Lessons Learnt from FSA

<u>Abstract</u>

The drive for technical education in functional safety has been very successful. More than 8,000 people have achieved ‘Functional Safety Engineer’ certification.

Over the past 10 to 15 years the level of understanding of functional safety engineering amongst users has improved steadily.

Independent audits and assessments of safety instrumented systems in process sector applications reveal that the most common problems are now systematic in nature rather than technical. They are not in engineering but in management, organisation and responsibilities.

Better training and competency management is needed for the managers and leaders who ultimately hold responsibility for risk management in hazardous facilities.

Outline

Functional safety assessments and audits

Over the past 10 years a team of 6 assessors at I&E Systems has carried out 28 assessments and/or audits of functional safety across a wide variety of industries, mostly in the process sector. The applications have included:

- Offshore oil and gas production
- Onshore oil and gas production (including LNG)
- Gas fired calcination for alumina processing
- Coal fired boilers for power generation
- Sodium cyanide production
- Titanium chloride production
- Nickel smelting furnace control
- High speed railways

This paper presents lessons learnt that are common to all of these audits and assessments.

We have usually been engaged by end-users concerned about the work carried out by design and installation contractors and by system suppliers.

The audits and assessments that we carry out are always limited in scope. I&E Systems' expertise is limited to the safety systems engineering. We are not experts in process engineering or in risk and reliability engineering.

Our expertise includes the application of SIS hardware but does not include the design of individual hardware components. We do not carry out assessments of SIS logic solver hardware, sensors or final elements.

Global Issues

The projects that we have reviewed have included participants from around the globe, though predominantly in Australia and SE Asia:

- Australia
- New Zealand
- Singapore
- Malaysia
- Japan
- Taiwan
- Korea
- USA
- Saudi Arabia

Compliance to the standards is improving steadily but we find the same problems occurring again and again in every assessment.

Most functional safety projects are excellent – but only in parts.

Bishop: "*I'm afraid you've got a bad egg, Mr Jones*";
Curate: "*Oh, no, my Lord, I assure you that parts of it are excellent!*"

"True Humility" by George du Maurier, originally published in Punch, 1895

The level of technical understanding is now generally very good. It is in **functional safety management** that we find widespread and common problems.

What is FSA?

Functional safety audits and assessments are essential to provide feedback to management.

There is a lot of confusion about functional safety audit and assessment. Most people find it difficult to understand these processes. They are not sure who is responsible for them and why they are important.

Audits are not assessments

The standards IEC 61508 and IEC 61511 require that both functional safety audits and assessments are carried out. It is easy to confuse audit and assessment but they are distinctly different.

The purpose of a **functional safety audit** is to provide feedback to management about whether the ***procedures*** for functional safety are working well in practice.

A **functional safety assessment** is an investigation with the specific objective of making a judgement as to the functional safety and safety integrity achieved by the ***safety instrumented system*** as a whole. Assessment includes making judgement on technical issues as well as on procedural issues.

To put it simply, functional safety assessment demonstrates to management that the safety instrumented system will achieve the risk reduction that is required from it.

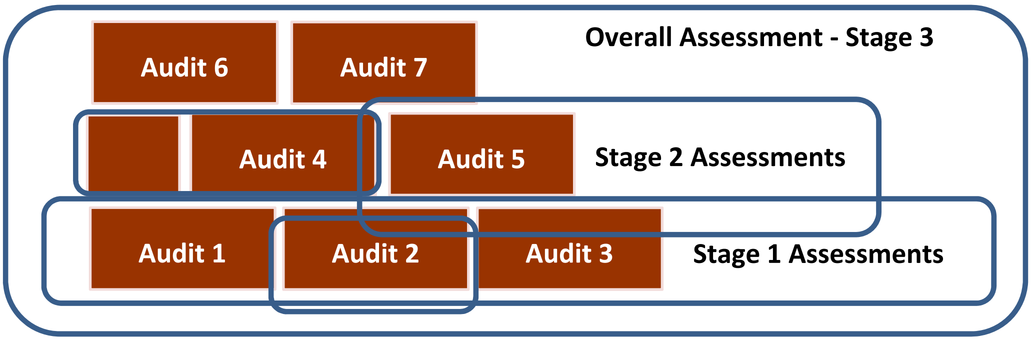
Assessment relies on audit

Functional safety assessments rely on evidence. The best way to obtain that evidence is usually through functional safety audits.

