The art of assessing functional safety through the supply chain

ABB's Stuart Nunns walks us through the principles behind Functional Safety Assessments, which are now mandatory for many organisations that aim to comply with the latest functional standards.

Functional safety cannot be achieved through a "tick-box" exercise. Got the right kit? Good for you, but that may not translate into functional safety. Used a reputable company to design and install your safety-critical systems? You're on the right track, but there's still no guarantee. Got your most competent people checking that everyone's following your agreed practices and procedures? You know where this is going…

Achieving optimal functional safety demands all this and more throughout the entire safety lifecycle, not only from the end users of safety-related systems but also back up through the supply chain.

In other words, the international functional safety standard (IEC61508) and the daughter standard for the process industries (IEC61511) are performance-based standards. They're not about having the right kit per se. Instead they're about achieving the right level of overall functional safety throughout the safety lifecycle, which includes specification, design, implementation and operation.

The safety lifecycle of equipment or other assets can span many years. It will involve different organisations and a variety of client-supplier contractual relationships that demand clearly specified responsibilities, activities and deliverables. It is therefore essential that all those organisations involved in implementing different phases of the safety lifecycle can demonstrate their competence and ability to work to the relevant standards.

Achieving the organisational capability needed to implement the requirements of IEC 61508 and IEC 61511 across the supply chain can be tricky. Each organisation must be fully conversant with the standards and clarify which clauses apply to its areas of responsibility. Many of today's regulatory authorities effectively require companies to show this level of familiarity with the standards when they are checking for good practice.

That's why the latest version of IEC 61508 has strengthened and clarified the mandatory requirements for Functional Safety Assessments (FSAs). They now require a clear definition on the scope and boundary of the functional safety assessment, e.g. safety-related system or compliant item (element/subsystems), the need to assess claims made by third-parties/suppliers and minimal requirements for the contents of functional safety assessment reports, including:

- a precise identification of the compliant item
- conditions assumed during the assessment
- clear and concise references to the evidence assessed
- procedures, method and tools used for assessing systematic capability and hardware safety integrity
- description and classification (e.g. acceptance, qualified acceptance and rejection) of deviations from relevant clauses of the standard

This is in addition to the traditional activities of verification, validation and functional safety audits.

Audit vs assessment

So what's the difference between an audit and an assessment in this context?

An audit is undertaken to ensure compliance with procedures and is an integral part of an effective quality management system and ISO 9000. Auditors don't need to make judgements on the adequacy of the work they are considering and make no specific judgements about whether functional safety and integrity has been achieved.

In contrast, an assessment is an investigation that involves assessors undertaking an evaluation and making a clear judgement about whether provisions are adequate for the achievement of functional safety and integrity. FSAs are beyond the normal scope of ISO 9000 and rely heavily on competent assessors using their judgement. So audit processes and findings play a role as an input in an FSA, but the broader scope of an assessment can span several organisations and drill down into specific technicalities.

Scope of supply

One of the first activities to be performed when developing an FSA methodology is to define the scope of supply for the organisation that wishes to implement FSAs. This scope of supply should be viewed in the context of those other organisations involved in the safety lifecycle and, in particular, those organisations implementing phase(s) immediately before and after. Which elements of the overall safety-related system are included in the scope of supply will vary significantly between different organisations.

At a basic level the overall safety-related system comprises three subsystems. The sensor or input subsystem includes the actual sensor(s) and components such as microprocessors, signal converters or IS barriers that lead to the logic subsystem. The logic subsystem begins where the incoming signals are first combined and includes any other components up to and including where the final signal(s) are presented to the final element subsystem. The final element or output subsystem comprises all the components and wiring that process the final signal(s) from the logic subsystem, including the final actuating element(s).

So, for example, the scope of supply for a typical systems integrator may be limited to the provision of the logic solver sub-system within the end-to-end safety-related system. In contrast, for an engineering procurement and construction (EPC) company, the scope typically includes the end-to-end safety-related system and all three subsystems.

Independence matters

Another key consideration is the level of independence required of the assessors performing the FSA. Unfortunately, the requirements regarding independence are significantly different in the two standards. The "parent" standard IEC 61508 has very clear requirements for independence and these vary based on the possible consequences of failure or the required safety integrity level (SIL). The acceptable possibilities also depend on the phase of the safety lifecycle under scrutiny. In contrast, the "daughter" standard for the process industries - IEC 61511 - proposes a more relaxed approach that doesn't consider the consequences or

SIL rating and is less rigid in terms of organisational or departmental independence. This makes it essential for any organisation developing its FSA methodology to decide upfront which standard they're looking to comply with.

This decision may also be influenced by which standard is being used to develop any wider functional safety management system (FSMS), as well as the specific requirements of any third-party accredited certification body if the participating organisation is hoping to get its FSMS certified. The organisational and management models operating within the company can also impact on the levels on independence between departments, making internal assessment more or less feasible. Finally, the availability – or lack – of competent resources in-house might be the determining factor.

