Assuring your Safety Instrumented Systems as part of your Process Safety Management requirements

Stuart R Nunns & John Walkington
ABB

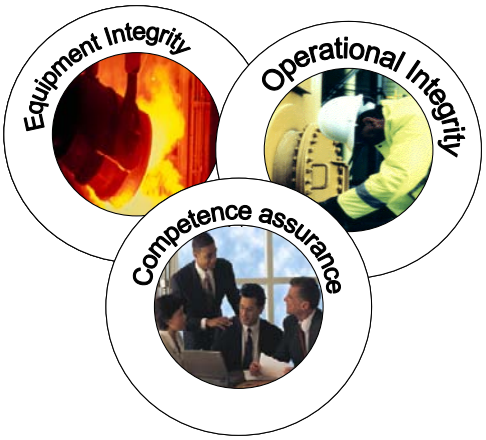
1. The need for additional safety assurance

Recent high profile incidents and accidents have highlighted the need to ensure more than ever that installed layers of protection on hazardous installations meet required reliability and safety integrity requirements. As operators improve their basis of safety as part of their process safety management obligations, there is an ever increasing need to develop assured methodologies that can link the hazard analysis with the confident development of credible layers of protection and in particular, embracing safety instrumented systems.

The key aspects to be addressed relate to corporate responsibility centred on company reputation and duty of care to shareholders, colleagues and the public. Fundamental in this process is the development of a culture that encourages safe working practices and senior management commitment.

Fundamentally, this commitment should ensure that an adequate *basis of safety* is derived for all 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 as integrated in figure 1 below.

Figure 1 – Key elements for developing an operational basis of safety

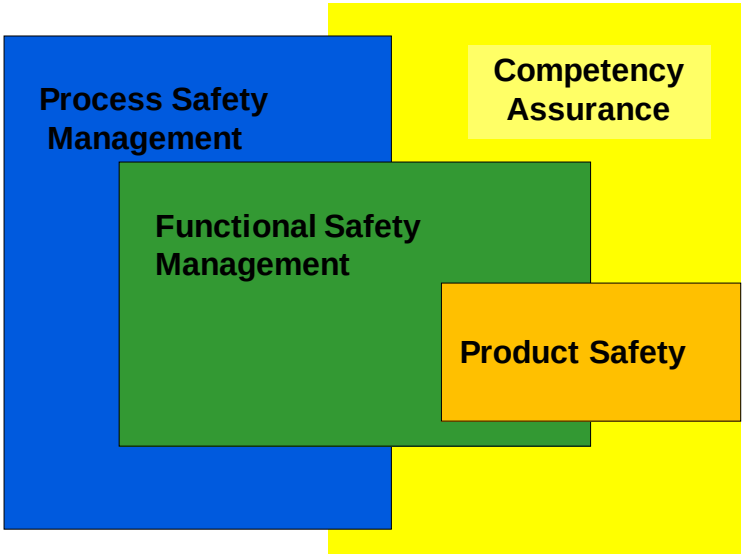


2. The key concepts to managing safety

There are a number of closely coupled attributes that collectively enable the Process Industries, faced with ever increasing demands, to demonstrate that their operating risks to people, the environment and the workplace are minimised to acceptable levels.

Taking occupational health and safety to one side, these attributes and linkages are highlighted in Figure 2 below,

Figure 2 - The key attributes of Safety Management



Each key attribute is described further below:-

Process Safety Management

- A key End User requirement
- Responsibilities and duty of care
- Safe manufacturing
- Compliance with regulation

Functional Safety Management

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

Product safety

- Fit for purpose
- Performance guarantees

Competency assurance

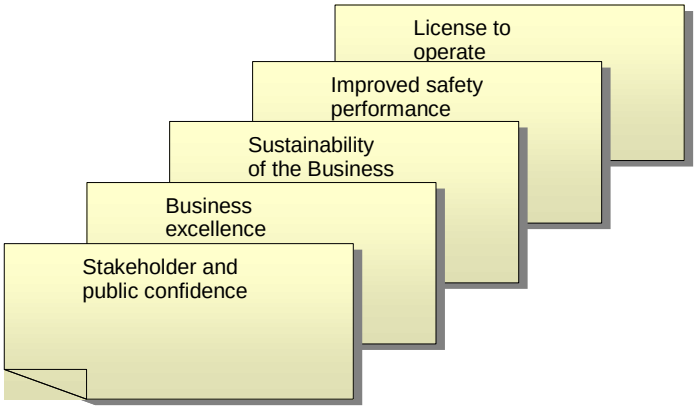
- People and organisations - knowledge, experience, training and qualifications