Audits are always limited in scope. The assessment process is built from a succession of audits and/or partial assessments – much like a wall is built from bricks.

A wall is much more than just a pile of individual bricks.

An assessment is much more than a series of audits.



Who is responsible for FSA?

End users often assume that suppliers or contractors are responsible for functional safety audit and assessment.

The scope of each supplier and contractor is limited. They can usually only audit what is within their scope. If they carry out a functional safety assessment it will be a limited, partial assessment.

Ultimately an overall assessment of functional safety needs to be made before hazards are introduced and before the equipment is handed over for operation.

That final assessment must consider operational readiness. It must examine the end-users planning for operation and maintenance of the SIS.

The end-user or owner of the plant always has overall responsibility for safety and must take responsibility for the overall functional safety assessment.

What we are asked to look for

Too little

End-users often expect audits and assessments to be more limited than they should be.

On several occasions end-users commissioned us to conduct audits because they lacked confidence in safety instrumented system software.

The users noted that the software had exhibited ‘unexpected behaviour’ and asked us to investigate whether ‘the software had been written correctly’. In each case the more pertinent question was whether ‘the correct software had been written’.

In all of these cases it turned out that the requirements specifications were incomplete or even completely missing. Without formal requirements specifications there is no chance that the software will do what is actually required.

The real problems are very rarely in the way the software has been written. They are invariably in the way the project has been managed.

Audits and assessments should not be limited to looking at work by contractors and suppliers. They also need to consider the end-user's organisation.

http://www.independentaudit.com/external-audit-boundary/

Too much focus on details

End-users are often concerned about whether the probability of failure calculations are 'correct' – with 3 significant figures of precision!

There is too much focus on relatively simple arithmetic without questioning the validity of the data and assumptions.

Too late

Too often the functional safety audits and assessments are not planned in advance.

A few weeks before handover we are asked to conduct an urgent assessment. There is not enough time to conduct a thorough assessment. There is no time to address the issues that are found.

Some reasons for late assessments are:

- Stage 1 and stage 2 assessments are skipped to save time and money. As a result fundamental mistakes in planning and requirements are not revealed until after the plant has been built.
- The end-user assumes that the suppliers and contractors will have carried out assessments
- The suppliers and contractors assume that the end-user will be responsible for assessments.

What we need to look for

There are 3 basic elements that we need to achieve functional safety:

- A management **Framework**: Effective planning and management
- A solid **Foundation**: Complete and clear safety requirements specification
- **Follow-through**: Traceability of the design, implementation and operation back to the requirements and to the planning.

The purpose is to provide **Feedback** to management.

Management Framework

Functional safety starts with management, it is fundamental.

More than 95% of major accident events are caused by multiple systematic failures.

Systematic failures have definite causes. Systematic failures are usually the result of human failings in specification, design, manufacture, software, installation, testing, operation or maintenance.

Systematic failures invariably occur due to a lack of planning, organisation and management.

The first priority in assessment must be to examine the management processes.

Success in management relies on making sure that everybody involved with the safety instrumented system knows what is expected of them, and making sure they have the necessary information, tools, resources and competencies.

Both IEC 61511 (sections 5, 6 and 7) and IEC 61508 (sections 6, 7 and 8) give similar requirements for management planning.

The management plan should clearly define all of the activities needed to achieve success and should define the records that are to be kept. It should define the 'why, who, how, where, when and what'.

Requirements – Foundation

The hazard and risk analysis sets the basic ***functional*** requirements and ***performance*** requirements for the safety instrumented system.

IEC 61508 and IEC 61511 stipulate many detailed requirements that need to be considered.

