One Approach to Functional Safety Assurance and Safety Lifecycle Compliance

John Walkington, Suresh Sugavanam, Stuart R Nunns

Safety Lead Competency Centre Manager, ABB UK, john.walkington@gb.abb.com, Safety Lead Competency Centre Functional Safety Consultant, ABB UK, suresh.sugavanam@gb.abb.com, Safety Lead Competency Centre Managing Consultant, ABB UK, stuart.nunns@gb.abb.com

Keywords: Functional Safety, Supply Chain, Assurance.

Abstract

This paper will explore and highlight the challenge for the Asset Owner/Operators and how they discharge their responsibilities for functional safety management (FSM) into the supply chain. In doing so, the paper will go onto explore how the four key elements of FSM (with a focus on instrumented safety systems) can be brought together to augment confidence and ultimately increase assurance that the developed basis of safe operation is valid and appropriate.

1 Introduction

Process Safety Management (PSM) and Functional Safety Management (FSM) is complicated by the fact that process owners have a duty of care to ensure that everyone in the supply chain is providing equipment and services that comply with Industry acceptable safe practices. When people talk about health and safety at work today, there is still a tendency to focus on managing the statistics associated with *occupational* safety issues, such as slips and trips and falls. Fortunately, most of the injuries from these sorts of accidents are relatively 'minor' when compared to the potential consequences of some of the other possible risks and hazards associated with high-hazard industrial workplaces. In contrast, *process* safety management is about securing industrial facilities against the sort of incidents that can lead to headline-grabbing catastrophes, such as Seveso, Bhopal, Texas City, DeepWater Horizon, Buncefield, etc.

Such high-profile events can have a widespread impact on people and businesses. What's more, the past five years have seen a shift in the legal landscape for those responsible for safety within the Process Industries. Any breaches in functional safety do not only impact the corporate entity involved at the centre of the incident; they can also have an impact down to the level of the individual managers.

In this environment, process safety management and its implementation through functional safety management regimes is more important than ever. If the worst happens, process owners and managers will need to show that they've fulfilled their *duty of care* or they could end up in challenging and difficult discussions with both internal and external stakeholders.

At the same time, there has been enormous competitive pressure on process operators in high hazard industries such as the Oil & Gas and Petrochemicals sectors to streamline their operations. For many companies, this has meant outsourcing expertise and manpower that is not central to their core business. While this may result in lower operating costs and a leaner organisation, it may also mean that certain in-house technical capabilities have been reduced and in the worst case scenario lost altogether.

2 The challenge of change

The Process Industries today are facing ever increasing demands to demonstrate that their operating risks to people, the environment and the workplace are minimised to acceptable levels. To achieve this requirement, operator's must continue and improve to:-

- Engineer the operating facilities to appropriate technical standards and industry good practices
- Operate and maintain plants using appropriate (functional) safety and quality management systems
- Use competent resources throughout both the project and operational lifecycle of the equipment in use

When we start to consider functional safety management and the development of risk reduction measures, invariably the use of a dedicated safety instrumented system (SIS) will usually be at the heart of the operational risk reduction strategy. Identification of such risk reduction requirements will be via the company's safety management systems and these responsibilities (but not ownership) can on occasion be discharged for implementation to key engineering partners for adherence and compliance.

Such management systems will need to address corporate responsibility, development of a safe culture of work, implementation of a basis of safe operation and competency for staff at all levels within the organisation and how this is mirrored and assessed within the supply chain. It will also need to consider how the various levels of compliance to industry good practice are discharged into the supply chain, where partners and suppliers are expected to meet their own

functional safety management and competency assessment obligations.

In developing a basis of safe operation, the Asset Owners need to have systems and procedures in place that can address the needs of linking together Process Safety, Functional Safety, Product Safety and Competency Assurance in a seamless and transparent manner. Ideally all four parameters (see figure 1 below) are required to come together in the desire to reduce the operating risks to a minimum, or 'As Low as Reasonably Practicable' (ALARP).

