Compliance to IEC 61508 means more than just Pfd!

Stuart Nunns CEng, BSc, FIET, FInstMC

ABB Ltd

Market environment

Statistics relating to the performance of major manufacturers are published internationally and incidents, especially those causing injury or death, make headline news. Recent inquiries into major incidents [1] [2] have reinforced the importance of international standards IEC 61508 [3] and IEC 61511 [4] as a benchmark of acceptable good practice in the management, design, application and operation of safety-instrumented systems.

In today's world, manufacturers and producers face significant liabilities if they act in a socially irresponsible manner. Such liabilities include direct financial costs arising from the incident itself, from legal costs and fines if found guilty of breaking the law, damages paid to injured parties and damaged reputation, which can have far reaching implications on the business. The result is that safety and profitability and reputation are inextricably linked.

The market environment can be summarised as follows:

- Increasing dependence on safety critical systems to achieve tolerable risk levels;
- Increasing need to justify that you have achieved adequate levels of safety;
- Safety Regulators using international standards as basis of what is reasonable;
- Maintenance of reputation in relation to safety a key business driver;
- Increasing formality of safety culture, management of functional safety, competence of the organisation and personal competence.

Standards and good practice

The demands of the safety systems market are becoming ever more exacting. International standards IEC 61508 and IEC 61511 are increasingly being used as a benchmark of acceptable good practice to both demonstrate compliance that (1) the required functional safety has been achieved and (2) that the legal requirements have been met. The adoption of these standards is not surprising given the increasing dependence on safety-instrumented systems to achieve the required risk targets. With heightened awareness to contractual rigour and the potential for litigation, should something go wrong, organisations need to demonstrate that their functional safety capability has achieved accepted good practice.

HSE's stated policy on use of IEC 61508 and IEC 61511 is as follows:

"HSE will use IEC 61508 as a reference standard for determining whether a reasonably practicable level of safety has been achieved when electrical, electronic and programmable electronic systems are used to carry out safety functions. The extent to which HSE will use IEC 61508 will depend on individual circumstances; whether any sector standards based on IEC 61508 have been developed and whether there are existing specific industry standards or guidelines. IEC 61511 and IEC 62061[5] will be used as reference standards for the process sector and for machinery respectively"

The Occupational Safety and Health Administration (OSHA) in the USA has stated its position in respect of IEC 61511 which is (abridged) [6]:

"OSHA considers the revised ANSI/ISA – S84.00.01 – 2004 Parts 1 – 3 (IEC 61511Mod) to be recognised and generally accepted good engineering practices for safety instrumented systems".

Supply chain issues

IEC 61508 and IEC 61511 are performance based standards and promote the concept of a safety lifecycle. The supply chain, in respect of a safety instrumented system, covers the specification, design, implementation and operation phases and demands effective functional safety management throughout all phases of the safety lifecycle if functional safety is to be achieved.

The safety lifecycle can span many years in respect of the life of the asset and the asset's safety-instrumented systems. In particular the safety lifecycle will involve many different organisations and a variety of client – supplier contractual relationships requiring clearly specified responsibilities, activities and deliverables. It is therefore essential that all those organisations involved in implementing phase(s) of the safety lifecycle take all necessary steps to demonstrate their competency and capability to implement the requirements of the relevant clauses of the phase(s) of the standards.

Achieving the necessary organisational capability to effectively implement the requirements of IEC 61508 and IEC 61511 is not an easy task and will require all those organisations in the supply chain that have responsibilities for one or more phases of the safety lifecycle becoming fully conversant with these standards and mapping their areas of responsibilities against the relevant phases of the standards. Many regulatory authorities use, or are likely to use the standards as a benchmark of acceptable good practice (as indicated above for HSE and OSHA) and expect those in the supply chain and end users to become sufficiently conversant with the requirements of those standards.

One particular area requiring attention, which is of fundamental importance, is the development of the Safety Requirements Specification which includes the specification of the safety instrumented functions and target SIL for each function. This is a specific area where co-operation between the end user and supplier is essential. In general, co-operation between the end user and supplier can reap considerable benefits by facilitating the clarification of project roles and responsibilities and is an important basis for ensuring that the SIL achievement/verification activities will be undertaken in an efficient and effective manner.

Revision of IEC 61508

Currently IEC 61508 is being revised with a planned publication date of 2010. Of particular importance to product manufactures is the proposal concerning the "Safety Manual for Compliant Items". This Safety Manual would encompass any component that is to be supplied to another party where the supplier is making specific claims of compliance to IEC 61508. The purpose of the Safety Manual is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of IEC 61508. The supplier will need to document a justification for all the information in the safety manual.

If this proposal is adopted then it will move the industry forward by providing a common set of data for each safety element including the information relating to systematic capability. One positive outcome of this will be to limit, and hopefully curtail, the appearance of so-called "claims to fame" for elements which more often than not state that the element is *"SIL rated"* or achieves the SIL only in respect of the Pfd for dangerous random hardware failures!

Functional safety management

Historically, *product* certification was originally undertaken to historical standards such as DIN 19250 or VDE 0801 and more recently to IEC 61508. However, the wide-spread adoption of the standard coupled with an increased awareness of the need for functional safety management and competency, at both an individual and organisational level, has seen a step change in direction to include the certification of the capability of an organisation to undertake specified functional safety activities. This would include the organisation's functional safety management arrangements and procedures together with the organisation's competence management system which would embraces personal competence in respect of the specific duties an individual has to perform.

Currently the development and implementation of functional safety management systems appears to be driven by safety system suppliers. However, it needs to be embraced by all organisations spanning the safety lifecycle and, in particular, end users who need to provide evidence to their regulatory authorities as a result of regulatory inspections/audits or in support of safety cases.