In practice it is often difficult to prepare the requirements specification because the end-user and the design engineers do not understand all of the issues that need to be considered. The system suppliers understand the issues but cannot prepare the requirements because they do not know what the end-user needs.

The requirements specification essentially belongs to the end-user but in practice it has to be prepared in collaboration with the designers and suppliers.

Traceability – Follow-through

The whole point of preparing clear and complete specifications is to ensure that system will function and perform as required when it is put into service.

The standards require traceability, which means that evidence is needed to show that all of the requirements are actually implemented in the system when it is built and that all of the features are actually as required.

The designers and builders need to keep records that demonstrate traceability. These records will contribute towards the 'validation' process, proving that all of the requirements are fulfilled.

What we usually find

What we usually find is that a lot of attention is given to getting the low level technical details right, but not enough attention is paid to the 3 fundamental elements: Framework, foundation and follow-through.

Policy

Most companies set clear expectations with corporate policies but it is sometimes difficult to see how the policies are implemented in practice. The relationship between the policies and the functional safety systems needs to be clearly stated and understood.

Some operating companies experience a conflict between safety and production. If the safety policies are not clearly stated and communicated then employees may believe that it is acceptable to compromise safety.

Strategy

Functional safety is one of the strategic elements used to achieve safety goals.

Functional safety cannot exist in isolation. Safety instrumented systems need to be considered as an integral part of the overall risk management framework.

Safety instrumented systems need to be given appropriate attention and resourcing by senior management.

Our conclusions from many assessments show that managers responsible for operation of hazardous facilities often do not have a good understanding of functional safety management. They usually do not have a background in risk engineering or in instrumentation and control.

Company managers need better training and development to be able to understand and manage functional safety more effectively.

Safety management systems

Functional safety brings together risk management and quality management. Many of the requirements that need to be covered in functional safety management planning should have already been covered in corporate standards, project execution plans, quality plans, safety plans, risk plans, maintenance plans or technical integrity plans.

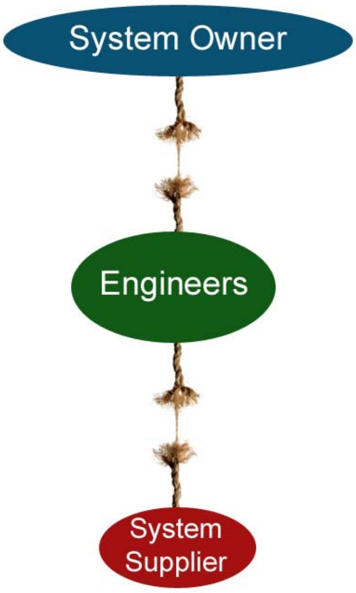
On large projects we often find that there are several overlapping plans that relate to functional safety management. The various plans are not cross referenced effectively. It is hard for people working on functional safety to know which plans and procedures are relevant.

EPCM (Engineering, Procurement and Construction Management) contractors have well established quality management systems. These systems include appropriate processes for controlling design basis, for checking and correction of deliverables, and for controlling changes to the design.

Many EPCM contractors routinely prepare functional safety management plans, but often the plans do not make any reference to quality procedures. The need to retain quality records is overlooked and not understood. Design engineers do not make the connection between functional safety, basic quality management and record keeping.

Quality procedures are mandatory for achieving systematic integrity in functional safety. Functional safety management planning should clearly define quality requirements.

Responsibility boundaries



On major projects responsibility for functional safety is inevitably divided across major contract package boundaries.

The need to manage technical risk and process risk is balanced against the need to manage project risk and commercial risk.

Contract styles that reduce commercial risk tend to prevent control, interface and integration of technical safety.

Authority levels are often not clearly defined. We have seen many instances where authority levels have been assumed without formal definition and agreement. On one project the EPCM contractor assumed responsibility for the safety requirements specification and then approved changes to it without any reference to the end-user.

Most system suppliers have effective procedures that include a ‘requirements qualification’ milestone. In practice it is difficult for system suppliers to challenge incomplete or inconsistent requirements.

