Introduction, background and guidance for completion of Part 3 of CASS32 'CASS Functional Safety Management Declaration lodged with CASS-appointed body'

Document History

Revision	Date	
0A	7 Jan 2011	Internal
0B	13 Jan 2011	internal, incorporating CdS Help Pt3 Rev 2, and BR detailed review and comment
0C	10 Feb 2015	Internal, accepting review comments to date
1	12 Feb 2015	Internal

Table of Content

References and related documents

The following documents are available from www.61508.org/cass:

CASS28	CASS Templates For Software Requirements In Relation To IEC 61508 Part 3 Safety Function Assessment
CASS32	The CASS Functional Safety Management Declaration Lodged with a CASS-appointed Body
CASS33	Help and guidance on CASS32 in general, and on completing Part 1 of CASS32 in particular
CASS34	Help and guidance on completing Part 2 of CASS32
CASS35	Help and guidance on completing Part 3 of CASS32
CASS48	IEC 61508-1_2010 CASS TOES FOR FUNCTIONAL SAFETY MANAGEMENT
CASS49	IEC 61508-1_2010 CASS TOES FOR THE OVERALL SAFETY LIFECYCLE
CASS50	IEC 61508-2_2010 CASS TOES FOR THE E-E-PE SYSTEM SAFETY LIFECYCLE

Other Documents, not available from www.61508.org/cass:

CASS36	Dossier Receipt from a CASS-appointed body, issued to an owner who has lodged an FSM Declaration

Normative references

IEC 61508-1:2010	Functional safety of E/E/PE safety-related systems – Part 1: General Requirements
IEC 61508-2:2010	Functional safety of E/E/PE safety-related systems – Part 2: Requirements for safety-related systems
IEC 61508-3:2010	Functional safety of E/E/PE safety-related systems – Part 3: Software Requirements
IEC 61511-1:2003	Functional safety – Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

Note: In this document, all references to IEC 61508 standards mean the 2nd editions (published in 2010). Where IEC 61508 is referred to without the part number (suffix), this refers to all or any of the parts generally.

Abbreviations and terminology

BPCS	Basic process control system
CASS	Conformity Assessment of Safety-related Systems; a methodology used to show compliance
FSM Declaration	CASS32, including any specified attachments.
E/E/PE	Electrical, Electronic, or Programmable Electronic. A descriptive term with reference to the technology of a safety-related system, as used in IEC 61508
E/E/PES	An Electrical, Electronic, or Programmable Electronic safety-related system
FSM	Functional Safety Management
owner	the person, business, partnership or other legal entity who is completing the CASS32 form describing and documenting their Functional Safety Management system
Part 1	When used alone, this is a reference to the specific Part 1 of the FSM Declaration (CASS32) document
Part 2	When used alone, this is a reference to the specific Part 2 of the FSM Declaration (CASS32) document
Part 3	When used alone, this is a reference to the specific Part 3 of the FSM Declaration (CASS32) document
PES	A Programmable Electronic safety-related System, usually with the emphasis on being 'programmable' or software-based.
SIL	Safety Integrity Level. An IEC 61508 term (q.v.) related to the increasing requirements in terms of performance properties and assessment rigour of a safety system with the increasing levels of risk reduction involved, from 1 (low) to 4 (highest)
TCSL	The CASS Scheme Ltd.
TOE	Target Of Evaluation. A specific property of a Functional Safety Management system for which the requirements are specified in one or more clauses in IEC 61508, and for which a demonstration of compliance is required.

1 Introduction

We all have a 'Duty of Care' to manage the hazards in our workplaces. Duty of Care obliges us to:

- identify appropriate standards and practices;
- take reasonable steps to comply with the standards and practices;
- monitor compliance;
- demonstrate that what we have done is reasonable.

IEC 61508 and its related standards are well established internationally as the standards that apply when instrumented systems are used to achieve safety through reducing the risk of hazardous consequences.

To ignore these standards would be negligent and might leave us open to prosecution. We need to be able to show evidence that we have complied.

