Session 17:

Effective Risk Reduction in Processes: the Contribution of Functional Safety Management Systems

Edgar C. Ramirez
Safety Instrumented Systems Specialist, ABB Inc.

John Walkington
Functional Safety Manager, ABB UK.

Abstract

Industries that manage hazardous substances and activities seek risk reduction through the use of safety protective layers. In the case of safety instrumented systems, the Industry good practice standards IEC 61508/IEC 61511 require that their design, engineering and operation is in accordance with a 'cradle to grave' safety lifecycle approach with supporting safety management practices and the use of proven application tools and techniques. However, various circumstances can lead to deviations from full compliance during implementation of safety-related systems. Unwanted consequences include design and engineering errors, and lack of adequate safety critical responses during operations. The use of a functional safety management system can help process end users deploy safety measures in full compliance with Industry good practice requirements. Effective safety protective layers result in fewer hazardous incidents, spurious plant trips and operator interventions.

Introduction

The use of programmable control systems to implement safety functions is now a common practice within the Process Industries having being introduced and in operation for over 30 years. Applications include Emergency Shutdown Systems, Fire & Gas Mitigation systems, Boiler Management Systems, etc; and in support of these applications, several regulations have been developed and issued to provide guidelines for the engineering and operation of such safety-related systems.

Unfortunately incidents still occur in installations where safety measures have been implemented. It has been found [1] that one of the primary reasons such incidents occur has to do with problems that arise due to the improper implementation and operation of safety related protections based on instrumented safety systems. In this paper, a discussion on activities recommended by best practice safety systems standards is presented, along with examples of incidents and experience obtained with the implementation of safety instrumented systems based on a functional safety management system.

Risk Reduction: Identify the Issues

Risk reduction to levels acceptable for process operations is a principle that the functional safety standards IEC 61508 / IEC 61511 [2,3] postulate as a generic framework for the management of safety-related system projects and plant operations. Hazard and risk assessment techniques are used to identify process hazards and set the foundations for design requirements which lead to the implementation of safety instrumented functions. The intent is for process risks to be prevented and/or mitigated through implementation of safety protective layers such as safety instrumented systems (SIS), along with other technology solutions such as pressure relief, etc.

However, design, engineering and operation of instrumented safety systems can be sources of errors that have been found to cause loss of control and system failures resulting in process incidents. According to [1], when a group of incident root causes were analyzed the largest fraction of the safety related system failures were found to originate in the areas of poor specification, design & engineering, and plant operational problems, and modifications.

Some of the key causes identified leading to the above issues were:

- Poor specification of safety requirements
- Lax or non-existing verification and validation activities
- Operation and maintenance errors
- Deficient or non-existing management of change processes

Implementation and operating of safety instrumented systems is therefore an area where there is work to be done to eliminate errors that are potential causes of incidents. Several cases of incidents including catastrophic cases likely took place in part due to deficiencies in operational procedures for functional safety management.

Consider the following simple case of failure as described in [1]:

'During maintenance of a commercial microwave oven, the maintenance engineer noticed warmth in his hand while the oven doors were open. The engineer received microwave radiation in a condition for which an interlock was designed to stop the oven. The problem was subsequently traced to failure of the door interlock: the oven designers had been provided information on the basis that the doors would operate four times a day while in reality the doors operated approximately 200 times per day. The interlock failure was due to contacts failing in a dangerous way: the contacts welded together.'

Subsequent investigations led to the identification of three key problems:

- Deficient specification of requirements for safety integrity. Erroneous requirements led to selection of the wrong type of contacts.
- Inadequate design of safety protection that led to a dangerous situation upon internal system fault. On the presence of internal faults safety protections are typically required to fail to a safe condition.
- Testing and maintenance procedures were inadequate to ensure continuing safety integrity.

Although the above is a simple example of safety system failure, the deficiencies identified above can be migrated as a common theme to safety related systems that protect modern high hazard operating facilities today.

As such, the functional safety standards [2,3] mandate that implementation of safety-related systems shall be based on validated practices and procedures to prevent engineering and operational errors, including verification and the use of proven techniques and measures i.e. an increase in the operational practices to avoid systematic errors.