Geographic and cultural barriers

The contractual boundaries are often made worse by geographic separation and by cultural differences.

Software engineers working in ‘low cost’ engineering centres such as Kolkata, Dhaka, Kuala Lumpur and Shanghai are less likely to question the quality of the design basis or requirements documents that they are given.

Responsibility for requirements

Though we may find issues with *how* work is done by the system suppliers; the most significant issues result from *what* they are asked to do.

Problems in software usually stem from inconsistent and incomplete requirements.

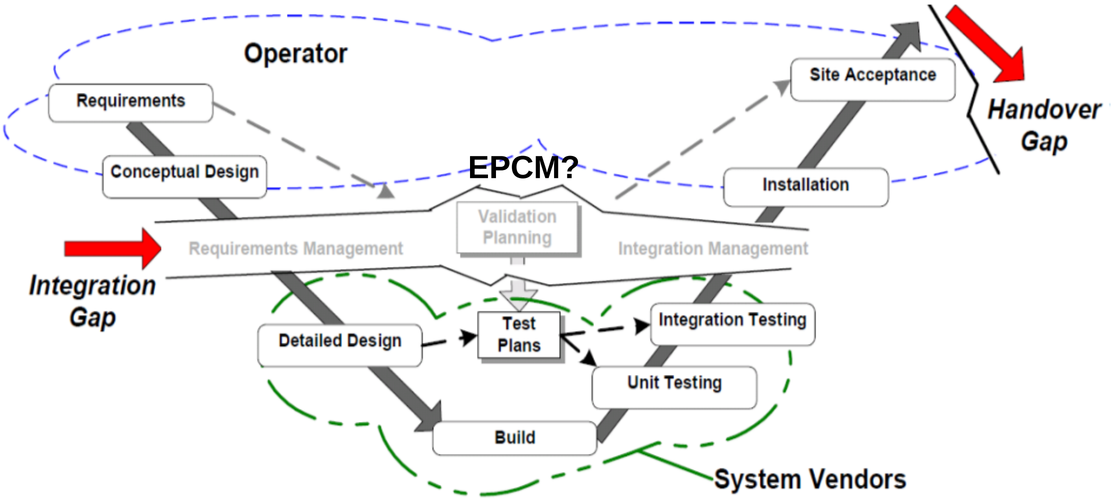
The end-user is ultimately responsible for the requirements even though preparation of the requirements may be delegated to the engineering design contractor.

Integration gaps

Intuitively people think of the safety instrumented system logic solver supplier as having the primary responsibility for functional safety.

The logic solver represents less than one third of each safety function. Most of the hardware failures in safety functions are related to the final elements and the sensors. Design of the sensor and final element sub-systems is usually the responsibility of the engineering design contractor.

Engineering design contractors seem to be reluctant to take on responsibility for integration of the logic solver systems into a complete integrated system.



Responsibility for the integration of each safety function as a whole must be clearly defined and understood.

The other common gap in responsibility occurs at handover.

The responsibility for ensuring operational readiness must be clearly defined. This includes planning, procedures and training. The end-user will need assistance from the design contractors and system suppliers in preparing test plans, procedures and training.

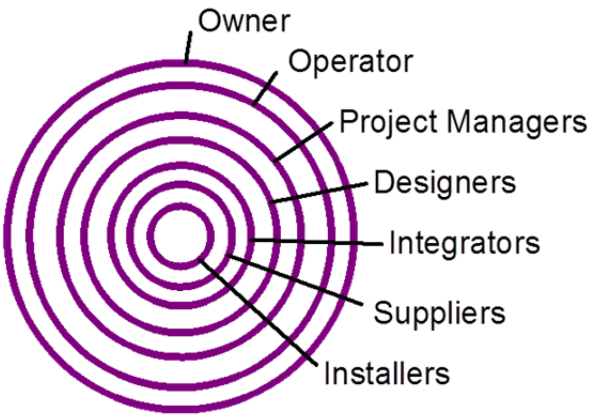
Integrated planning

It is normal for Project Execution Plans (PEP) to be 'nested'. Each contractor and supplier has a PEP that relates to the work in their scope.

