5.2.5, 5.2.6</td>
</tr>
<tr>
<td>16</td>
<td>Operation &amp; Maintenance Procedures including: Proof testing regime Proof Test Procedures Fault Reporting Procedure (Assessing dangerous failures)</td>
<td>5.2.5.3, 5.2.6, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>17 FS Assessment</td>
<td>Functional Safety Assessment Procedure and plan for functional safety management system formal review</td>
<td>5.2.6.1, 10, 11, 12</td>
</tr>
<tr>
<td>18 FS Audit Process</td>
<td>FS Audit Procedure and Schedule</td>
<td>5.2.6.2, 10, 11, 12</td>
</tr>
</tbody>
</table>

**Filling the Gaps in the Management of Functional Safety System**

The output from the functional safety capability gap analysis and mapping of the organisations existing plans, procedures and work instructions to IEC 61511 will be a set of recommendations to either update, revise or introduce new documentation and systems to improve compliance.

The introduction of changes to the existing system should be in the form of a roll out exercise through out the organisation and include a series of workshops / toolbox talks to keep staff up to date with the overall activity and to allow for feedback into the implementation team (Functional Safety Management Team).
The roll out exercise should also include for competency testing and assessment of staff that will be directly interfacing with the safety-instrumented systems, this should cover operations as well as maintenance and engineering. The next sections cover in brief the main components of the FSM with typical requirements for a process organisation implementation.
Organisation and Resources

The implementation, development and execution of the functional safety management system and all life cycle activities are overseen by a Functional Safety Management Team (FSMT) typically made of the plant management team.

The effective implementation of the functional safety management system is dependent on the skill set represented in the FSMT. Table 2 shows a typical skill set for a plant management team. The UK HSE provide guidance on managing competence for safety related systems [10] and this guidance should be implemented by using the task and function assessment Competency criteria in the IET guidance for Safety-Related Systems Practitioners [11] and the skill-requirements indicated below.

Table 2 Functional Safety Management Team Skill Set for a Process Plant

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Principal Competence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production Manager</td>
<td>Site-wide process knowledge, Operations Experience, Process safety</td>
</tr>
<tr>
<td>Engineering Manager</td>
<td>Legal Regulatory requirements, Maintenance Experience, Cognitive Viewpoint, Organisational Viewpoint</td>
</tr>
<tr>
<td>SHE Manager</td>
<td>Safety Management</td>
</tr>
<tr>
<td>C&amp;I Manager</td>
<td>Safety Instrumented Systems, Design Knowledge, Functional Aspects</td>
</tr>
</tbody>
</table>

Risk Evaluation and Risk Management

The FSMT ensures that, for each new project or plant modification, hazards are identified, risks evaluated and the necessary risk reduction determined as defined in process hazard and risk assessment below.

Planning

Based on the tasks that need to be performed at each phase of the safety instrumented system (SIS) implementation the FSMT should allocate roles and responsibilities to people (departments, individuals, staff or contractors) to perform those tasks and ensure that the activities identified in the FSM are included in the plan as listed below in the functional safety life-cycle section. This organisation and planning should be documented and reviewed as necessary when changes occur throughout the operational life of the SIS.

Implementing and Monitoring

The FSMT will take on the responsibility of ensuring that the FSM standard is correctly implemented and will monitor this through the use of the functional safety assessment process.
Functional Safety Assessment

Functional safety assessments should be undertaken at five stages during a project as detailed in figure 1. The FSMT will undertake and record formal functional safety assessments at each stage in the life cycle. As a minimum a stage three assessment must be carried out before the introduction of chemicals following a plant change.

