Implementing Functional Safety on Ageing Installations Offshore

Jasjeet Singh, Senior Consultant; Matthew Baggaley, Senior Consultant, DNV GL Ltd., Applicon House, Exchange Street, Stockport, SK3 0EY

The offshore oil and gas industry in the United Kingdom Continental Shelf (UKCS) is a mature oil and gas producing region, with more than half the fixed platforms approaching or exceeding their originally projected field life. There are potentially significant future challenges to be met associated with the prospect of some installations operating significantly beyond their original design life. Operating an ageing installation presents numerous challenges such as equipment obsolesce, changing legislation in an increasingly competitive market. There is widespread recognition and concern in the industry over retrospectively implementing current standards as not only can this process prove to be an expensive undertaking, the benefits are normally seen as not a good return on the investment. An example of the area where ageing installations are attempting to implement current standards is functional safety. In principle, implementing standards such as IEC 61511 on legacy equipment should yield immediate benefits such as a rigorous yet highly optimised management of instrumented systems.

A good functional safety programme should be able to identify safety functions that have a high integrity requirement on the installation taking into account the depleting field pressures, history of equipment performance in the field and team experience in operating the installation. It should also be able to optimise the testing regimes thus increasing plant availability and reducing the maintenance workload. This has direct cost savings. A good functional safety programme forecasts equipment obsolescence in instrumented systems, and trends the actual performance data to optimise management of these systems whilst predicting when the criteria of non-conformance may occur. This allows the pre-emptive actions to be implemented.

This paper is a continuation from the paper presented in Hazards 25 which was focused on new build offshore projects. The paper lays out a suggested road map for implementing functional safety management on a legacy asset and discusses the various steps of the process, challenges, potential pitfalls and benefits drawing on the experience from project work. It also highlights areas where significant improvements can be made resulting in improved safety performance, a manageable maintenance program for instrumented systems and associated cost savings.

Introduction

Background

The offshore oil and gas industry operates high hazard installations in increasingly harsh environments, and the effects of major incidents are potentially catastrophic in terms of safety, environmental and commercial impacts. The industry has evolved to become one of the largest consumers of sophisticated technology, with process safety heavily reliant upon state-of-the-art automated systems. The use of electrical/electronic/programmable electronic (E/E/PE) systems in safety applications is not new, but the way these are designed and managed is changing as the offshore industry progressively adopts international standards and best practice.

The International Electrotechnical Commissioning (IEC) introduced a series of standards after an elaborate consultation process involving a variety of industries where instrumented safety systems are employed. The standard IEC 61508 has become the basis of design for all safety systems that use E/E/PE technology. The use of E/E/PE systems in safety has been termed Functional Safety.

Implementing the functional safety standards on an existing facility is often perceived as a difficult, time consuming and expensive undertaking. Many question the benefits of such an exercise and even attempt to use the As Low As Reasonably Practicable (ALARP) principle as a way of avoiding implementing IEC functional safety standards. There is a widespread concern that such an exercise for an existing facility will result in a large increase in the numbers of safety instrumented functions (SIFs), and subsequently expensive re-engineering and increased maintenance and testing requirements. In reality, this is rarely the case. In fact, most installations can significantly reduce their operational costs related to instrumented systems by optimising their number, maintenance effort and testing requirements. A good functional safety program is capable of separating the wheat from the chaff of instrumented systems on a safety duty. Experience has shown that many existing safety systems are over-engineered, too complex, and include a number of functions which are not necessarily critical safety functions. Rigorous maintenance and testing of these systems has an associated financial cost which may be better allocated elsewhere. There is scope for a significant reduction in maintenance and testing workload and associated costs by reducing the number functions engineered into safety systems and reengineering them into non-safety systems or perhaps decommissioning them all together.

The focus of this paper is to highlight the benefits of implementing functional safety program on an ageing plant using offshore oil and gas installations as an example. The paper also presents learnings from a recent project undertaken by DNV GL to assist an operator in the North Sea, UK in implementing their functional safety program on an existing asset. The underlying principles mentioned in this paper are equally applicable to onshore oil and gas facilities, chemical plants and other process industry sectors. The authors hope that the contents of this paper will trigger operators and engineers to re-evaluate their strategy on functional safety and identify areas where the potential for reducing operating costs exists whilst improving overall safety of the installation.