A safety lifecycle shows relevant activities and sequences

The definition of a safety lifecycle is a requirement within the functional safety standards [2,3] to illustrate activities in safety-related systems projects and operations and describe the phased completion sequence that is to be followed.

Considering the safety lifecycle defined within the IEC 61511 standard as an example, the representation of activities and sequences towards an end objective are provided in a simple and clear model which can be used to provide a ready visualization of the key requirements for both project execution and continuing plant operations.

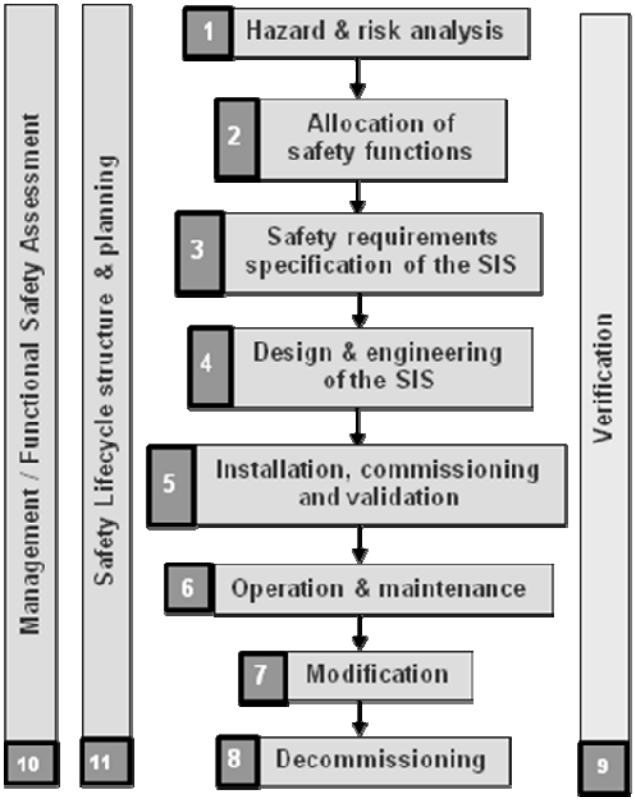

Figure 1. IEC 61511 Safety Lifecycle

Corporations that implement and operate safety instrumented systems are required to develop their own safety lifecycle in order to comply with requirements in the standards [2,3].

An important aspect of the safety lifecycle is that it allows Corporations to validate their safety management activities and responsibilities for the implementation of safety protective layers. Once a safety lifecycle is defined, it can be subject to analysis by internal and external auditors and any key stakeholders in order to provide a structured methodology to demonstrate compliance with best practices.

On the contrary, the lack of a safety lifecycle leaves the application of procedures and the sequence of activities open to interpretation by different teams who are involved in their use. Some activities and procedures can be completely missed if there are no descriptions of an agreed safety lifecycle detailing competency, deliverables, approvals, responsibilities, etc!

In addition, late completion of key activities within the safety lifecycle can also lead to problems. Safety functions that require modification of process equipment once it has been manufactured or installed can be very expensive, and pressure to keep projects within budget and/or schedule could lead to not implementing the full safety measures which were originally detailed at the risk and hazard analysis phase. Both situations can be much more costly, and the potential lack of safety protective layers post commissioning can lead to operational incidents with severe consequences at some point in the future.

Safety Lifecycle Management for SIS Design and Engineering

As an example, in the case of the specific activities related to the design and engineering phases of safety-related systems (Phase 10 of IEC 61508 Ed 2 and Phase 4 of IEC 61511), the safety lifecycle requirements include project activities covering the preparation of a proposal, receipt of a comprehensive safety requirements specification (SRS), interpretation of the SRS into a functional design specification (FDS), supported by appropriate project documentation and quality systems arrangements, detail design, engineering, manufacturing, testing and delivery of equipment to site.

Verification and management activities such as reviews, testing and management of change take place at various stages during the safety lifecycle. Figure 2 identifies the initial activities of the safety lifecycle, covering design and engineering of safety-related systems.