All of the requirements of Functional Safety Management (FSM) shown in IEC 61508-1:2010 clause 6 and within other clauses of the standard need to be demonstrated by anyone involved in safety instrumented systems and in any part of the lifecycle if the system is to comply with the IEC 61508 group of standards.

FSM is essential in achieving compliance for all safety-related systems throughout the life of each system. (IEC 61508, Figure 2).

FSM provides a framework so that people working in functional safety have a clear understanding of:

- Why is functional safety important to the business?
- What processes and procedures need to be followed to achieve and maintain functional safety?
- What are the main activities that are required?
- Who is responsible for each functional safety activity?
- What skills and experience are needed for each activity?
- What output documents or information records need to be produced to support each activity?
- How are the outputs to be checked?
- How are issues and recommendations to be managed and resolved?
- How is the performance of functional safety systems to be monitored?
- How will the managers monitor the effectiveness of the management system?
- How will changes and modifications to the system be managed?

History over the last 30 to 40 years shows us that almost without exception all major accident events have been caused by multiple systematic failures. These failures are primarily due to a lack of management. Management is the most important and fundamental technique that is used to achieve 'systematic integrity', which means reducing the risk of systematic failure.

The CASS32 FSM Declaration form enables you to understand what is needed in FSM and to demonstrate the steps that you have taken to manage your lifecycle phases and activities relating to E/E/PE safety-related systems.

An FSM Declaration held by a CASS-appointed body is made available to the relevant national safety authority[1] upon request by that safety authority. An FSM Declaration will be held for a period of 10

1 In the United Kingdom a relevant national safety authority would be the Health & Safety Executive.

years from the date accepted for filing of the un-audited FSM Declaration.

For an FSM Declaration held by a CASS-appointed body to be accepted by that body, all sections of the FSM Declaration must be completed[2].

The CASS-appointed body makes no warranty concerning the contents of the FSM Declaration nor accepts any liability for its contents. There shall be NO reference to a CASS-appointed body certificate for a CASS FSM Declaration. The document is a self-declaration by the owner who has completed Part 3 and Part 2, and it does not need to be audited.

On each occasion that a customer of the owner named above requests a copy of the FSM Declaration then the CASS-appointed body will contact the owner named on page 1 to confirm that the customer making the request is a customer of the owner and then a copy will be made available on payment of an administration fee to the CASS-appointed body by the customer.

Copies of the FSM Declaration requested by a relevant national safety body will be made available free of charge, let or hindrance.

The statements made in this Part 3 show the FSM system. Part 2 shows the activities being covered by the safety management system. When reading the completed FSM Declaration, Part 2 is the context for Part 3. FSM activities are mapped to documents in Part 2, Table 4 of the FSM Declaration. The purpose of this part, Part 3, is to explain the rationale for the FSM framework in detail. This is to demonstrate compliance clearly and completely.

2 Within the FSM Declaration table the "Systems and procedures in place" column and the "Documentary evidence" column must both be completed for all case but the "Notes" column need only be completed where relevant.

2 Completing Part 3 opening section

Part 3 begins with the date upon which the declaration of FSM has been completed by the safety manager (or equivalent) and acknowledged by the Board or Managing Director, i.e. the owner of the FSM Declaration. The term “owner” is used to describe the person, business, partnership or other legal entity who is completing the form describing and documenting their FSM system. For example,in the case of an operator the owner is the person with ultimate accountability for the safety of people at the facility. In the case of an equipment manufacturer, the owner is the person who is responsible for ensuring the equipment is correctly specified and manufactured.

The opening lines of this Part 3 of the FSM Declaration are:

PART 3: FUNCTIONAL SAFETY MANAGEMENT SELF-ASSESSMENT REPORT

Date:

Safety Manager or equivalent (write name here):

Signed: Date:

Board chair or Managing Director (write name here):

Signed: Date:

The Date is the date for which the information in Part 3 was completed. The FSM Declaration is not intended to stop you from improving your FSM systems and so there is a date at which the statements made were true.