Functional Safety Implementation on an Ageing Plant

Regulatory Perspective

The Health and Safety Executive (HSE) recognises BS IEC 61511 as relevant good practice for safety functions implemented by safety instrumented systems (SIS) in the process industry sector in the context of assessing compliance with the law in individual cases and the use of good practice1. Although this guidance is currently explicitly stated for industrial sites covered under control of major accident hazards (COMAH) regulations, the regulatory guidance is also widely considered to be appropriate to the offshore industry. The HSE recognises that a SIS commissioned prior to the publication of the IEC functional standards may not be engineered as per current expectations. In such cases the duty holder is expected to undertake a gap analysis to determine the extent of deviation from current good practice and put in place an action plan to bring such systems into line with the IEC standards.

The regulator further notes that:

"This standard can be used when reviewing health or safety measures on an existing plant/installation or situation (such as when considering retrofitting, safety reviews or upgrades), duty holders should compare existing measures against current good practice. The good practice measures set out should be adopted so far as is reasonably practicable. It might not be reasonably practicable to apply retrospectively to existing plant, for example, all the good practice expected for new plant. However, there may still be ways to reduce the risk e.g. by partial solutions, alternative measures etc.

Based on this information, it would appear logical that, if a site hasn't already done so, it should review its existing measures for managing the risks from use of safety instrumented systems against the provisions of BS IEC 61511. As a general rule, sites should be aware of which safety-instrumented functions are the most critical. It would make sense, therefore, that every site using non-61508 based standards should carry out a review of at least a sample of their installation to get some idea of how well the existing design compares with those required by BS IEC 61511. The findings from this review should then be used to make a decision as to whether or not further work is required."

The HSE has contributed substantially to the development and maintenance of the IEC standards, and has contributed to the development of guidance regarding its application[2]. In DNV GL's experience, the HSE expects a degree compliance with IEC 61511 and IEC 61508 in the management of legacy systems which includes the maintenance and testing regimes. This requirement is also formalised in the hazardous installations directorate (HID) inspection guide offshore – inspection of loss of containment[3], which includes a requirement for inspectors to review the functional safety assessments (FSAs).

It is worth noting that retrospective implementation of the functional safety lifecycle does not necessarily imply that legacy systems must be upgraded to meet new standards. This decision has to be made using techniques such as cost benefit analysis as part of ALARP demonstration. In practice, for systems where the required reliability targets are of significant magnitude such as a high integrity pressure protection system (HIPPS), it is advisable to plan continuous improvement; less critical systems where the risk reduction target for safety is outside the scope of IEC 61511 can be operated as existing legacy systems until such time when an upgrade is reasonably practicable.

Independent Verification Body Perspective

In our experience, most independent verification bodies (IVBs) such as DNV GL consider that in principle all installations should review their existing safety systems against the provisions of IEC 61511 and implement appropriate modifications where it is reasonably practicable to do so, although minor differences in interpretation of the standards may exist.

It is worth noting that such retrospective analysis of safety and control systems does not necessarily imply that legacy systems must be upgraded to meet new standards. The findings from the reviews should be used to aid a decision as to whether or not further work is required, and establish the extent of the required improvements so as to demonstrate ALARP. However, this does not imply that costly reengineering is always required. This decision can be made using techniques such as cost benefit analysis as part of ALARP demonstration. In practice, for systems where the required reliability targets are of significant magnitude, it is advisable to plan continuous improvement; less critical systems where the risk reduction target for safety is outside the scope of IEC 61511 can be operated as existing legacy systems until such time when an upgrade is reasonably practicable.

A number of requirements in IEC 61511 and IEC 61508 relate to management systems, rather than pure technological issues. It is prudent to review any existing systems against IEC 61511 and IEC 61508 as a part of the ongoing review of safety management systems.

This paper contains a road map which can be used as a guide to plan implementation of functional safety on an existing asset which employs safety systems engineered prior to the introduction of IEC 61508 i.e. systems commissioned before 2000 when edition 1 of the standard was published.

[1] http://www.hse.gov.uk/comah/sragtech/discguidciretro.htm

[2] Guide to the application of IEC 61511 to safety instrumented systems in the UK process industries, EEMUA 222

[3] http://www.hse.gov.uk/offshore/ed-loss-of-containment.pdf

The Benefits on Implementing Functional Safety on an Existing Asset

Implementing functional safety on an existing asset can yield significant benefits if it is implemented in a pragmatic and well thought-out manner. A rushed tick-box type approach on the other hand is likely to result in confusion, frustration and increased expense. Some of the more tangible benefits of a good functional safety program are described in the following sections.