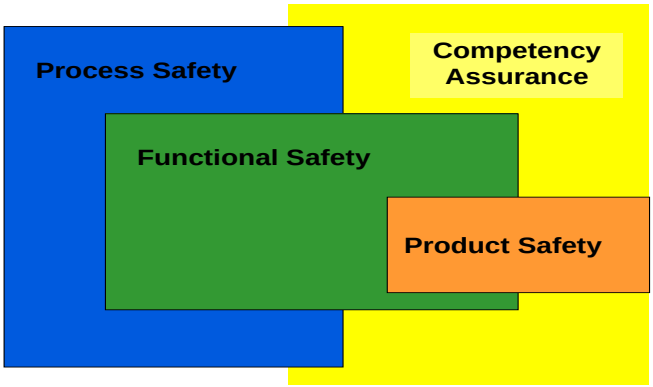

Figure 1 – Linkage of the key safety assurance parameters

Fundamentally, this commitment by the Asset Owner should ensure that an adequate *basis of safety* is derived for all of their operating facilities. This *basis of safety* should cover the requirements for process safety management, hazard and risk assessment, the development of protective and mitigation measures, and the standards and systems to design, engineer, install, operate and maintain to world-class standards.

Each key attribute for the basis of safety is described further below:-

Process Safety Management

- A key Asset Owner requirement
- Responsibilities and duty of care
- Demonstration of safe manufacturing
- Compliance with regulation
- Continuous measurement, improvement reporting and key performance indicators

Functional Safety Management

- Technology driven
- Methodology, procedures and systems
- Compliant with legislation, prescriptive standards/Industry good practice
- Compliance with the overall safety lifecycle

Product safety assurance

- Fit for purpose
- Safety manuals in accordance with corresponding safety standards
- Performance guarantees

Competency assurance

- People and organisations
  - Knowledge, experience, training and qualifications
- Attainment of recognised Industry training and certification

Fundamental in this process is the development of a culture that encourages safe working practices and senior management commitment. This means there is an Industry requirement to improve the basis of safe operation covering (see figure 2 below):-

- Equipment integrity
- Operational integrity
- Competency development

Of course, day-to-day safety will always be a priority in any responsible organisation, but a lack of in-house competent resources can make it difficult to manage and optimise functional safety reliably, when any big changes occur such as during a new-build project, or a major plant upgrade.

Figure 2 – Linkage of the Key Safety Assurance Parameters

3 Impact on the Supply-Chain?

Today, in most Asset Owner organisations, the capacity to engineer large scale safety projects and have resident functional safety expertise is no longer the norm. Rightsizing and downsizing is common place, mergers and acquisitions frequently result in core expertise becoming fragmented or lost. For these lean organisations and management structures there is an ever increasing requirement for the provision of products and services from competent third parties. Equally many large safety projects involve complex supply-chain models with complex interactions, responsibilities and deliverables. This can typically involve a consortium of Asset Owners, Regulatory Bodies, Engineering Procurement Contractors (EPC's), third-party auditors and functional safety assessors, engineering and design organisations, accredited certification bodies, independent consultants, etc.

In some cases, Asset Owners have difficulties in fully understanding the requirements of the functional safety standards themselves and experience difficulties in understanding on who has the overall responsibility for

managing the achievement of functional safety throughout the lifecycle of the project.

Whilst the Asset Owners are the ultimate duty holders, the above dimensions are not solely confined to and owned by them within the execution of the lifecycle. For example, the requirement for functional safety management and competency spans all organisations within the safety supply chain; product safety aligns more closely with the suppliers of mechanical safety devices, safety instrumented systems and system integrators, whilst process safety aligns more closely with the operators of hazardous installations.

This requires Asset Owners to drive the requirements down through their supply chains, define and implement a consistent safety/asset life cycle model and for the whole organisation to take responsibility for their respective roles within this safety life cycle. In every phase of a project and in on-going operations following its completion, the person(s) responsible for functional safety management need to identify hazards and risks, and build in layers of protection to reduce those risks to a tolerable level. Protection will probably include control measures such as safety instrumented systems (SIS), physical protection such as pressure relief and containment systems, as well as management and working practices that build safety into daily operations and are designed to promote traceability and transparency (with human factor considerations included).

4 Someone needs to "own" this functional safety role and manage the complex chain of events?

The difficulty is that large projects often involve complex supply chains, including the Asset Owner, the primary contractor, several secondary contractors, component suppliers and system integrators; and the list can include dozens of separate entities. Then there's the regulatory compliance input on top of that and the potential for corporate auditing and compliance linking back to the PSM leading and lagging indicators for the demonstration of continuous improvement.

In the past, process owners may have had an entire team responsible for designing, specifying, checking and verifying safety-related systems. These days, there might be one person who takes on the responsibilities of implementing functional safety , in addition to their other duties as site manager, production manager, control engineer, or whatever.