The owner or overall project manager should have an overall PEP that ties together and integrates the individual PEPs.

A similar approach must be taken for functional safety.

It is essential to coordinate the individual FSM plans so that the interfaces and boundaries are understood, controlled and managed.



Competence

The standards require a systematic approach to managing competence. The basic steps required are:

- Identify the skills and knowledge required for each activity
- Define the level of competency required
- Assess the competency of the resources (people and organisations)
- Address the shortfalls with supervision, training and development, or with additional resources

We have found that all of the logic solver system suppliers have established some sort of formal system for managing competence in accordance with the standards.

None of the end-users and none of the EPCM or design contractors that we have assessed have yet demonstrated any systematic approach to managing competence.

An excellent set of guidelines has been available since 1999 from the Institution of Engineering and Technology (IET) in conjunction with the Health and Safety Executive, UK and the British Computer Society.

Refer to < http://www.theiet.org/factfiles/msc/ > for further information.

These guidelines can be applied by owners and operators as well as designers, developers and suppliers.

Safety Lifecycle Dossier

Early in the planning process the safety lifecycle is defined in terms of inputs and outputs.

The logic solver system suppliers that we have assessed have always clearly defined the inputs and outputs in detail and assigned unique reference numbers to each item. They have also defined the verification records to be produced.

The EPCM and design contractors by contrast have not made the connection between the safety lifecycle and document planning. The EPCMs' safety lifecycle plans describe the inputs and outputs only in generic terms. The plans do not specifically identify individual documents. EPCMs produce large databases of documents without any clear reference to the functional safety lifecycle. It has always been difficult to find the documents that we need for audit because they are hidden amongst a large number of non-safety documents.

When we request functional safety documents at the beginning of each audit the EPCM engineers struggle to understand which documents will be relevant.

The standards give clear guidelines on what information must be kept. Refer to IEC 61511-1 section 19.2.9 or to IEC 61508-1 section 5. This information should be identified and tracked throughout the lifecycle of a safety instrumented system.

Defining a set of safety lifecycle deliverables at the start of a project is a good way of giving project team members a clear understanding of what they are expected to deliver in the end.

These deliverables will make up the functional safety documentation 'dossier' (or database) which is handed over to the end-user when the system is placed into service. The information will have to be maintained and regularly updated by the operations and maintenance team throughout the life of the plant.

Techniques and measures

Both IEC 61508 and IEC 61511 stipulate that techniques, measures and procedures must be planned deliberately in order to achieve systematic integrity.

Not even one of the many parties that we have audited has provided any evidence recording rationale for selection of techniques, measures and procedures.

The logic solver suppliers mostly apply appropriate techniques and measures because they have prepared corporate standards and procedures specifically for functional safety. However they do not review the ***'effectiveness'*** that is required according to the complexity of the work and the required SIL.

The level of care to be taken in SIL 3 functions must be something like 100 times more effective than for SIL 1 functions.

Risk Studies

The risk studies and SIL determination studies that we have assessed have been generally in compliance with the standards.

The risk targets have been reasonable. The SIL targets have been determined using a consensual approach by assessment teams that have had appropriate experience and expertise.

The most common concerns that we have found are:

- No consideration of the cumulative demand rate on common elements shared between safety functions
- No rationale recorded justifying the assumptions made
- Relying unquestioningly on software packages, assuming that the results are valid because the software is from a trustworthy supplier
- Taking credit for other protection layers that are not dependable or not valid
- Presenting results with too much precision, implying an accuracy in the calculations that is simply not credible (e.g. RRF = 973)
- The exclusion of entire units or categories from the SIL studies due to arguments regarding scope of work boundaries (for instance excluding all 'packaged equipment').

Requirements

Over the past 5 years we have seen a gradual and progressive improvement in the way that safety requirements are documented and coordinated.