Possible methodology

Once the scope of the FSA has been determined, the organisation will need an implementation strategy. An FSA will typically be needed for each safety system supplied, but unlike a safety audit or spot check, a proper assessment may involve work at several different stages within the safety lifecycle. For instance, a Preliminary FSA typically follows the completion of a Safety Lifecycle Management Plan and the Functional Design Specification (FDS). This may be followed by a Design FSA once detailed design specifications, SIL Achievement and test plans have been completed and reviewed internally and before it is approved by the client (whether that's an OEM, integrator, contractor or end user). The Final FSA then follows Factory Acceptance Testing (FAT).

The specific elements of the functional safety management system that are the most relevant will vary with each phase of the FSA, so extensive checklists can be a useful tool to help ensure that assessors cover all the bases. However, checklists should be used with caution, because an assessment is much more than a tick-box exercise, as already mentioned. Checklists should not be used in a rigid way or as the sole means of ensuring that sufficient evidence has been examined to demonstrate that functional safety has been achieved or, if not, for identifying those areas of the safety system and project that require remedial work.

People are the key

People are the real key to achieving an efficient and effective FSA. Assessors should be looking to collect evidence from those who have been involved with the project, while the most significant contribution to the breadth and depth of coverage of the FSA comes from the knowledge and experience of the assessors themselves.

Once the evidence has been gathered and sifted and judgements have been made, the results of an FSA cover a spectrum, rather than delivering a simple yes/no answer.

Acceptance means there is sufficient evidence that the relevant requirements supporting the functional safety objective have been achieved.

Qualified Acceptance at the Preliminary FSA and the Design FSA stages means there is insufficient evidence that the relevant requirements have been achieved and remedial action must be taken within a specified period agreed with the assessor. Qualified Acceptance at the Final FSA stage again points to insufficient evidence and a requirement for remedial

action to be taken. The reason for not achieving full Acceptance does not have to be anything that would have a material impact on the required functional safety.

Rejection means there is insufficient evidence that the relevant requirements have been met, giving the assessors serious concerns about whether functional safety has been achieved. It calls for urgent attention by the safety project team, followed by a reassessment by the FSA team.

It is not uncommon to find that many qualified acceptances relate to an absence of formal reviews and approval of key documents by clients – this may be due to the clients not fully understanding their roles and responsibilities within the project and/or their lack of detailed knowledge of the scope of the assessment or fuzzy terms and conditions relating to sign/offs and approvals.

Also, qualified acceptances relate to inadequate Safety Requirement Specifications (SRS), often resulting in:

- Large amounts of assessor time in evaluating the evidence (or lack of) supporting identification of Safety Instrumented Functions (SIF) from Cause & Effect charts including rationale and assumptions
- Lack of traceability from specification through to validation of individual safety instrumented functions

They can also quite often relate to SIL Achievement/Verification activities and the adequacy or otherwise of safety data-sets for third-party elements, as well as the competency profiles and capabilities of team members.

Furthermore, in respect of the specific safety systems, it should also be asked whether there is evidence of an analysis of the certification claims supporting elements/subsystems and systems; whether there is a definition of what can and cannot be done within the bounds of the certification and safety manual, and, if these have been transgressed, what was the supporting rationale and whether a detailed impact/risk assessment was performed by competent persons.

Assessor Code of Conduct

Functional safety assessors may find themselves being drawn into discussions relating to detailed corrective actions, project time/cost issues and/or constraints. These can create tensions and conflicts between project teams and the assessor; the latter must make it clear throughout the assessments that they work to a code of conduct. This should be clearly documented and include the following attributes:

- Act in a professional manner
- Ensure that nothing affects or challenges impartial assessment and judgement
- Demonstrable evidence of competency
- Clear formal communication, timely, objective
- Distinguish fact and evidence from opinion
- Assessment rigour shall be in proportion to safety risk assessment
- Only provide advice if it cannot compromise independence

- Ensure assessor judgements are not influenced by inappropriate pressures or other factors
- Ensure safety is given due priority
- Ensure safety implications are made known to appropriate persons and organisations
- Ensure FSAs are planned, managed and minimise disruption to projects

Fit for purpose

Every organisation involved in supplying and implementing systems that relate to functional safety has a duty to familiarise itself with the relevant standards and ensure that it's fulfilling its role in the overall process of delivering a safe working environment. Suppliers must be able to demonstrate to customers and regulators that they are a strong link in the safety chain, and the FSA is the crucial tool that enables them to do so.

ABB has extensive experience in the design and performance of Functional Safety Assessments. For more information, email moreinstrumentation@gb.abb.com ref 'Functional Safety Assessments'.