However as you can imagine, the breadth of competency requirements spanning the functional safety management lifecycle will need the skill sets that are to be applied across all technical engineering disciplines. Clearly this cannot be undertaken by one person alone, so the fundamental question is, how is this managed within a multi-company operational dimension (or a Matrix Project Environment) i.e. just who is responsible for what, where and when?

5 Other influencing factors?

Building further on the issues raised above, both the Asset Owners and the supply chain are constantly affected by both macro and micro market dynamics usually in the form of:-

- Rightsizing/downsizing, mergers and acquisitions
- Fragmentation of core expertise, loss of competencies and 'corporate memory'
- Increasing reliance from Asset Owners on sourcing credible third party providers of appropriate products and services
- Complex supply chain delivery models
- Difficulties in the recruitment of competent resource caused by the current 'skills gap'

So what problems does this create for managing the requirements of both PSM and FSM? With such complex interactions being evident and with several organisations working within the supply chain this could potentially lead to issues affecting:-

- Ownership/roles & responsibilities?
- Specifications, sizing, performance?
- Project costs, timeframes and risk
- Competency assurance
- Traceability
- Terms & conditions
- Approvals, audits, assessments & fitness for purpose
- System maintenance
- Regulatory compliance and due diligence

Experience suggests that this usually manifests itself in a lack of clarification of safety requirements from the standard hazard identification studies, a too conservative or inadequate development of the basis of safety, overspend on unnecessary equipment, lack of definition and cost effective proof testing regimes, inadequate assessment of supplier's capabilities and competencies, etc.

Ultimately for the Asset Owner organisations this has the potential for non-compliance with regulatory expectations and demonstrating due diligence via an auditable, documented and comprehensive audit trail. Therefore what is and should be attractive for Asset Owners in this demanding environment is, working with a supplier who can help address the management issues identified above. Certain organisations can offer leading edge safety related products and certified competencies as a lifecycle approach and in doing so can provide additional assured confidence when developing their basis of safe operation.

Today, one Industrial approach to assist in achieving these requirements is, utilising the safety lifecycle models as found within IEC61508[1] & IEC61511[2] (and the equivalent ISA84[3]) functional safety standards (see figure 3 below), to align the FSM requirements in terms of processes, structure and deliverables as a means of demonstrating overall improvement.

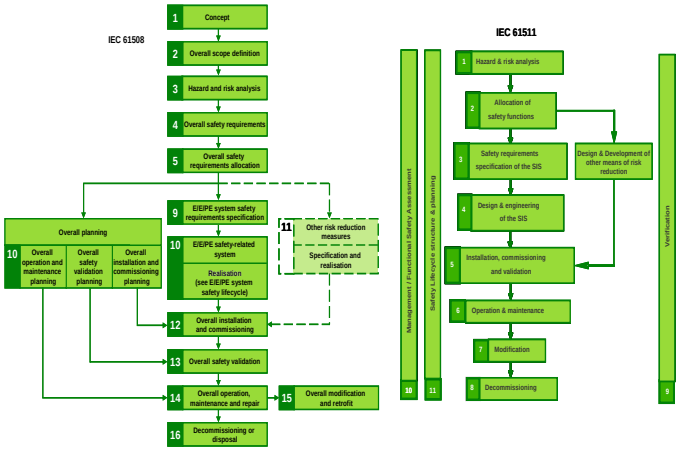

Figure 3 – IEC 61508 & 61511 Functional Safety Lifecycle

6 Competency expectations?

The right person to manage this complex interaction and varied mix of FS management deliverables will need enough expertise to ask the right questions to contractors and suppliers, and to analyse and understand the answers. A competency model needs to be established covering knowledge, experience, training and qualifications. These need to be measured against a specific set of functional and task-related competencies, set in a specific context.

There's no tick-box prescription for the perfect functional safety responsible manager, but they will invariably derive the necessary expertise from some combination of the following:

- Knowledge. They may have specific functional safety competencies at a sector, plant and systems level, covering a multitude of technologies. They'll know about the relevant regulations and directives.
- Experience. Someone with, say, 10-15 years of working in relevant roles within the Industry will typically have an in-depth understanding of functional safety issues, with or without higher level qualifications.
- Industry training. Third-party certified or equivalent training providers can deliver continuing professional development with functional safety in mind. Some also add to this training by way of a third-party certificate for the individual, which recognises their functional safety competence.
- Qualifications. They may have specific qualifications that give them the background knowledge to understand the relevant theory related to safety instrumented systems. Qualifications might include:
    - A degree or similar in control engineering/system safety engineering.
    - Personal professional development leading to Chartered or Incorporated Engineer status.
    - Formal recognition by industry peers as an expert in the field.