The relevant personnel to sign for Part 3 depends upon the structure of the business undertaking the safety instrumented systems work and the more common situations are as follows:

The "owner" is an individual:

If an "owner" is an individual then that individual is both the safety manager and the board chair for their own-self-employment. For completeness, and for the avoidance of doubt, the "owner" should write their name on both the line for the "Safety Manager or equivalent" and on the "Board chair" line and sign and date both. The date next to the signature should be the date it was signed.

The "owner" is a partnership:

If a partnership is completing the document then the partnership will need to identify the partner that has overall responsibility for ensuring that the partnership as a whole undertakes its safety work properly. That role is equivalent to that of a "Safety Manager" and so that partner should write their name against the role of "Safety Manager or equivalent" and sign for that role and date their signature. The partnership will have meetings of the senior partners, usually equivalent to a board meeting of a company. It is a good idea that it be agreed at such a meeting which of the partners is to sign on behalf of the whole partnership. The nominated person should then write their name against "Board chair or Managing Director" and sign for that role and date their signature.

Note that for the partner taking the equivalent role to the Safety Manager, the name allocated should be in agreement with the statement made against the responsibilities for safety assigned and defined on the organisation chart, or equivalent, that has been referred to in response to item 3 of the CASS32 Part 3 table and as required by IEC 61508-1, clause 6.2.3.

The "owner" is a business or company:

If the form is being completed by a business or company then such a business will have responsibilities for safety assigned and defined on the organisation chart, or equivalent, that has been referred to in response to item 3 of the CASS32 Part 3 table and as required by IEC 61508-1 clause 6.2.3. The statement made in response to the responsibility for safety under the standard should be that of the Safety Manger or equivalent and should be the name written against "Safety Manager or equivalent" at the beginning of Part 3 of the CASS32 declaration form. That person should then sign for that role and date their signature.

A business or company will also have a board and/or a Managing Director. The name written here is signing on behalf of the business or company as a whole. The person accepting that responsibility, whether they are a board member or a Managing Director, should write their name against "Board chair or Managing Director". That person should then sign for that role and date their signature.

3 Understanding the table structure in Part 3

The table in Part 3 of the CASS32 FSM Declaration lists all of the information required in order to claim compliance with IEC 61508. This also meets the needs of IEC 61511 1st edition.

The structure of the table is shown below.

Item	Target of Evaluation (TOE)	Requirement (for all SILs)	Systems and procedures in place	Documentary evidence	IEC 61508-1 clause references	Notes
		Purpose				

The purpose and intended content for each column is described below.

3.1 The "Item" column

Item
This column gives an item number that is used for reference throughout these sets of guidance pages and the Declaration itself.

Do not change the "Item numbers" shown in the item number column of the table.

3.2 The "Target of Evaluation (TOE)" column

Target of Evaluation (TOE)
This column shows the title of each part of the Functional Safety Management system that should be described. The title is written in terms of which attribute of the FSM should be evaluated.

IEC 61508-1 clause 6 contains all the basic, fundamental requirements of an FSM system. The same requirements are also described in IEC 61511-1 clause 5.

In order to demonstrate that an FSM system complies with the standards it is necessary to evaluate the management system that exists.

The titles show the various attributes of the FSM as 'targets of evaluation' (TOE) that are to be assessed in order to demonstrate that the FSM system in place complies with the standard. The list of TOEs is the same as given in Part 2 Table 4 of the FSM Declaration.

Do not change the content of this column.

3.3 The "Requirement (for all SILs)" column

Requirement (for all SILs)
Purpose
This column shows the purpose of the requirement of the standard and, hence, also the purpose that needs to be fulfilled by the systems and procedures for Functional Safety Management.

The statements made in the neighbouring columns on this row will fulfil the purpose described in this column.

IEC 61508-2 and IEC 61508-3 Annexes, and IEC 61508-7 provide requirements and guidance on techniques and measures to avoid or to control systematic failures. The tables classify techniques and measures as 'mandatory, highly recommended or recommended', depending on the SIL target for the safety function.

Project management and documentation are the only two techniques that are ***mandatory for all SIFs having any SIL from SIL1 to SIL4***, which is why the column title contains the 'for all SILs'. Although these requirements apply to all SIL ratings the level of effectiveness necessary does depend on the SIL. Systems that implement SIL 3 functions need more effective management than systems that implement only SIL 2 functions. The level of effectiveness is generally improved by applying an increased level of independence and an increased level of detail in verification and validation.