Updating the Understanding of Hazards and Safety Measures

Many of the ageing installations would have gone through formal hazard identification and risk assessment processes at some point in their lifespan. Overtime, installations implement a variety of changes such as the addition of new equipment and the revision of operating procedures. In addition, the hydrocarbon reservoirs may have depleted and operating pressures may have reduced significantly since commissioning. Although, installations usually go through risk assessment processes analysing the impacts of these changes, a holistic assessment is often not completed due to time and resource issues. This can sometimes result in patched risk assessments.

In addition, there is typically excessive repetition of protection against some hazards whilst other hazards are not given due consideration. For example, an installation may have had a requirement for a high integrity pressure protection system (HIPPS) in its initial life but due to depletion in pressure, the HIPPS may no longer be required. Continuing with maintenance and testing of the HIPPS in the same manner as before is costly and unnecessary.

The functional safety program can be implemented to aid development of specifications for the replacement technology which reflect the installation's current design and operation regimes. A good functional safety program will specify the following activities as a minimum:

- Re-assess the hazards and current safety measures;
- Define a new set of safety functions taking into account the current hazard profile of the installation. The new set may include some of the previously defined functions, reject those functions which are no longer considered necessary and define new additions;
- Define the required performance level (e.g. SIL) and mode of operation (on-demand or continuous); and
- Explore other means of risk reduction which may be a better option than use of an instrumented system.

Changes to the physical equipment on an installation, or the way in which it is operated may significantly impact the number and nature of hazards, especially for field with depleting pressures. This in turn will impact the number and complexity of potential SIFs; typically resulting in a reduction.

For example, a project undertaken by an operator in the North Sea and DNV GL involved re-assessment of the HAZOPs where it was found that a significant number of hazard scenarios were either no longer valid, or not as severe as initially assumed due to lower operating pressures and revised operating procedures. Approximately 6000 line items of HAZOPs were reviewed, out of which approximately 600 were judged to be of sufficient hazard potential or complexity such that they would benefit from further analysis using layer of protection analysis (LOPA). A significant number of these were subsequently found to be false alarms i.e. they did not have the severity or complexity initially assumed. The overall assessment resulted in 55 SIFs which is a relatively small proportion of approximately 800 functions in the asset's current process and emergency shutdown systems.

Obsolesce Prediction and Management

Legacy systems are prone to obsolescence and careful consideration should be given to the useful life of critical components (including control system and ESD/PSD logic solvers). The obsolescence may occur due to technical or functional reasons, or it may be a planned change.

Technical obsolescence: Technical obsolescence usually occurs when a new product or technology supersedes the old, and it becomes preferred to use the new technology in place of the old, even if the old product is still functional. Another reason for obsolescence can be that supporting technologies may no longer be available to produce or repair the system components.

Functional obsolescence: Particular items may become functionally obsolete due to natural wear, or due to some intervening act. Products which naturally wear out or break down may become obsolete if replacement parts are no longer available, or when the cost of repairs or replacement parts is higher than the cost of a new item. A product may intentionally be designed to use a faster wearing component, a form of a planned obsolescence.

Planned obsolescence: Obsolescence can form part of a larger strategy with the objective of introducing more efficient technology, changes in requirements (e.g. new instrumented loops or higher reliability targets) or need for higher automation.

How Does Implementing a Functional Safety Program Help?

If it is considered that the relevant system could be rendered obsolete in the near future, the implementation of a functional safety program may prove to be highly beneficial. Installations will typically have a good overview of systems nearing obsolesce. However, there is a tendency to replace the outgoing system with a new system on a 'like-for-like' basis. This

implies that the safety functions implemented by the outgoing system are replicated in the new system without any consideration of whether they are now required, their required performance level (e.g. target SIL) or their testing options. This typically results in a mismatch between the hazards and the safety functions overtime.

DNV GL recommends that operators evaluate whether obsolescence is of consideration for the control and safety systems. This is likely to have an impact on the decision making process when evaluating whether implementing functional safety on legacy systems is reasonably practicable.