Yet, however competent they might be for the role, those responsible for today's functional safety compliance requirements are likely to have far fewer resources at their disposal than they might have done in the past. Given such pressures on resources and time, this means that they are effectively looking for ways to manage as much of the detailed work as possible down through the supply chain. The priority then is for them to understand enough about functional safety management to engage with suppliers and ensure that each organisation is fulfilling its responsibilities and securing its deliverables in the overall safety lifecycle supply chain.

Functional safety standards have a vital role to play here. More specifically, using suppliers and contractors who are third-party certified as compliant with IEC61511 and IEC61508, can give process owners and operators additional confidence that they can rely on the organisations they're working with not to drop the ball on functional safety. What's more, it means that the functional safety deliverables within the supply chain are demonstrable and transparent to key stakeholders, both internally and beyond the Asset Owner organisation.

7 Differentiation in the safety related supply chain?

In practice, this means that a company supplying safety related systems in accordance with good practice standards will be able to offer robust designs and have the testing and verification processes in place to ensure that critical safety systems are installed fit-for-purpose and will work properly when demands are placed upon them.

The challenge for the Asset Owner on how they discharge their responsibilities both internally and with their supply chains i.e. (EPC's), is how the four key elements described earlier can be brought together to increase confidence and ultimately increased assurance that the developed basis of safe operation is valid and appropriate.

By working with companies that can align their services to the overall safety lifecycle(s) requirements; the key functional safety parameters can be matched in a seamless and competency assured way i.e. the use of a supplier who has a third-party accredited certified competency assurance scheme in place, supported by third-party accredited certified safety products and design and engineering application solutions.

There are advantages provided by compliance and the potential to improve efficiency in SIS implementation when having a repeatable process that leads to compliant SIS. For instance, during execution of a phase such as "safety requirements specification of the SIS" (see phase 3 of IEC 61511 in figure 3) the safety requirements specification

document would be available as a template which provides structure and a basis for subsequent design engineering.

Such reuse of engineering procedures and documentation leads to more efficient use of resources. There may also be significant potential for efficiencies for process operators who deploy and operate many SIS as part of their continuous operations.

Management commitment is of course very much needed to ensure that the functional safety management system is developed and adequately maintained/modified should there be changes to international, national or corporate standards and regulatory requirements.

Functional safety management systems (FSMS) can help process operators achieve functional safety beyond the implementation of a SIS. Effective safety related systems need to be engineered, operated and maintained according to the functional safety requirements i.e. safety related systems need to be validated after construction to ensure that they meet risk reduction requirements and that they include proof testing regimes required to ensure that safety integrity is maintained.

A FSMS can provide some of the detailed definitions needed to achieve and maintain safety integrity of safety instrumented functions (SIF's) and there is increasing evidence that process operators are implementing functional safety as part of an overall safety management scheme.

8 So what does a FSM system need to cover and by association, what needs to be managed between the Asset Owner and the supply chain?

In considering such a seamless approach, the following detailed activities are considered core in supporting both Process Safety and Functional Safety management requirements:-

Hazard & Risk Management

- Development of process safety management systems
- Behavioural safety & culture
- Process hazard review (PHR) and/or hazard studies (including HAZOP 1-6)
- Mechanical integrity assessment and asset Life
- SIL determination
- Computer hazard & operability studies (CHazop)
- Hazardous area risk assessment and zone classification
- Environment impact assessment
- Risk modeling
- Occupied buildings risk assessment
- Pressure relief design & calculations
- Civil & structural systems i.e. bunding and containment

Safety Instrumented System Delivery (ESD, PSD, Alarms and Fire & Gas)

- SIL achievement
- SIS specification
- Detailed design and engineering - SIL capable
- Competency assured TüV[4] certified FS Engineers
- TüV[5] global certified safety execution and engineering centres (SEC's)
- Comprehensive functional safety management systems methodology and documentation aligned to IEC 61508 & IEC 61511 including functional safety assessments and audits[6]
- Commissioning
- Validation

Operations & Maintenance

- Reliability and operations improvement
- Modifications, upgrade management
- Brownfield project delivery
- 24/7 service level agreements
- TUV global certified service organisations (CSO's) for maintaining functional safety performance
- Safety management assurance and improvement
- Proof testing and repairs
- Operating and maintenance procedures

Operational Management and Management of Change

- Organisational culture/change
- Human reliability assessment
- Safety critical procedure assessment
- Staffing levels and workload assessment
- Pre start-up safety review
- Legacy systems review
- Control room performance assessment
- Alarm management and nuisance alarm health check
- Safe systems of work
- Management of change auditing
- Mechanical integrity auditing
- Incident investigation support

Critical to managing the above work scope is the visibility of who is responsible for ensuring that, functional safety is delivered throughout the safety lifecycle activities. The above core activities require dedicated, competent resources in full alignment throughout the supply chain to truly deliver the necessary risk reduction requirements and this is by no means a straightforward task. This is where a FSM system which has been assessed as being compliant with the standards by a reputable accredited third party can assist the visibility and traceability of functional safety scope requirements and verified deliverables.