Do not change the content of this column.

3.4 The "Systems and procedures in place" column

Systems and procedures in place
This column provides the space in which you describe and list the systems and procedures employed by you to achieve the purpose shown in the same row and in the preceding column.

All systems and procedures must be documented, but the form in which they are documented is not mandated (paper, electronic etc.).

What is essential is evidence that the systems and procedures exist and are sufficiently effective in practice. That evidence requirement is dealt with in the next column of the table.

The list of all your relevant systems and procedures will be the same as those given in CASS32 Part 2 Table 4.

Include the specific document reference and revision identifiers for the systems and procedures.

4.1. The "Documentary Evidence" column

Documentary evidence
This column provides the space in which you identify the documentary evidence for both the existence of the systems and procedures, and the evidence for their implementation. The systems and procedures are those that have been documented and described on the same row and in the preceding column.

The systems and procedures are already summarised in Part 2, Table 4. In this section we need evidence that the systems and procedures are effective in practice.

The best evidence of this would be records of audit (either internal or external) against the specific procedures. The audits need to be regular and current, although the frequency will be specific to the activities being carried out. Evidence is needed of how the audit recommendations have been resolved. Evidence is needed that the audit reports have been reviewed and accepted by the manager responsible for FSM.

Reference to a specific audit report (by number, title and date) covering the item in question should be sufficient. A single overall reference may be made to a separate assessment report that covers all of the items together. In that case the assessment report should be submitted as part of the FSM Declaration.

Note that the purpose of an ***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 system*** as a whole. Assessment includes making judgement on technical issues as well as on procedural issues.

3.5 The "IEC 61508 2nd edition clause references" column

IEC 61508 2nd edition clause references
This column gives the reference from the standard for the relevant clause and paragraph.

The format of the reference shown in this column begins with the IEC 61508 part number and is followed by the clause number, and so on. For the reference the nomenclature 1:6.1.8 denotes IEC 61508-1, clause 6.1.8.

Do not change the content of this column.

3.6 The "Notes" column

Notes
This column gives space for additional explanatory notes of your choosing

There is no requirement to provide additional notes and so this column can be left blank. The space is provided for the owner to insert notes that assist the reader of the declaration in understanding anything written in, or omitted from, that row.

4 Completing the table in Part 3

In Part 2 of the FSM Declaration, you have identified the specific methods and procedures by which you intend to comply with requirements of the standard, and have identified for each of those a 'conformance plan' in which you have argued / demonstrated that the procedure is appropriate and will be compliant if followed as intended.

In Part 3 of the FSM Declaration, you will be identifying the evidence supporting your claim that those procedures are in place, and being followed appropriately. The Part 3 table is organised in the same general structure as Part 2 Table 4, against the same set of TOEs.

It is necessary to write something in all of the columns, with the single exception of the "Notes" column. The owner will find that the "notes" column is available to them to give additional explanatory information here to assist the reader and examiner of the declaration.

In Part 3 of the FSM Declaration it is necessary to write something in the "Systems and procedures in place" column and in the "Documentary evidence" column for every item in the table. For some owners involved in IEC 61508 not every item will be applicable and so it is possible to write "Not applicable because ..." in a row within the column. However, it is essential that a statement that a row is "Not applicable because ..." must be reflected in the scope shown in Part 2 of the FSM Declaration as well as being explained here in Part 3. For example, if the owner's part in the safety instrumented system does not include operation and maintenance then it is not applicable to have a procedure for operation and maintenance performance analysis and so, in this example, the owner might write "Not applicable because operation will be undertaken by X" (where "X" is the name of the third party).

It is not sufficient to write "Not applicable" without explanation. The majority of basic FSM applies to all owners.