It is interesting to note that the "Recommendations on the design and operation of fuel storage sites" in relation to the Buncefield major incident [1] and the "Report of the BP US. Refineries Independent Safety Review Panel" [2] raised issues of competence and management but are also relevant to the management of functional safety. Paragraph 15 of the Buncefield report states:

"We have noted with interest the recent report of the BP US refineries Independent Safety Review Panel by James Baker's panel in the United States. Some of the recommendations and findings in that report align with our thinking arising from the Buncefield investigation. In particular the Baker report's recommendations relating to process safety leadership, process safety culture, performance indicators, independent monitoring and industry leadership are relevant. The Baker panel's findings regarding the implementation of good engineering practices, safety knowledge and competence also a line with our views".

ABB's capability strategy

Organisational and individual functional safety competence is an essential requirement for ABB as a whole and it is paramount for ABB to demonstrate compliance and competence in an irrefutable way. The requirements of IEC 61508 and IEC 61511 standards are important to ABB especially as many major clients are specifying them as a functional safety benchmark and as a contractual requirement.

In order to achieve organisational and individual functional safety competence, ABB's strategy is to establish a number of Safety Execution Centres (SEC's) around the world and for these SEC's to:

- Achieve third-party certification through TUV Rheinland for their Functional Safety Management System (FSMS) against IEC 61508;
- Integrate and configure safety-related systems using wherever possible subsystems and elements which are certified to meet all relevant requirements of IEC 61508;
- Use staff who can demonstrate competency through experience, knowledge, training and qualifications. This underpinned by:
    - ✓ adoption of the guidelines "Competency Criteria for Safety-related System Practitioners" [7];
    - ✓ achievement of TUV Functional Safety Engineer Status for key professional engineering staff.

The benefits to ABB of certification of its FSMS are:

- Providing independent assurance that ABB's FSMS has achieved accepted good practice;
- Limiting the risk exposure to potential liabilities;
- Demonstrating due diligence;
- Establishing an efficient, repeatable 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;
- Gaining a competitive advantage.

In addition, as industry becomes more mature in its understanding of IEC 61508 and the details of what product compliance means, it is apparent that many claims currently being made for the achievement of a specified SIL of a product will not meet the full requirements of the standard in respect of:

- The requirements for hardware safety integrity comprising:
    - ✓ Architectural constraints; and,
    - ✓ Probability of dangerous random hardware failures
- The requirements for systematic safety integrity comprising:
    - ✓ The avoidance and control of systematic failures; or,

- ✓ Evidence that the equipment is “proven is use”

There is, unfortunately, a perception that in order to meet the target SIL for a safety instrumented function all that is required is the Pfd of the dangerous random hardware failures!

In demonstrating organisational and individual functional safety competence ABB developed a comprehensive and generic functional safety management system capable of being rolled-out and tailored for each SEC. This was the most significant activity undertaken. It entailed defining a comprehensive safety life cycle model mapping the relevant phases of IEC 61508 and IEC 61511 (notably phase 9 of IEC 61508 and phase 4 of IEC 61511). This safety life cycle model is fully supported by procedures, framework documents (basic default information for a safety project to be customised to meet any specific project variations) and skeletons (a template consisting of all necessary headers to be completed) – collectively known as the Functional Safety Management System (FSMS).

In addition the FSMS documentation covers all aspects of the life cycle including the management system, policy, competency, assessments and audits, modification and impact procedures, verification procedures and reporting. It also included skeleton documents for all the main working documents such as Functional Design Specification, System Design Specification, Testing, Factory Acceptance Test, Site Acceptance Test and operational manuals.
The development of this safety lifecycle model also makes full use of the existing quality management processes and procedures.

In order to minimise company liabilities, it is essential that the same rigorous approach to functional safety must apply to any third-party integrators using ABB products. A programme of work is required to perform a gap assessment of third-party integrators and to thereafter work with them to develop a compliant functional safety management system, preferably in line with that of the main system vendor. This process benefits the third-parties in that they can also achieve certification and gain all the advantages.

Summary

The international safety market is undergoing many changes driven by technology, standards, legislation and incidents. Those organisations working in this demanding and highly competitive arena seek to differentiate themselves, secure market advantage and demonstrate competence and due diligence. Many organisations see accredited certification of the organisation as a positive step forward.

Accredited certification for an organisation is a significant undertaking. It requires management commitment at the highest level in addition to a comprehensive work programme involving not only that part of the organisation selected for certification, but other groups within the organisation itself.

References

[1] "Recommendations on the design and operation of fuel storage sites"; Buncefield Major Incident Investigation Board: << http://www.buncefieldinvestigation.gov.uk/reports/recommendations.pdf >>.

[2] "The Report of the BP US Refineries Independent Safety Review Panel" (concerning the Texas City incident). << http://www.csb.gov/completed_investigations/docs/Baker_panel_report.pdf>>.

[3] IEC 61508 – Functional safety of electronic/electrical/programmable electronic safety-related systems.

[4] IEC 61511 – Functional safety – Safety instrumented systems for the process sector.

[5] IEC 62061: Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control; systems.

[6] OSHA position on IEC 61511: Stated in a letter from OSHA to ISA dated 29 November 2005. (Permission to state the content of the letter obtained from ISA).

[7] Competence Criteria for Safety-Related System Practitioners. Guidance provided by the IET in collaboration with the HSE and BCS. Revision published 2006. Available from:
<< http://www.theiet.org/publishing/books/policy/comp-crit.cfm>>