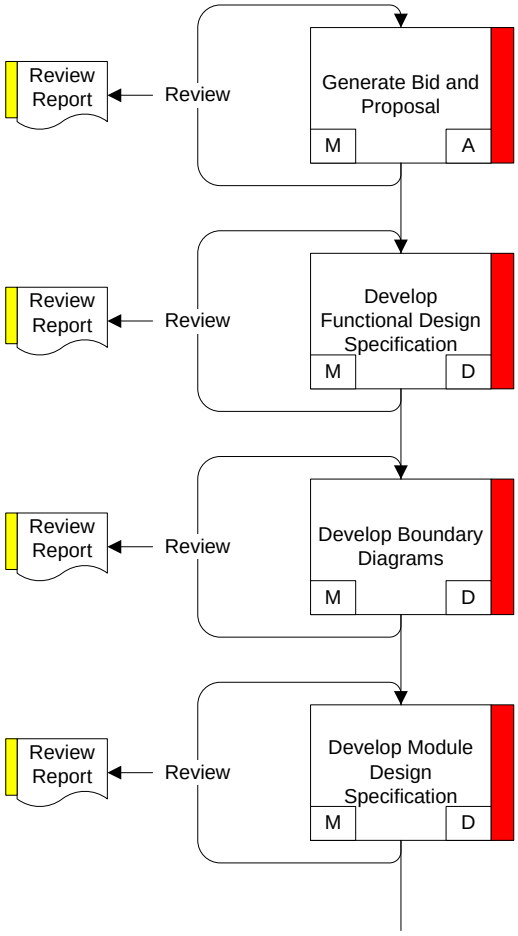

Figure 2. SIS Design and Engineering Activities in Safety Lifecycle

Developing an overall safety lifecycle management plan allows visualization and understanding of all the activities and deliverables required in projects and operations and contributes to enabling functional safety compliance to be adhered to. This type of approach supports the project team in maintaining functional safety awareness and to ensure life cycle phase completeness against the safety standards [2,3].

Management of Tools and Processes for SIS Projects and Operations

A fully developed safety lifecycle includes numerous activities that need to be managed. Adherence to the safety lifecycle requires Corporations to commit and manage resources. Engineering and project management processes and tools need to be used, and competent personnel are needed to take responsibility for activities. Securing and managing the required resources is understandably a critical function.

Management of Functional Safety is a fundamental requirement as found within the standards IEC 61508 / IEC 61511.

Validated Procedures and Documentation

Validated procedures and document templates are a means to support systematic capability requirements for safety-related projects and operations. For instance, requirements for performance of safety-related systems must be specified according to the risks that are being targeted and a sufficient level of detail on the safety functions to be implemented must be provided. Documentation that includes such items of information can be validated for compliance and released as templates for future uses.

Safety Requirements Specifications need to be produced for every implementation of the safety-related systems. Evidently validated procedures and templates for developing significant documents such as the Safety Requirements Specification will help prevent re-defining of the baseline safety case concepts, activities, documents, etc and if not systematically addressed by the use of validated procedures, may be the 'norm' repeated for every different project impacting on cost, time and resource management.

Implementation of safety-related systems requires the securing of competent resources and establishing compliant management processes to conduct all activities.

The need for Safety Management Systems

Functional Safety Management is identified in the Industry good practice standards [2,3] as an overall, permanent component of safety-related systems. It is a necessary step to make Corporations aware of the need to allocate appropriate resources and supporting management systems to accomplish risk reduction targets.

Safety-related system projects and operations implemented without a Functional Safety Management System (FSMS) in place, may give rise to diverse processes and practices conducted with varying results across the organization across all phases of the safety lifecycle. Consider the operation of safety instrumented systems for which there is not an enforced procedure to manage trip bypasses. Field instruments or final control elements could be out of operation without personnel noticing or being aware that safety systems are disabled with potentially serious consequences.

The lack of a FSMS in itself leads to non-compliance with the functional safety standards.

Implementation of a FSMS is not as arduous as people may think, as a FSMS is usually an extension of the company Quality Management System (QMS). Its scope is defined according to the activities of the company. Process industries need to manage the whole safety lifecycle, from conceptualization, hazard identification and specification of safety protective layers, through to engineering, implementation and operation, and including decommissioning when the asset is to be shutdown.

To support industry operators within this overall safety management lifecycle, companies such as responsible manufacturers of safety-related systems will already provide the necessary expertise and safety management deliverables that are focused on implementation of the control systems and engineering of the safety instrumented functions that a process user requires.