It is now common practice for users to prepare a cross reference table based on IEC 61511-1 section 10.3.1, defining how and where requirements have been specified. Many companies have developed requirements specification templates that are comprehensive and useful.

The problems that still commonly occur in requirements specifications are:

- Traceability to the risk studies is not maintained
- Traceability of the requirements through into the design specifications is not managed
- Users find it difficult in practice to consolidate all of the requirements into a single safety requirements specification. Requirements are still distributed across many different documents and are not reconciled
- In practice the designers and developers only use a limited subset of the requirements specification documents, missing some of the requirements completely.

Some requirements are not specified simply because they are not understood.

For instance in almost all of the systems that we have assessed the requirement to identify and reduce common cause failures has not been considered adequately. It is not enough to specify the values of β-factor that are to be used in calculations. The factors that lead to common cause failures must be analysed. The techniques and measures to be applied to minimise common cause failures must be specified.

The 'process safe state' is usually not understood. Simply closing a valve does not necessarily make the process safe.

‘Process safety time’ is rarely defined. EPCM engineers specify response times based on what can be achieved rather than based on what is actually required to prevent a hazard from developing.

Design

The detailed design is generally well executed but there are several problem areas that always cause difficulty. Most projects fail to meet the standards in all of these areas:

- **Traceability**

The inputs for each output must be clearly identified (including the revision code). Inputs can be identified using a table within each document or in some sort of document register or traceability table.

Traceability must be used to ensure that every requirement is fulfilled in the design, included in the specifications and in the test procedures.

If a requirement is not included in the specifications it will not be implemented and it will not be tested.

- **Common cause failures**

Common cause failures should be systematically analysed and controlled.

Electromagnetic compatibility (EMC) should be based on EM risk assessments (refer to IEC 61000).

Cabling installation practice must be specified to avoid electromagnetic interference. The cabling installation specification is an essential document for functional safety.

Degraded failure modes (not just on/off failures) should be considered for electrical power supplies and air supplies. Response to high impedance faults and drooping voltage levels must be considered.

Environmental requirements and environmental tests should be specified. This may include factors such as temperature, humidity, vibration, solar or heat radiation, water ingress and corrosion.

Elements that are shared between safety functions (e.g. trip groups with shared final elements) or between protection layers must be considered and analysed.

- **Hardware fault tolerance**

It is always difficult to demonstrate compliance to hardware fault tolerance requirements. The hardware fault tolerance for SIL 3 functions is usually questionable.

Failure rate data cannot simply be taken from reference books without question.

Many commonly used references do not comply with IEC 61508 Ed. 2; undue credit is taken for ‘no effect’ failures when calculating Safe Failure Fraction. Most engineers have trouble understanding or accepting the fact that the dominant failure mode for shutdown valves is to jam in the open position, an unrevealed and dangerous failure.

Many certificates from seemingly reputable agencies contain information that is potentially misleading (such as confusion between ‘no-effect’ and ‘safe undetected’ failures).

Evidence for claims of ‘prior use’ is usually inadequate.

Engineers assume that all valves can be simply classified as Type A, ignoring the stringent requirements for quality and documentation that are necessary for classifying a device as Type A.

The confidence levels required for failure rate data (λ_{70}, λ_{90}, etc.) are not considered or are ignored because that information is not readily available.

Diagnostic coverage is confused with proof testing. Engineers do not understand that the diagnostic testing interval must be within the claimed mean time to restoration. Partial stroke testing is not usually frequent enough to be classed as a diagnostic function.

Verification and validation records

Audit (and therefore assessment) relies on objective evidence. Almost without exception the records that we have reviewed have been incomplete and inadequate.

Checks, inspections and tests have been incomplete or not properly recorded. Deficiencies found have been left unresolved.

The systematic integrity that is achieved depends on how thoroughly work is checked and on how carefully records are kept.

If no evidence is available to show how work has been checked there can be no confidence that it has been checked at all.

Functional safety management plans prepared by EPCMs show that many engineers and managers do not understand the terms ‘verification’, ‘validation’ and ‘assessment’.