Maintenance and Testing Workload Optimisation

Design engineers are usually bound by the available capital and delivery schedules. Hence, little consideration is given to the operating costs. Process design contractors rarely consider operating costs during the design phases, mostly because the involvement of the intended operator is minimal. The lack of involvement and lifecycle considerations often results in a significant imbalance between the initial capital investment and future operating costs. This skewed relationship impacts the effort required for testing and maintenance of safety systems and these activities can prove to be overly disruptive to asset operation.

It is worthwhile to note that reducing operating costs does not imply 'less frequent' or 'reduced' maintenance. By due consideration of the safety lifecycle, an operator can achieve alignment of maintenance and testing strategies with the system design and operating procedures. The biggest benefit aside from safety of implementing functional safety on an existing asset is the potential to optimise maintenance and testing. A typical installation offshore will have at least a requirement to test every safety related item annually. This generates a large amount of workload and testing incurs significant costs. An optimisation process will help the operators to assess:

- What and when to test? Finding out what systems require testing and at what interval.
- How to test is it better? Improving the way a test is carried out.
- Who can test it? Improving the competence of the personnel.

The opportunities for significant cost savings from the optimisation of maintenance routines are many. Simply reducing the number of SIFs (or functions deemed safety critical) based on a thorough analysis, the maintenance workload can be significantly reduced. Also, the testing methods can be significantly improved using a bespoke method of testing which reduces both the time taken for the test and costs involved. Although the test routine on a single element may be more time consuming, existence of a pre-defined method makes management of the test much easier. Direct cost savings by reducing equipment downtime which affects production can also be significant. By developing optimised testing and maintenance routines, these can be scheduled to fit into planned shutdown periods resulting in further savings.

During the design phase, it is not uncommon to take the equipment failure and reliability data from generic sources, and assume the 'worst case'. An existing installation which has maintained good records of equipment reliability can make use of their databases and experience to estimate more representative reliability data. This, in some cases, may further enhance the potential for cost saving by giving reliable equipment due credit. It can also highlight the equipment items which have proved to be of low reliability. An operator can then assess if replacing these culprits with a different technology may yield long term benefits by improving upon the overall reliability of the system.

There is number of software applications available to end users to solve the complex mathematical relationships of functional safety and generate optimal test frequencies.

Quicker Turnarounds

Planned shutdowns cost money as the installation is spending on testing and maintenance whilst not producing. By reducing the number of instrumented items that require full, sometimes end to end testing, and performing tests online where feasible, the duration of planned shutdown can be reduced. A quicker and well planned test is also likely to be a cost effective test, especially in the long run.

Challenges in Retrospective Implementation of Functional Safety

Implementing functional safety in line with current standards on an existing installation is a challenging task. The challenges are a mixture of technical problems pertaining to the hardware and the software and safety management problems which include the safety culture and historical operating regime on an installation. Implementing functional safety retrospectively will cover more than the safety system and loops within that system; it will require a good understating of the process plant itself. Examples of the challenges that one might face in such a program are discussed in this section, drawing on experience from a recent project undertaken by an operator where they are being assisted by DNV GL.

Where to Begin? Need for Prioritisation

A major challenge in retrospective implementation of the IEC standards is deciding where to begin. A typical offshore production platform will house surprisingly large amount of process equipment ranging from subsea items to compressors. Process support systems such as gas dehydration and conditioning also play a critical role in the plant. Unlike a new build where the functional safety can follow the natural project lifecycle, an existing installation which has been in continuous operation cannot use the same approach effectively. Hence, there is a need for prioritisation to decide which part of the process plant should be the first one to be subjected to the functional safety implementation. This decision will vary based

on the objectives of the plan (e.g is it being implemented due to foreseeable obsolesce of safety system or addition of major new equipment?), the available time and resources.

The regulator will expect that the installation has at least reviewed its critical safety systems which provide risk reduction against process related major accident hazards. Hence, it would make sense to focus on the main hydrocarbon processes to begin with. Due to the very nature of the processes, it is inevitable that the majority of the critical systems will fall in this category. This approach was adopted by DNV GL for the North Sea operator. The team focussed on the main process systems such as separation, dehydration and compression to begin the process and get accustomed with the overall process systems. Other plant items were gradually brought into the scope of work based on their criticality, availability of relevant expert personnel and potential to cause major accidents.