As in the case of a QMS, the requirements and components of a FSMS relate to procedures, document templates, forms and checklists, and an overall structure where all activities involved in safety-related systems projects are contained and linked to corresponding procedures and documentation.

As noted before, the functional safety standards [2,3] refer to the overall structure as a safety lifecycle that organizations involved in safety-related systems projects need to define and manage to be compliant for the lifecycle phase, or phases they are responsible for.

Functional Safety Assessment

As in the case of other engineering activities, design and engineering implementation of safety systems is still potentially subject to systematic integrity issues and omissions in the form of errors. A mechanism to help validate the integrity of safety systems during design, engineering and operation is through the use of supporting project functional safety assessments.

Functional Safety Assessments of safety instrumented functions (which are different to audits) are conducted as an investigation and judgment of functional safety associated with the safety-related system under review. During this assessment, typical engineering and operational activities analyzed would be:

- Definition of a safety lifecycle
- Satisfaction of competency requirements
- The application of functional safety procedures
- Functional safety verification and validation activities
- Re-verification of risk reduction requirements on a periodic frequency
- Etc

The above would be required to achieve safety integrity based on the initial requirements as outlined in the SRS stage of the safety lifecycle.

Note that the validation of full safety instrumented functions is the overall responsibility and therefore the challenge for the End User. The assessment of integrated sensors, logic solvers and final control elements, remains under their functional safety management lifecycle and hence a team within the process operator organization will need to meet functional safety competency requirements i.e. knowledge, experience, qualifications and training

Experience and Feedback from use of Functional Safety Management Systems

As with any new culture change, it is not untypical that as projects are executed with newly issued workflow and activity requirements, these initial work packages are often slower to realize due to the ‘learning curve effects’.

However as experience is gained, execution times greatly improve. What is important is that by adoption of such systems, the organization can clearly demonstrate its duty of care and professionalism when it comes to managing the requirements associated with safety related systems.

Increased Awareness of Safety Requirements

Awareness of safety standard requirements and expected deliverables during the project conceptualization, hazard & risk management and design stages is crucial in order to avoid difficulties to satisfy requirements later in the project and in particular to ensure that all required activities are identified and included within the project cost estimations and scheduling requirements. Here, supporting training for compliance to the safety standards and the importance highlighted for the additional safety verification activities are essential requirements for the project manager to ensure that functional safety compliance activities are satisfied.

Development of Personnel Competencies

One of the key elements for reduction of systematic failures during engineering, design and operations is personnel competency. Personnel involved in engineering, design and operation of safety-related systems need to have demonstrable competency for these activities, with related knowledge and experience. Competency requirements increase for engineering roles carrying a higher responsibility i.e. differences between SIL 1 and SIL 3 engineering.

Provisions for personnel development programs require decided effort and focus. Mentorship programs are an approach that have allowed participation of junior engineers to receive exposure and experience to safety related projects whilst at the same time receiving knowledge & application advice; including having their work reviewed and approved by experienced engineers.

Training courses and certification programs on functional safety standards [2,3] have proven valuable to introduce engineers to the requirements for safety-related systems. It is also important to maintain training programs to introduce new personnel to the companies Functional Safety Management System.

Certification schemes such as those provided by accredited third party organizations help provide supporting evidence to both the supply chain and the End User communities regarding suitable training level attainment and as part of the overall individuals competency development requirements.

Engineering Efficiency

Safety-related systems engineering activities while working under Functional Safety Management Systems have benefited from the clear understanding and sequencing of activities and completion of tasks and deliverables. This is due primarily to the availability of well proven procedures that balance and fit well the QMS procedures and in doing so list and describe project activities and are complemented by design documents that are initiated based on templates and guidelines.

While this is a standard engineering expectation, to accomplish this while achieving compliance with functional safety requirements can be very challenging and time consuming if there is a lack of validated procedures for safety-related systems projects.

Updates and Revisions

The need to maintain awareness of safety standards changes and updates can be demanding for organizations: procedures and documents may need updating when new versions of the standards are released. Revisions to

procedures may also be needed when feedback from projects and operations is received.

For End Users seeking additional assurance from their suppliers regarding such functional safety management systems the feedback and validation of supply chain procedures can be provided by accredited third-party certification agencies.