To achieve these requirements operator's must:-

- Design and build plants to appropriate technical standards and good practices
- Operate and maintain plants using appropriate safety and quality management systems
- Use competent delivery resources throughout both the project, asset and operational lifecycle of the equipment in use
- Use technology that is fit for purpose

Achieving these requirements will provide a World Class delivery model as indicted in figure 3 below,

Figure 3 – World class delivery model.



including all necessary regulatory approvals which ultimately manifest into a licence / permission to operate.

The focus for delivery of all of the above is through the company's safety management systems. Such 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.

In developing a basis of safe operation, operator's need to have systems and procedures in place that can address the needs of process safety management, functional safety management, product safety and competency assurance.

All four attributes identified in Figure 2 above are required to interface and function seamlessly with the objective of reducing the operating risk to a minimum, or 'As Low as Reasonably Practicable' (ALARP). The emphasis here being that all four attributes operate as an integrated set and need to be managed together otherwise weaknesses in overall compliance will be revealed over time. Treating these in total isolation or in a fragmented manner will not work, or more importantly deliver satisfactory and consistent results.

3. Supply-chain essentials

In most end user organisations today, 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. A recent project within which the authors participated, involved a consortium of end users, regulatory bodies, EPC's, third-party auditors and functional safety assessors, engineering and design organisations, accredited certification bodies, independent consultants, etc.

In addition, many end users have difficulty in fully understanding the requirements of the functional safety standards themselves and experience difficulties in a number of areas such as:

- A lack of clarification of safety requirements
- A too conservative or inadequate development of the basis of safety
- Overspend in unnecessary equipment
- Defining and implanting cost effective Proof testing regimes
- Project management and safety assessment and auditing
- Assessment of suppliers capabilities and competencies
- Meeting regulatory compliance and demonstrating due diligence
- Providing an auditable, documented and comprehensive audit trail

Therefore what is attractive for end users in this demanding environment is working with a supplier who can help address the issues above and can offer *leading edge* safety related products and certified competencies as a lifecycle approach and can provide additional assured confidence when developing their basis of safe operation.

In doing so, end user operators should seriously consider the selection of a supplier that has unparalleled experience and expertise in assisting companies with addressing the whole safety lifecycle and in particular the key areas of:

- **Process Safety Management**
  - Responsibilities and 'duty of care'
  - Safe manufacturing
  - Compliance with regulations
  - Sustainable operations

- **Functional Safety Management**
  - Application of appropriate safety related technologies
  - Third-party accredited and certified methodologies, procedures and systems
  - Compliance with standards / good practice
  - Compliance with the overall safety lifecycle

- **Product safety**
  - Third-party accredited and certified SIL capable products
  - Performance guarantees