Unavailability of Up-to-date Documentation

A major challenge which a retrospective functional safety program will face is to obtain accurate and up-to-date documents which are required to perform the various analyses. Typically, the following are required for the analysis phases where safety functions and their required integrity levels are allocated for an existing system:

- As built process and instrumentation diagrams (P&IDs);
- Up-to-date HAZOP studies; and
- Cause and effects charts.

In addition, equipment specific documents such as operating instructions and design manuals should also be consulted in the analysis. In our experience, these are not seen as an essential item by a number of technical consultants. However, we believe that analysis on an existing equipment item must consult these documents as they contain valuable information and more importantly, the operating boundaries and limitations of the equipment which are essential for completing an analysis which is a truly reflection of plant and the way it is operated. There is little value is assuming these limitations just to be verified or questioned during the later phases of the safety lifecycle.

In practice, the documents required for the analysis on an exisiting plant may not all be available. Also, the quality and consistency between these documents will vary, especially if the asset has completed these over a long period of time. For example, HAZOPs may have been completed and/or updated in stages. It is not unusual to find the HAZOPs to have followed different templates, guidewords, risk criteria etc. Hence, establishing a common baseline for the hazards can be challenging. In addition, the amount of information and detail available in the HAZOPs may vary significantly.

In recognition of this challenge, DNV GL adopts a stepped approach for completing the LOPA exercise on an existing asset. The approach essentially comprises data gathering followed by a review exercise to produce a list of hazards and initiating events to be subjected to LOPA.

Time, Resources and Commitment

It should also be kept in mind whilst planning the work that the analysis phases (review of the HAZOPs and completing the layer of protection analysis (LOPA) exercise) take significant amounts of time and resource. It can be very challenging for an operator to allocate their personnel to attend these studies, particularly in the current market situation. Hence, careful planning of the work is essential.

An operator should keep in mind that a functional safety program can take many months to reach a stage where it can be introduced with confidence. Rushing without careful planning severely limits the potential benefits such a program can deliver. For example, a carefully crafted and well run program will significantly reduce the costs related to testing of safety functions as not everything will need to be tested annually as a blanket requirement. In addition, by defining bespoke testing procedures, operators can reduce the time required for a test. On the other hand, a rushed program is not likely to consider capabilities of the equipment and whether an annual test is required. Mere allocation of ‘SILs’ in a quick fashion is likely to result in increase in SIFs.

A Road Map for Retrospective Implementation of Functional Safety

The IEC standards for functional safety are performance based rather than the traditional prescriptive style, hence DNV GL does not recommended a one size fits all recipe for implementing functional safety retrospectively. A fixed recipe would be considered against the spirit of the performance based style of the standards. In this section, an attempt has been made to list the primary activities, documents etc. that are considered key to the successful implementation of functional safety. The aspects covered are as follows:

- Functional safety management system;
- Project functional safety plan;
- Project competency management;
- Project configuration control;
- Functional safety assessments;
- SIS operations and maintenance procedures; and

- Proof testing procedures.

These aspects are similar to those described in a previous paper presented at Hazards 25 by the author.

Functional Safety Management System

It is recommended that the installation (or the operating company if dealing with more than one asset) develop a Functional Safety Management (FSM) system which provides the baseline approach to functional safety. The functional safety standards (IEC 61511 / 61508 / 62061) have a mandatory requirement to have a FSM system in place.

The SIS lifecycle consists of several phases which can be grouped into distinct periods as summarised below:

- Analysis Period: Phase 1 Hazard and Risk Assessment, Phase 2 Allocation of Safety Functions to Protection Layers and Phase 3 Safety Requirement Specifications;
- Realisation Period: Phase 4 Design and Engineering and Phase 5 Installation, Commissioning and Validation;
- Operations Period: Phase 6 Operations and Maintenance, Phase 7 Modifications and Phase 8 Decommissioning; and
- Management and Planning Period: Phase 9 Verification, Phase 10 Functional Safety Management and Functional Safety Assessments and Phase 11 Safety Lifecycle Structure and Planning.

The FSM system may be developed such that the strategy for retrospective implementation for the above periods is written to take into account the fact that functional safety will be implemented retrospectively. The overall FSM system is akin to a combination of four separate FSM systems, with one dedicated to each period. One benefit of such a structure during the execution of a project is that the workload can be distributed to different teams, each of which is responsible for different phases of the safety lifecycle.