The functional safety assessment should be performed and revalidated after any modifications, mal-operation or failure to deliver the required safety function. The depth and scope of the functional safety assessment should be based on the specific circumstances including the size of the project, complexity, SIL and the consequences of failure. The functional safety assessment should include consideration of:

- Hazard and risk assessment
- Functional safety management and planning;
- Hardware details; Minimum hardware fault tolerance; Random failure rates;
- Expected demand rate; proof testing;
- Design processes/systematic failures;
- Equipment quality;
- Software design process techniques/measures adopted;
- Maintenance; Operational and security arrangements;
- Organisational interfaces;
- Verification and Validation

A typical methodology to be applied for a process plant functional safety assessment is:

1. Review the HAZOP to identify the safeguards that are to be implemented as safety instrumented functions (SIF).

2. Review the cause and effects matrix to establish that all SIFs identified in the HAZOP have been carried forward.

3. Review the Layers of Protection (LOPA) report to establish that all SIFs identified in the HAZOP have been carried forward and a SIL determined as appropriate or carried forward for further analysis.

4. Review the SIL Verification report to establish that all SIFs that have a target SIL of 1 or greater have been carried forward for verification that the target SIL is achievable in terms of the Probability of Failure on Demand (PFD)

5. Review the SIS Validation Plan to establish that all SIFs that have a target SIL of 1 or greater have been carried forward for validation that the target SIL is achievable in terms of the techniques and measures used to reduce the risks from systematic failure.

6. Review the type of evidence used in the SIL Verification with respect to BS EN 61508 Certification or BS EN 61511 Clause 11.5.3 Proven -In-Use for validity.

7. Review software development plans and documentation structure to assure that the software FSM lifecycle has been applied to the appropriate target safety integrity level for each SIF.

8. Review the SIF loops to assure that all components within sub systems have been included in the SIL verification calculation and that architectural constraints have been met with respect to Safe Failure Fraction (SFF) and Device type.
9. Review Operation and Maintenance manuals to assure that the SIS can be operated and maintained to the designed safety integrity level for the lifetime of the plant and that the safety manual includes design / certification / P-I-U data for each component type and it is clearly referenced.

10. Review of the suitability of proof test procedures

11. Review of the Installation / commissioning plans and assurance that documentation is available and signed off for each SIF in terms of calibration, inspection, function, commissioning and check out sheets

**Auditing and Revision**

An annual internal audit of the FSM standard should be undertaken and a record made of any non-conformance and corrective actions in terms of non-application.

**Configuration Management**

Configuration Management is the process through which the FSMT can ensure that the correct versions of software are loaded and in use on a SIS. Through this process, a system can be completely rebuilt following a catastrophic failure, and the resulting system can be guaranteed to perform identically to the system prior to the failure and when modifications are required to the SIS software, it is important to know that all necessary changes have been made and no other. The configuration management system should include as a minimum a record of serial and version number for sub system, date and time of the last software change (if applicable) and by whom for each sub system component.

**Functional Safety Life Cycle**

The FSMT ensures that, for each new project or plant modification a Functional Safety Plan (FSP) is produced as defined below, figure 1 pictorially shows the life-cycle activities in each phase. The plan ensures that systems are in place to provide:

- Clear accountabilities with appropriate communication between all parties;
- Handover of information and delivery of equipment in accordance with the lifecycle plan

The FSP will comprise the following sections, which must all be present

**Identification and Competence of Personnel**

The FSMT will assess the competence of personnel in accordance with the IET guidance for Safety-Related Systems Practitioners [11] and decide who will be responsible for the various phases of a project or plant modification.

People with responsibilities should be competent to perform those tasks. The required competence is wide ranging and depends on the type of task. Competence typically includes engineering knowledge, process knowledge, system technology knowledge and experience, safety engineering, legal and regulatory requirements, management and leadership skills, understanding of the potential consequences of a failure and hazardous event, safety integrity levels and maintenance and testing activities.
Development of the Functional Safety Plan

Introduction & Overview
This section should state who produced the document, project or modification name and a brief description of the work and relationship to any external standards, if appropriate and Regulatory requirements

Organisation
In block diagram form showing interfaces between the various departments involved. These interfaces should highlight deputies to act in the event of the principal contacts being unavailable.

Reference Documentation
This section will include any specific reference documentation being used on the project.