Invariably the basis of safety will identify the need for SIS. The application of modern programmable technology offers significant economic and safety benefits to Asset Owners and operators of hazardous processes. However, to exploit this potential the technology must be applied in a compliant and

competent manner and this means the adoption of Industry good practice and the corresponding relevant standards such as IEC 61508 and IEC 61511. In any case, the requirements of these standards cannot be ignored, especially as Industry across all sectors is specifying them as a functional safety benchmark and a contractual requirement.

So what are the perceived benefits from an increased safety assured solution? By harnessing the use of a supply chain that can provide a seamless safety assured solution and in doing so, provide all the necessary deliverables as outlined previously, an Asset Owner is better able to demonstrate that their Process Safety Management and Functional Safety deliverables do indeed match the whole of the safety lifecycle requirements. By engaging with such a provider, the benefits to both the Asset Owner operators and the project EPC's would be as follows:-

Asset Owner/Operators

- Assured and traceable safety related solutions
- For SIS systems, third party assessed & certified
- For pressure relief – design verification approved
- For mitigation and containment - design verification approved
- Demonstrating that due diligence in terms of competency assurance has been discharged
- Meets 'ALARP' for the cost of safety
- Stakeholder/shareholder increased confidence
- Meets corporate and regulatory expectations
- Basis of safety fully documented in relevant safety case material
- Best in class Process Safety Management sustained

Engineering Procurement Contractors (EPCs')

- Global approach to design and installation of SIS
- Ease of contractual arrangements/less variability
- Confidence in meeting clients requirements
- Independent (functional) safety assessment and audit
- Appropriate documentation and auditing
- Ease of production of a safety case file
- Reputation and differentiation

9 Conclusions

Whether embarking on delivering a new (Greenfield) project, or for managing your existing (Brownfield) asset, for increased safety assurance, the requirement to ever improve process and functional safety management techniques and competencies should be paramount within any responsible organisation.

To do, this requires senior management commitment and a willingness to persevere whilst under pressure to possibly compromise. In a competitive manufacturing environment, we should not forget that in addition to minimising risks to as low as reasonably practical, profit and safety are inextricably linked.

What is essential for application will be an amount of pragmatism to be applied by using an experienced organisation to get the fundamentals right and not necessarily blind compliance so that clarity of purpose is not lost. This will be required so that an organisation will be able to ensure, a suitable equilibrium is achieved and that functional safety is not comprised; but the benefits are cost effective.

In some cases, this may require some significant re-evaluation of the current safety and asset integrity strategy within an Asset Owner organisation and the ever increasing internal burden to manage a means to deliver a robust and repeatable implementation programme for improvements to process safety, functional safety, product safety and competency.

Achieving this balance is an ever present dilemma which continues to challenge all stakeholders at all levels of the business. It therefore follows that Asset Owners and EPC's have an increasing desire to work with suppliers who can provide lifecycle safety assured solutions and in doing so deliver:-

- A means for meeting the regulatory and legal requirements
- Support in the ability to demonstrate an operational duty of care
- Facilitation of increased Stakeholder confidence
- Delivery of a 'fit for purpose' technology, solution and service support
- A demonstrable approach to managing functional safety assurance and safety lifecycle compliance

References

[1] IEC 61508: "Functional safety of E/E/PE safety-related systems, Edition 2", (2010-02)

[2] IEC 61511: "Functional safety – safety instrumented systems for the process industry sector. Edition 1", (2003-01)

[3] ISA 84 Functional Safety: "Safety Instrumented Systems for the Process Industry Sector". (ANSI/ISA-84.00.01-2004)

[4] TüV Rheinland: "Functional Safety Certified Technical Training"

[5] TüV Rheinland and TüV Sud: "Global Functional Safety Management Certification Programme"

[6] ABB Safety Lead Competency Centre UK: "Accredited TüV Certified Functional Safety Management System for the Design & Engineering of SIS"