The FSM system should define the strategy for at least the following components of functional safety implementation:

- Organisation and resources management;
- Risk evaluation and management strategy;
- Functional safety planning;
- Requirements for implementing and monitoring functional safety; and
- Strategy for conducting functional safety assessment and auditing.

The FSM system should also define the following critical aspects of retrospective implementation of functional safety:

- Prioritisation of systems and equipment within scope, and setting boundaries for the assessments;
- Defining tolerable risk criteria for all risk types within scope (safety/environmental/commercial);
- Defining the integrity level calculation philosophy, including gathering information about equipment repair times and historic reliability data;
- Define baseline requirements and limitations on proof testing regimes and establish an ideal testing frequency for online and offline testing – perhaps to coincide with planned turnaround outages; and
- Define the philosophy of using prior use data.

Project Functional Safety Plan

The Functional Safety Plan (FSP) should be prepared by a multi-disciplinary team representing all departments involved in the project to ensure that the plan is developed in a mutually agreed manner. The plan should identify the technical and management activities, and the procedures to be applied for all functional safety related activities. The plan is a live document that should be continually updated and maintained by the designated individual(s). As a minimum the functional safety plan should include:

- Roles and the responsibilities of individuals, departments and organisations;
- Competencies management and assurance plan of individuals;
- A description of the scope, timing and expected outputs for all relevant safety lifecycle phases;
- A description of the documentation requirements and configuration control techniques;
- The verification strategy;
- The validation strategy;
- Action tracking and management;
- Initiation, approval and management of modifications;

- The timing and scope of functional safety auditing; and
- The timing and scope of functional safety assessments.

Project Competency Management

The project should produce a competency management plan which acts as evidence of active competence management and assurance. The aim of competence management is to ensure that demonstration can be made that the persons involved with or responsible for the functional safety lifecycle activities are competent to complete their assigned duties.

Each role within the project requires a different set of competencies, and the requirements are also dependent upon the lifecycle phase. The project's competency management plan should define the minimum competence required in each phase of the lifecycle for various roles. This information can be presented in the form of a competence matrix.

Project Configuration Control

The intent of configuration control is to manage and maintain the traceability of all hardware, software and documents related to the SIS and to ensure that all modifications to the SIS are recorded, controlled and traceable throughout its lifecycle. Such a system may already be implemented on an existing asset. There is no requirement for a complete revamp of the existing system but it may need changes to include specific aspects of the FSM system. Configuration control procedures should ensure:

- All SIS devices are uniquely identified. Since an existing plant will have already allocated a system to tag items, it is critical that the functional safety implementation does not allocate 'new' tags;
- Unique identification of a logic solver firmware and operating system. This is of critical importance when functions are added or removed from a system. Hence it should include unique identification of the logic solver application software and function blocks;
- Protection against unauthorised manipulation and modification of the SIS; and
- Prevention of unauthorised items from entering service.

Configuration control for non-programmable components or items that incorporate fixed programs may be achieved through revision controlled equipment data sheets that record the following:

- Device tag number, manufacturer's name, part and serial number;
- SIL assessment certificate number (if available);
- Software firmware revision (if required); and
- Fixed program parameter settings (if required).

Programmable electronic systems (PES) that utilise a limited variability language (LVL) should have a separate software configuration control document that records the following:

- PES manufacturer, model, operating system version and edition, compiler version;
- Central processing unit (CPU) model number;
- Communication settings (Bus number, system ID, Baud rate, IP address etc.);
- Licence numbers (if required); and
- Access passwords.

The software configuration control document should record the revision history of the software application program and may include the revision number, date of revision, the author, code version and the description of version or modification.

The FSP should define the procedures and practises that ensure the above requirements are fulfilled. This may be done explicitly or by reference to the relevant documents. The plan should also detail the tools and techniques that will support the configuration control activities; this is of specific importance when external organisations will be responsible for configuration control during the lifecycle.

Functional Safety Assessments

Functional Safety Assessments (FSAs) are intended to provide an appropriately independent judgment on whether the functional safety provided by the SIS has been achieved and maintained throughout the life of the system. The standard describes five stages at which an FSA may be completed in the lifecycle. Stages 1, 2 and 3 occur in the natural gap between the periods described earlier. An FSA gives the project an opportunity to review progress, check the deliverables and take a view on the general health of functional safety activities.