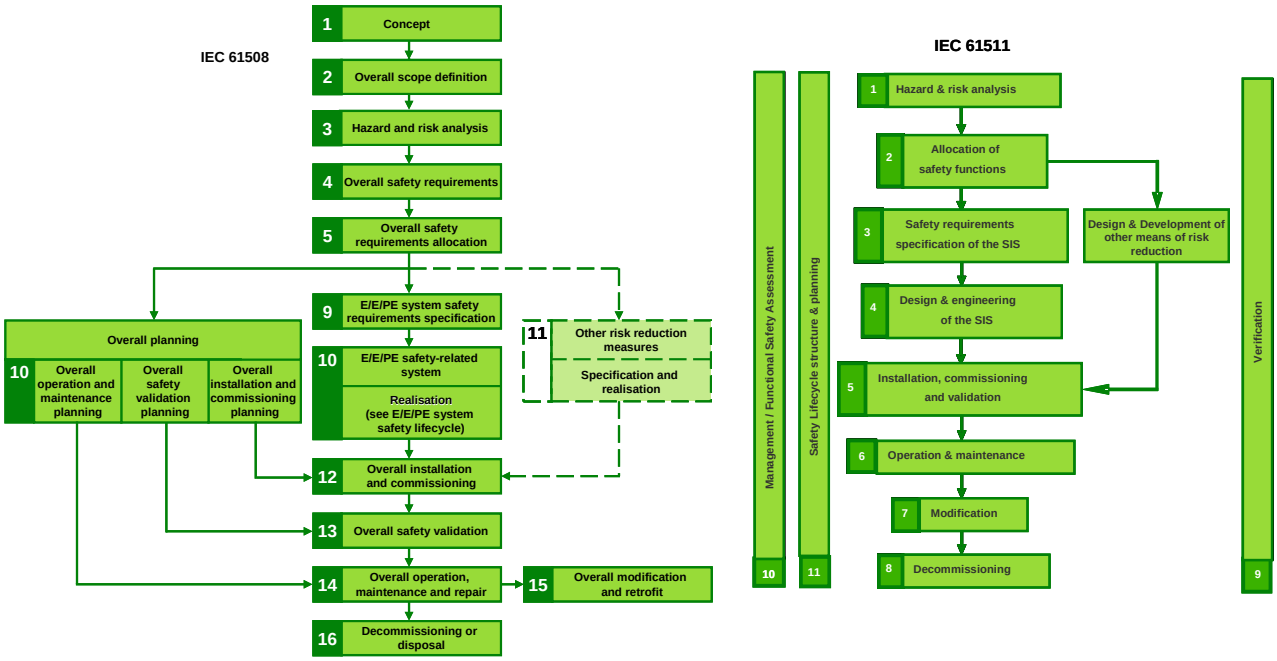
- **Competency assurance**
  - People - knowledge, experience, training and qualifications
  - Recognised third-party certified competency schemes

The result is one that bridges the often difficult requirement to align all the management, key assumptions, tangible deliverables and essential documentation needs into a structured and cohesive basis of safety.

Whilst the End Users / operators are the ultimate duty holders, the above requirements 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 safety-instrumented systems and system integrators whilst process safety aligns more closely with the operators of hazardous installations.

This requires end users to drive the requirements down through their supply chains, define and implement a consistent safety/asset life cycle model and for all organisations to take responsibility for their role within this safety life cycle. In order to achieve this Industry today is implementing the safety lifecycle models within IEC61508 [1] and IEC61511 [2] (Figure 4 below) to align the above requirements in terms of structure and deliverables as a means to demonstrating overall safety improvement. The challenge for the operators in respect of how they discharge their responsibilities to their supply chain, is how the four key elements of process safety management, functional safety management, product safety and competency can be brought together to increase confidence and ultimately assurance that the developed basis of safe operation is valid and appropriate.

Figure 4 – IEC 61508 Ed 2 & 61511 Functional Safety Lifecycle



Further refinement of the four fundamental attributes of safety management leads to a set of underpinning essential criteria that are required to be analysed, addressed and delivered. The authors have identified these based on their significant experience within the process industries.

Addressing these requirements is not an insignificant task; indeed it is very challenging and time consuming for those involved and often misaligned with the needs of day to day plant operating pressures. With regard to each of the attributes the key underpinning processes and deliverables to be considered include:-

Process Safety Management

Process plant operators/ owners: -

- Identification of the potential hazards i.e. The ABB Process Hazard Review Methodology (PHR)
- Quantification of the risk posed by the hazards

- Demonstration that the risk has been reduced As Low As Reasonably Practicable
- Capable of using appropriate methods for assessing the risk reduction needed including Risk Graph, Layer of Protection & Fault Tree Analysis, i.e. The ABB 'TRAC' SIL determination software tool
- Appropriate and suitable identification, specification and installation of protective measures
    - Design and engineering of safety instrumented systems
    - Design and engineering of pressure relief i.e. The ABB PSHEG 8 Design Standard for Pressure Relief
    - Design and engineering of other required technologies i.e. fire walls, bunding, etc.
- Provision of evidence supporting the basis of safety
- Defined strategy and implementation programme to operate, maintain and modify

Functional Safety Management

Providers of an engineered instrumented safety system and 'Other' technology solutions as part of your basis of safety:

- Ensuring compliance to good practice standards i.e, IEC 61511
- Using certified:-
    - Safety products
        - For example the ABB 800xAHi, SafeGuard, PlantGuard safety systems
        - Field Instruments
        - Final elements
    - Engineers
    - Organisations
- Mapping the appropriate phases of the IEC 61508-61511 safety lifecycle to the scope of supply