Operations and maintenance readiness

End-users expect that functional safety assessments will focus on compliance by the project team and contractors.

A project typically takes 1 or 2 years to design and build but it might remain in operation for over 20 years.

It is essential that a Stage 3 FSA must examine the end-user’s preparations and planning for operations, maintenance and modifications.

The issues that we usually find with end-users include:

- Functional safety management planning is either informal or completely missing
- Training for operators and maintainers does not specifically address functional safety
- Competence needs to be managed more systematically
- Plant managers need to be competent in managing functional safety and providing leadership
- Configuration management is not well understood
- Performance management (analysis of failures and trips) needs better planning

Functional safety management should be included as an extension of the asset integrity maintenance plan.

Proof test and inspection planning

There is often a responsibility gap between the project team and the operations team with respect to proof test and inspection planning. Most ‘design and construct’ contract exclude preparation of proof test and inspection procedures.

Ideally the proof test and inspection planning is developed in close cooperation between the design team and the operations team.

The extent of the testing and inspection should be based on failure mode studies such as ‘FMEDA’.

There should be a close interaction between the design and the test and inspection plans.

The proof test intervals that are assumed in the design must be feasible and acceptable to the operations team.

The design must facilitate the testing and inspection. Provision must be made for access to test parameters. Examples include providing test points to enable seat leakage testing for valves or providing inspection points for sensor tubing.

The emphasis seems to be on ‘proof testing’ rather than on ‘inspection’. At least 95% of major accidents and incidents are caused by multiple systematic failures. Regular inspection to identify systematic problems is arguably much more important than testing.

Audit and assessment

Audits and assessments provide essential feedback to the management. Functional safety cannot be managed effectively without feedback.

Functional safety audits and assessments are generally not well planned.

Most logic solver suppliers have formal procedures for functional safety audits and assessments. To win the contract in competitive tendering suppliers will exclude audit and assessment unless they are specifically required by the contract specifications.

The EPCMs do not plan or carry out functional safety audits and do not understand that audits are necessary.

The end-users expect that contractors will take responsibility for audit and assessment.

Conclusions

Assessment scope

What we are asked to look for is too little and too late. Audits and assessments need to be better planned and coordinated to provide essential feedback to the management.

What we need to look for in functional safety assessment is:

- Framework
- Foundation
- Follow through

Planning and management

Systematic failures can only be controlled by applying an effective management framework.

Senior company managers provide direction, assign responsibilities and resources, and set priorities. Senior company managers need to understand their roles and responsibilities in achieving and maintaining functional safety.

Functional safety management must be considered together and coordinated with quality management and risk management. Functional safety achieves risk reduction as part of a wider corporate risk management framework. Functional safety cannot be achieved without quality management.

Responsibilities and authority levels must be clearly defined and understood.

Provisions for the integration of functional safety activities must be included in the contracts on major projects.

End-users need to be aware of the ‘integration gap’ and the ‘handover gap’. The gaps can be bridged through active management, planning and coordination.

Functional safety management planning is needed in the operations phase as well as in design and development.

Competence

End-users and EPCM or design contractors need to have a systematic approach to managing competence. A comprehensive set of guidelines is available.

In particular more attention is needed to ensure that managers and leaders are competent in providing direction and leadership.

Requirements

End-users and design contractors need to continue improving the way that safety requirements are documented.

Engineers need better training to understand some of the details that should be specified.

Traceability

Evidence must be produced and kept to show traceability of the design and implementation back to the safety requirements and to the planning.

The evidence to be kept should be clearly defined at the beginning of the project. Planning for evidence should be revisited and updated at the start of each new lifecycle phase.

Verification and validation evidence

Complete records of verification and validation must be kept. This includes:

- Records of review and checking of documents and software
- Inspection and test records for components and field installation
- Test reports with records of inspections and tests completed and including resolution of all discrepancies and issues raised.

Performance feedback

End-users need formal processes for evaluating the failure rates and demand rates in the operations phase.