Accredited certification can provide independent assessment on compliance with safety standards requirements. This assessment gives the End Users the added benefits relating to safety systems when seeking suppliers that can readily communicate to business partners their compliance with Industry best practices.

In large organizations where multiple offices / sites deliver and operate safety-related systems it is convenient to maintain a common Functional Safety Management System (FSMS). Consider the case of ABB, integrated by local business units in numerous countries where the same third party accredited FSMS model is used to engineer safety-related systems. The local units adapt the FSMS according to local regulations while maintaining compliance with safety standard requirements. A lead unit is responsible for maintaining and updating the master set of procedures and documents. In doing so, ABB provide the same functional safety rigor and project deliverables mapped to the safety standards lifecycle models over some 20 geographical regions.

Operational Requirements: Less Incidents and Spurious Trips

The definition of the Safety Requirements Specification (SRS), a key activity where the safety instrumented functions to be implemented are specified in detail, is the main technical enabler in order to ensure that essential information is transferred from the hazard studies into the design arena. This is required so that incidents are prevented through the deployment of appropriately engineered safety related systems to reduce the potential impact from the critical risk demands identified.

Operational requirements should be expressed in the SRS including the SIS performance and conditions to maintain continuous operation. Considering that certain safety instrumented systems are designed to bring plant and processes to a safe state, in most processes it is desirable to avoid frequent shutdowns caused by spurious trips. Definition of requirements that include additional fault tolerance and supporting diagnostics can help prevent frequent shutdowns due to safety system module faults.

Hence operators of process plants seeking sufficient risk reduction combined with availability can prevent accidents while optimizing the cost of safety with less spurious trips.

Management of Change

Poor management of change has repeatedly been found to be a cause of incidents as this has often led to safety systems being operated in conditions different from their original specifications.

Experience suggests that technical ‘impact assessments’ on the necessary changes have not been as thorough as required and as a result, potentially affecting safety integrity. This can also be significantly compounded over time whereby multiple modifications have occurred to the SIS without the supporting

impact assessments and documentation being available. This is even more challenging when it comes to evolve the system to the next generation logic solvers as the actual number of SIF's, their cause and effects and specific hazard scenarios they are protecting against, may well not be fully known or documented by the operator at the point of upgrade.

Ideally the use of tools and procedures for management of change includes a formal assessment of impact on safety integrity which includes the documentation of reasons for the changes, a detailed description of the scope of the change, and supporting safety impact analysis affecting all elements in the SIS. This also allows maintaining backward and forward traceability records as required in the IEC 61508 standard [2].

Summary

The adoption of functional safety management best practices requires the commitment of both the Process Industry Corporations and the Supply Chain to support safety lifecycle management and implementation to ultimately provide the End Users with the necessary systems to operate in compliance with their 'duty of care' requirements. The resulting processes within such safety lifecycles facilitate the engineering and operation of effective safety solutions.

Key contributions to this duty of care are delivered from the adoption of Functional Safety Management Systems towards the achievement of risk reduction objectives which can be listed as follows:-

- Focus on hazard identification and risk reduction
- Adoption of measures to prevent errors during implementation of safety-related systems
- Traceability from specification, throughout design, engineering, and changes during projects and operations
- Adoption of functional safety best practices that are auditable by third parties. This leads to reduced company liabilities

Corporations lacking a Functional Safety Management System will still need to ensure they have in place the resources and competencies to address the above requirements in order to operate safety-related systems. By implementing such a lifecycle management system and seeking supply chain partners who have the same consistency for improving safety performance, then the benefits to the End Users are clear and represented in the form of:-

- Assured safety related solutions
  - For SIS systems, third party assessed & certified
- Meets 'ALARP' for the cost of safety: risk reduction *'As Low As Reasonably Practicable'*
- Stakeholder/shareholder confidence
- Traceability for both technical and competency requirements
- Meets corporate and regulatory expectations
- Basis of safety fully documented

- Best in class Process Safety Management (PSM) sustained
- Sustainability of functional safety throughout the asset lifetime

References

1 Out of Control - Why control systems go wrong and how to prevent failure. HSE Books, 2003

2 IEC 61508 Edition 2.0. Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010

3 IEC 61511. Functional safety – Safety instrumented systems for the process industry sector. 2003

Contact: edgar.c.ramirez@ca.abb.com