It is highly recommended that an existing asset undertakes a stage 4 FSA (or equivalent gap analysis) at the start of the program to generate a clear list of deviations from the current standards. This exercise will prove to be essential in prioritisation of activities within the retrospective implementation of functional safety.

The FSM system and FSP should define the requirements for any FSAs, and provide general information for the project personnel on expectations at each FSA. The person(s) completing the FSA should consider the activities carried out and outputs generated during the lifecycle phases within the scope of the FSA being carried out. The appointments of the FSA assessor(s) should be made at an early stage in the project. This will ensure that the appointed person(s) can maintain a suitable level of independence from the project. In most cases a single competent person can be nominated to carry out the FSA. However, for large or complex projects an assessment team comprising several people with the appropriate competencies may be required.

SIS Operations and Maintenance Procedure

Ideally, the existing operation and maintenance procedures should be adapted such that they meet the requirements of functional safety as far as considered practicable by the asset. The procedures can be introduced gradually and adapted on an ongoing basis until an acceptable method is reached. However, certain aspects of maintenance may require a complete overhaul, especially if the current method is deemed poor or cumbersome by the operators.

The project should consider the intended method for operating, proof testing and maintaining the SIS. This includes consultation with the operations and maintenance representatives to note the desired proof test intervals. Also, the existing methods of trip and fault annunciation and diagnosis should be considered to minimise the mean time to repair and to facilitate the collection of demand and failure data. Typically, the following procedures will need to be developed (or require changes to the existing procedures) to implement functional safety:

- SIS by-pass and override procedure which may introduce restrictions and limitations on such activities when compared to the existing methods;
- Proof test method statements which will define the exact step-by-step procedure for testing a SIF;
- Proof test deferral procedures; and
- SIS spares holding procedures.

The team should also consider gradual introduction of the following:

- The instructions for completing and documenting a full proof test after repairs or like for like replacement;
- The process for tracking SIS component failures to facilitate the analysis of failures;
- The process for tracking demand rates to facilitate analysis;
- Procedures for the management of obsolete equipment;
- Processes for investigating SIS incidents including failure on demands, testing failures and spurious trips.

It is suggested that the operator develops and/or updates the procedures in the following sections. These can be refined and updated by the operations and maintenance teams who are able to provide feedback and suggestions to the functional safety team to ensure that any reasonable and/or essential changes can be made.

Proof Testing

The SIFs operating in demand mode of operation require periodic testing to evaluate if the SIF is performing as per the SRS and meeting its designed reliability targets. The Proof Test Method Statement (PTMS) should provide a clear, unambiguous, step-by-step methodology for testing the functionality of the SIF in line with the requirements of the SRS. It is suggested that a PTMS includes the following to improve the robustness and validity of proof tests:

- Description of the tests and inspections performed;
- Dates of the tests and inspections;
- Name of the person(s) who performed the test and inspection;
- Unique identifier of the SIF or equipment tested (for example, loop number, tag number, equipment number, and/or SIF number);
- Visual inspection of SIF elements;
- Validation of trip initiating values (set-points);
- Validation of correct logic action;
- Validation of the final element activation;
- Validation that the SIF speed of response is less than the process safety time;
- Validation of correct alarm and indication; and
- Test equipment used, serial number and calibration details.

Ideally a single test will cover the full operation of a SIF from the initiator to the final element. However, in some cases it is necessary to separate elements of the test to support operational requirements. In such circumstances, the testing of individual components/sections of the SIF must overlap to ensure full coverage is achieved and the PTMS should fully describe how full coverage is delivered.

Conclusions

Retrospective application of the functional safety standards can appear to be overwhelming. These standards, however, provide an excellent opportunity for operators to not only meet current good practice but save significant OPEX, year-on-year while boosting installation life and enhancing the safety of their operation.

A carefully planned and implemented functional safety program can efficiently support operators in reducing their operating costs. The introduction of functional safety management will require significant effort up-front and investment, but it is possible for the results to deliver large cost savings. Retrospectively applying functional safety yields improvements in quality, operations and maintenance costs, but above all, it results in a safe, efficient and profitable installation which manages its safety systems intelligently, in conformance with regulations.