Product Safety

Suppliers of safety-instrumented products

- Implementing certified processes for the design and engineering of safety products – preferably Third party SIL capable
- Providing certified product performance – Third party SIL capable
- Continual investment in next generation, best practices, meeting market requirements and existing installed base
- Providing after sales support and sustainability of the installed base

Competency Assurance

In respect of suppliers:-

- Demonstrating long term commitment to the global safety market
- Providing significant investment and development of people for global delivery
- Ensuring staff have adequate and appropriate:
    - Training
    - Experience
    - Knowledge
    - Qualifications
- Actively involved in industry focus groups and standards
- Having processes and procedures to manage and deliver succession planning
- Ensuring continued professional development of all staff

It should be noted that during project execution, the end users / operators need to ensure they have visibility and control over the whole SIS safety lifecycle. For example the plan and programme for functional safety assessments.

There are advantages provided by compliance and the potential to improve efficiency in SIS implementation when having a repeatable process that leads to compliant safety instrumented systems. For instance, during execution of a phase such as "safety requirements specification of the SIS" (see phase 3 of IEC 61511 in Figure 1) the safety requirements specification document would be available as a template whereby the safety instrumented functions would be described according to inputs from the previous phase (e.g. phase 2, Allocation of Safety Functions).

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 that deploy and operate many safety instrumented systems 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 protections need to be engineered, operated and maintained according to functional safety requirements.

- Safety protections need to be validated after construction to ensure that they meet risk reduction requirements

- Operation and maintenance of safety protections, including proof testing regimes, need to ensure that safety integrity is maintained

A FSMS can provide some of the detailed definitions needed to achieve and maintain safety integrity of instrumented functions and there is increasing evidence that process operators are implementing functional safety as part of an overall safety management scheme. Some of these cases have been observed among the chemical and oil & gas companies that have a track record of compliance and adherence to functional safety standards. Some of the initial results indicate that the FSMS and SIS implemented are considered defendable under stakeholder scrutiny and that such 'best practices' are being planned to be used in other sites.

So having discussed the key issues above, the real challenge for the end user / operators is how they discharge their responsibilities both internally and with their supply chains i.e. Engineering Procurement Contractors (EPC's), and how the four key elements above can be brought together to increase confidence and ultimately increased assurance that the developed basis of safe operation is valid and appropriate.

It follows that end users/operators and EPC's, are therefore seeking supply-chain partners that can provide seamless process safety consultancy, technical design & delivery coupled with operations and maintenance support for their safety and asset lifecycle requirements.

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

4. So what has to be done?

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

1. Hazard & Risk Management

- Development of Process Safety Management Systems
- Behavioural Safety & Culture
- Process Hazard Review (PHR)
- Hazard Studies (including HAZOP 1-6)
- Mechanical Integrity Assessment and Asset Life
- SIL Determination
- Computer Hazard & Operability Studies (CHazop)
- Hazardous Area Risk Assessment and Classification
- Environment Impact Assessment
- Risk Modelling
- Occupied Buildings Risk Assessment

2. Design & Engineering

- Pressure Relief Design & Calculations
- Civil & Structural Systems i.e. Bunding and containment
- Safety Instrumented System Delivery (ESD, Alarms and Fire & Gas)
    - SIL Achievement
    - SIS Specification
    - Detailed Design and Engineering- SIL 3 Capable
    - Competency Assured TuV Certified FS Engineers
    - TuV 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
- Commissioning
- Validation

3. 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
- Testing and Repairs
- Operating and Maintenance Procedures

4. 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 Health Check
- Safe Systems of Work
- Management of Change Auditing
- Mechanical Integrity Auditing
- Incident Investigation Support

5. The ABB approach

For ABB, compliance is not only about minimizing liabilities for both the company and its clients, but it is also about leading by example and achieving engineering efficiencies through company-wide common practices and procedures. When it comes to focusing on the area of safety systems, like many other automation technologies, they are undergoing a revolution. Instrumented process protection relies increasingly on networked "smart" equipment, integrated control and safety systems, reprogrammable components and subsystems with automated configuration tools that are supported by comprehensive process safety management processes.