Corrective Action Standards
All corrective actions arising during the project should be followed up and resolved. As these are reactive they cannot, by definition, be included in the FSP. The management of corrective actions should form a part of the auditing process.

Modification Standards
All modifications must be formally approved, authorised and initiated.

Phase Definition
This will indicate the lifecycle phases to be applied to the specific project or plant modification, the responsible person/organisation/department for the phase, the relevant documentation and the functional safety assessment activities relating to each phase.

Configuration Management
The timescales for configuration management are included in the FSP.

Operation & Maintenance / Safety Manual
The FSP should outline the standards used to produce the O & M Manual and the timescales for completion.

Functional Safety Assessment/Audit
Functional safety assessment activities must be planned into the FSP at the agreed stages.

Personnel Competence Forms
The FSMT should produce a Competency Assessment Report based on the IET guidance for Safety-Related Systems Practitioners [11] for each person responsible for lifecycle phases. These forms should only be referenced in the FSP as verification of competence of project personnel the actual forms should be administrated securely in accordance with the requirements for data protection.

Level of Independence
The FSMT will identify the appropriate level of independence in accordance BS EN 61508 [5], commensurate with the SIL level.
Figure 1 - Key stages of the Functional Safety Life Cycle (Total UK)

**Phase 1: Hazard and risk assessment**
- Description of hazards, safety functions and associated risk reduction
- Determine hazards and hazardous events, sequence of events, process risks and safety functions required

**Phase 2: Allocation of safety function(s)**
- Layers of protection, each SIF defined and SIL for each SIF
- List all SIF's, prepare detailed functional specification for each SIF, define software logic tasks and specify all factors relevant to SIL

**Phase 3: Safety requirements specification**
- Functional specification for each SIF, Software safety requirements
- Each SIF defined & SIL for each SIF

**Phase 4: SIS design and engineering**
- Design of SIS to meet the requirement for SIFs and safety integrity
- Integrate logic solver hardware and software, Factory acceptance test, Installation at site, commissioning of SIS, validation testing of all SIS functions on plant

**Phase 5: Installation, commissioning and validation**
- SIS operating in conformance with safety requirements, completed commissioning report, completed validation report
- Functional Safety Assessment (Verification)

**Phase 6: Operation and maintenance**
- SIS protection of plant achieved, Fully trained operators and maintenance team, Document records of proof tests and inspections
- Functional Safety Assessment (Validation)

**Phase 7: Modification**
- Evaluation of impact of design change on safety, Identify 1st phase of Safety Life Cycle affected by change, Authorize change, Changes to all affected phases and documents, Changes to SIS and retesting of affecting parts
- Proposed SIS design changes

**Phase 8: Decommissioning**
- SIF placed out of service
- As built safety requirements and process information
Verification
The FSMT should make arrangements to evaluate the performance and validation of the SIS that ensures that the identified safety requirements, functionality, integrity and BS EN 61511 requirements are met. This should include validation that the system design meets the requirements of BS EN 61511 and the system operation fulfils the design intent. Failures of the system or of any component should be investigated and recorded along with any modifications and maintenance performed. The details of any demands on the system, and system performance on demand, should be recorded including data on any spurious trips, any revealed failures of the system or its components and in particular any failures identified during proof testing. Records of all these events should be kept for future analysis. Records may be paper or electronic.

Process Hazard and Risk Assessment
A hazard and risk assessment is carried out on the process the assessment will result in the development of process safety performance indicators identifying the risk control systems in place for each hazardous scenario, and determining which of these are important to prevent or control the various challenges to integrity. The output from the assessment will provide:

- A description of each hazardous event and the factors that contribute to it including human factors;
- A description of the consequences and likelihood of the event;
- Risk control systems in place to control these risks and determination of requirements for additional risk reduction
- A description (or information) of measures taken to reduce or remove the hazard or risk and assumptions made
- The barriers and allocation of the safety functions to layers of protection;
- Identification of the safety functions to be applied as Safety Instrumented Functions.