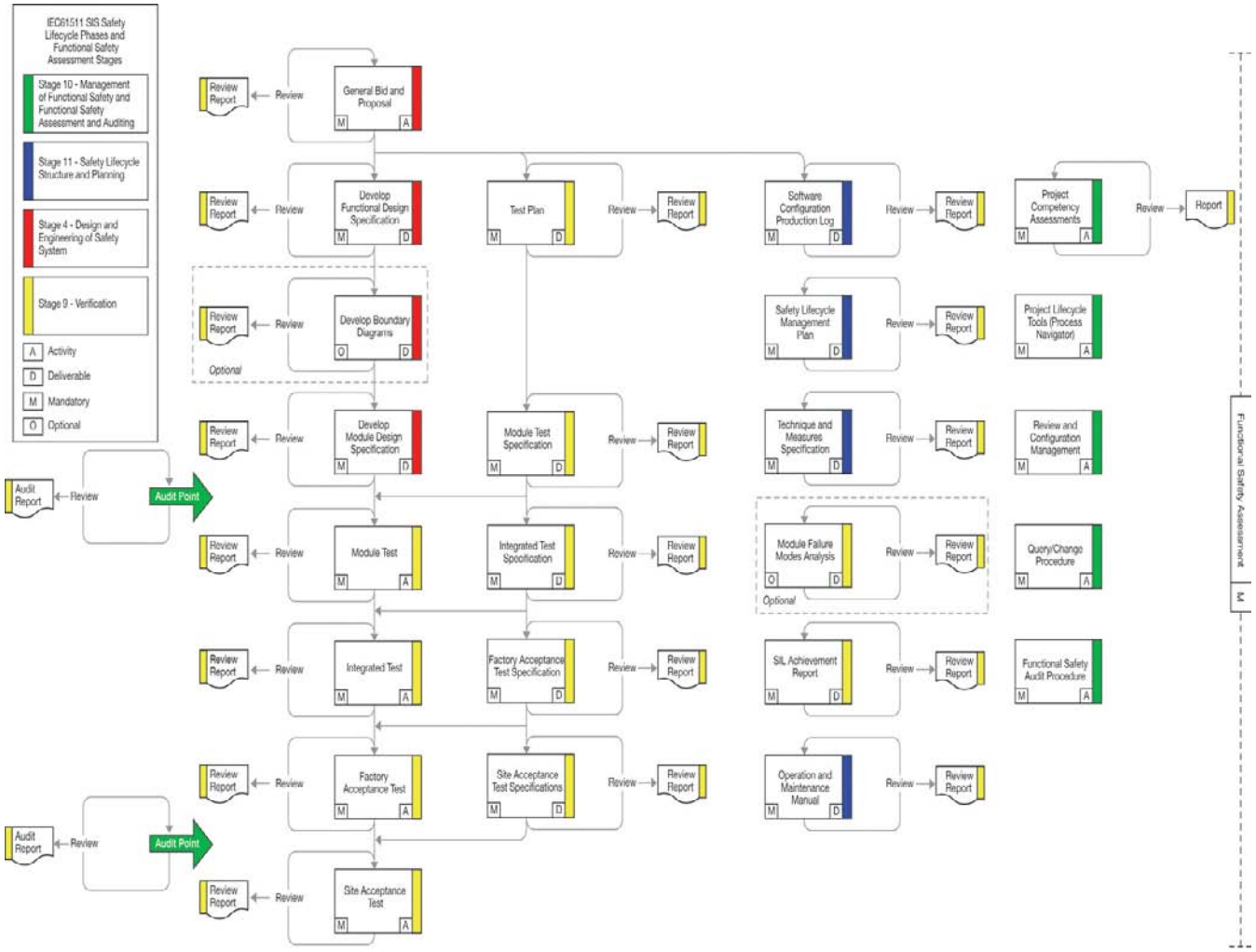
Invariably the basis of safety will identify the need for SIS. The application of such technology offers significant economic and safety benefits to end users and operators of hazardous processes. However, to exploit this potential the technology must be applied in a compliant and competent manner and this means the adoption of Industry best 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 many major clients are specifying them as a functional safety benchmark and a contractual requirement.

To underpin this benefit, ABB has embarked on a global program to achieve third-party accredited certification through TUV Rheinland in accordance with the Management of Functional Safety requirements of IEC 61508 and IEC 61511 for 20 of its Safety Execution Centres (SEC's) around the globe.

These SEC's:

- Design, engineer, Integrate and configure safety instrumented systems implementing a safety lifecycle model (see figure 5 below) using wherever possible subsystems and elements which are themselves third-party certified to meet all the relevant requirements of IEC 61508-61511.

Figure 5 – Safety Lifecycle model for design and engineering a SIS



- Provide full-service support for the client installed base of safety instrumented systems
- Provide functional and process safety consultancy
- Deploy staff who can demonstrate competency through experience, knowledge, training and qualifications. This is underpinned by:
  - Adoption of the guidelines "Competency Criteria for Safety-related System Practitioners" [3];
  - Achievement of TUV Rheinland Functional Safety *Engineer* and *Expert* Status for key professional engineering staff.

The benefits of certification are:

- Limiting exposure to potential liabilities
- Demonstrating due diligence
- Establishing an efficient, repeatable functional safety management system (procedures, techniques, tools, etc.)
- Reducing unnecessary pre-contract discussions (a benefit to both ABB and client)
- Cost-effective proposals
- Reducing requirements for bespoke project safety procedures
- Streamlining ABB – client supply chain relationships and implementation models
- Gaining a competitive edge for both ABB and their clients

- Being seen as best-in-class

In addition, recognising the importance of competency as an integral part of this functional safety management system, ABB has developed and rolled-out to all its SEC's a competency framework for functional safety assessors drawing on *good practice* competency guidance by way of the IET [3], IET/BCS [4], HSE [5] and the CASS Scheme [6]

6. So what are the perceived benefits from an increased safety assured solution?

By harnessing the use of a supplier such as ABB that can provide a seamless safety assured solution and in doing so provide all the necessary deliverables as outlined previously, an operator is better able to demonstrate that their PSM 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 end user operators and the project EPC's would be as follows:-

- **End users**
  - Assured 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 (PSM) sustained

- **EPC's**
  - 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

7. Conclusions

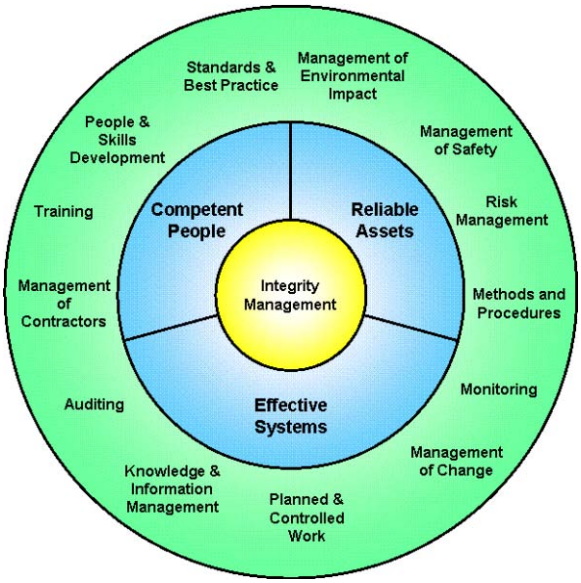
Whether embarking on delivering a new (Greenfield) project, or for managing your existing (Brownfield) asset, for increased safety assurance, the requirement to ever improve process and functional safety management techniques and competencies should be paramount within any responsible organisation.

It therefore follows that end users and EPC's have an increasing desire to work with suppliers that can provide lifecycle safety assured solutions and in doing so deliver:-

- A means to meeting your regulatory and legal requirements
- Support in your ability to demonstrate duty of care
- Facilitation of increased Stakeholder confidence
- Delivery of a 'Fit for purpose' Technology, Solution and Service Support

In some cases, this may require some significant re-evaluation of the current safety and asset integrity strategy within an end user / operator organisation and the ever increasing internal burden to manage a means to deliver a robust and repeatable implementation programme, as shown in figure 6 below, for improvements to process safety, functional safety, product safety and competency.

Figure 6 – Integrated safety and asset integrity



To do this requires senior management commitment and a willingness to persevere whilst under pressure to possibly compromise. One should not forget that in addition to minimising risks to as low as reasonably practical, profit and safety are inextricably linked. Achieving this balance is an ever present dilemma which continues to challenge all stakeholders at all levels of the business.

This paper has highlighted a number of key attributes which need to be addressed and their supporting criteria to enable end user / operators and the supply chain to take full benefit of best in class safety assured solutions.

References:

1. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems
2. IEC 61511Functional safety – Safety instrumented systems for the process industry sector
3. IET Competence criteria for safety-related system practitioners
4. IET/BCS Competency Framework for Independent Safety Assessors (ISAs)
5. UK Health & Safety Executive - Managing competence for safety-related systems
6. The CASS Assessor Competency Scheme