Allocation of Safety Functions
An allocation of safety functions is carried out on the process and its associated equipment using the Layer of protection analysis [9] (LOPA) as the technique for allocating safety functions.

Safety Requirements Specification
A safety requirement specification is developed for each safety-instrumented function. The SIS requirements must contain the functional and integrity requirements and provide sufficient information to design and engineer each SIF.

Design / Development and Application Software
The design and development of the SIS must be in accordance with the FSM, the guidance in BS EN 61511 [6] and the Safety Requirements Specification for the specified target safety integrity level. The design documentation should specify and justify the techniques and measures applied during the safety lifecycle phases to achieve the systematic requirements of the specified target SIL. The application software must be specified, developed, coded and tested in accordance with the guidance in IEC 61511-1 clause 12 to satisfy the SRS and the specified target SIL.
Factory Acceptance Testing

Factory Acceptance Tests are performed to verify that the logic solvers and associated software together satisfy the SRS. Tests take place on a defined version of the software, and the version should be recorded. Results of the tests must be documented, stating whether the test objectives and criteria have been met, failures are also documented, stating the reasons and analysis of the failure and what corrective action has been taken.

Installation and Commissioning

To verify that all SIS components are properly installed, function checked and commissioned according to the specifications and drawings, an installation and commissioning plan is prepared that includes a listing of the installation activities, testing standards, measures and techniques to be used; timing and personal responsible.

Validation

Validation ensures that the SRS and BS EN 61511 requirements are met and includes Site Acceptance Testing (SAT) and commissioning. Software validation must demonstrate that the software does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation or by executing software functionality not defined in the specification.

Operation and Maintenance

Written procedures should be agreed and personnel identified as responsible and competent for the operation and maintenance of the SIS. The proof test interval will be determined by the calculation during the design process, and assessed and amended periodically based on plant operational experience and any discrepancies between expected and observed SIS behaviour.

Modification

All modifications to a SIS including software changes must be planned, subject to a management of change process and reviewed and authorised in accordance with the site MOC and the FSM system. The procedure should identify and address any potential safety implications of the modification, address the earliest relevant phase of the functional safety lifecycle dependent on the scope and complexity of the proposed change and consider not only the direct scope of the change, but also the full extent to which existing plant may be impacted. Operations and maintenance personnel must be advised of changes and training must be provided as necessary.

Decommissioning

The FSM must include a process for authorising and controlling changes prior to any decommissioning of a SIS or individual SIF. Particular attention should be paid to the sequencing of activities so that protection against process hazards is always provided. An impact assessment must be carried out updating any previous hazard and risk assessment and the relevant safety requirements including re-verification and re-validation.

Information and Documentation

The documentation should include process and instrumentation diagrams, system design and testing requirements, and a description of maintenance activities for the various components of the SIS from sensors to final elements inclusive. Documentation of the design should include risk assessment for SIL determination, design specification, factory acceptance testing, installation specification, and commissioning tests.
Product supply and safety manual

Product and service suppliers must have in place a FSM system including competency management and material control standards and provide a safety manual for their scope of supply.

Conclusion

To effectively assess the functional safety capability of an organisation against peers in an equivalent industry a benchmark is required and within the process industries IEC 61511 is the framework and risk based performance standard on which that benchmark and FSM should be based.

For successful implementation of the FSM continued monitoring of performance and a structured / systematic audit process are critical

This paper has demonstrated one methodology to benchmark an organisation against a set of targets based on IEC 61511 and offered a brief introduction into the FSM process.

References and Further Reading

1. The Control of Major Accident Hazard (COMAH) Regulations 1999
2. Health and Safety at Work Act etc., 1974
3. SI 1999/3242 The Management of Health and Safety at Work Regulations 1999
6. BS EN 61511, Functional safety – Safety instrumented systems for the process industry sector, IEC, 2004 Parts 1-3
7. Reducing Risks, Protecting People, HSE decision making process (R2P2) ISBN 0 7176 2151 0
13. The CASS Guide 26th April 2000 Issue 2.a