The list of TOEs in the table in Part 3 of the FSM Declaration comprises:

- Functional Safety Management
- Functional Safety Policy
- Organisation and Responsibilities
- Identification of relevant lifecycle phases
- Documentation structure and content policy
- Techniques and Measures of conformance plan
- Corrective action procedure
- Competence assessment process
    - Procedure for handling of hazardous incidents and near-misses
    - Procedure for Operating & Maintenance performance analysis
    - Functional safety audit process
    - Modification process for Safety related systems
    - Procedures for maintaining information on hazards with respect to Safety-Related Systems or to the Safety Instrumented Function.
    - Configuration Management procedures
    - Procedures for provision of training and information for the emergency services
    - Functional safety Management - Formal Reviews

- Supplier assessment process
- Functional safety assessment

Each of these relates to a specific set of clauses in IEC 61508, as given in the Table column "IEC 61508 2nd edition clause references". A detailed consideration of the required information for each of the above is given in the following sub-sections.

4.1 Functional Safety Management

The overall responsibility for achieving and maintaining functional safety must be clearly defined and assigned by the owner.

The requirement of this opening section is to specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety. IEC 61508-1 clause 6.1.1 requires that we specify the responsibilities in the management of functional safety. In IEC 61508-1 clause 6.2.1 the standard talks about a typical organisation appointing one or more persons to take overall responsibility for a list of functions and duties.

The organisation needs to have a top-level framework, procedure or management plan that establishes the context for the detailed items that follow. That document must be reviewed and approved by the owner. It must be communicated to all parties with accountability for functional safety activities.

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

Evidence must be available to show that this top-level document is current, effective and regularly reviewed by the owner.

The evidence required here will be the evidence that demonstrates that the FSM system stated by the owner in Part 3 of the FSM Declaration has been applied in practice on projects, by reference to the project records of compliance.

4.2 Functional Safety Policy and Strategy

For a team to work together they need to have common policies for safety so that conflicting and inconsistent approaches to safety are avoided. In this section of the FSM Declaration the owner identifies the policy statements and strategies that are being applied.

This section needs to reference the policy and to show that the policy exists, is understood and implemented through the strategy.

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.

Functional safety is just one of the strategic elements an organisation can use to achieve its safety goals.

FSM is an extension of quality management and risk management. It must be seen in the context of the organisation's overall risk management systems.

Many of the requirements that need to be covered in FSM planning will have already been covered in

corporate standards, project execution plans, quality plans, safety plans, risk plans, maintenance plans or technical integrity plans.

It is not sufficient to assume that existing risk management and quality management systems cover the requirements for FSM. The FSM planning should specifically consider the requirements for functional safety and make reference to the relevant parts of the risk and quality management systems.

4.3 Organisation and Responsibilities

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. The contractual boundaries are often made worse by geographic separation and by cultural differences. The FSM planning must specifically address the boundaries and gaps in responsibility.

The gaps that commonly cause problems include:

- gaps between the owner, the engineering contractors, and the system suppliers;
- gaps between the project teams and the operations and maintenance teams;
- gaps between the instrument and control team and the facility manager.

IEC 61508-1 clause 6.2.3 requires clear identification, assignment and communication of responsibilities.

IEC 61508-1 clause 6.1.1 requires that we specify the responsibilities in the management of functional safety. Ensure that all processes are 'owned', and that all hand-overs and transfers of ownership are positively managed.

Authority levels must be clearly defined. Where authority levels are not clearly understood individuals may assume responsibility beyond their level of authority and beyond their level of competence.

The evidence will be required to demonstrate that roles and responsibilities were allocated, integrated and managed effectively.

4.4 Identification of relevant lifecycle phases

Many users have trouble understanding what is meant by lifecycle phases. Confusion arises because the lifecycle phases will inevitably overlap.

Lifecycle phases can be defined most easily and intuitively by the key inputs, activities and outputs in each phase. People generally have no trouble in identifying the key documents or key outputs that govern their work. The lifecycle phases are effectively defined by the milestones at which the key outputs are issued for use.

Lifecycle planning is required by IEC 61508-1 clause 7.1.4. Lifecycle phases may be defined with reference to IEC 61508-1 Figures 2, 3, and 4, and Table 1. Users are able to define their own phases to suit their own particular methods.

The lifecycle plan should make clear which phases are in your organisation's scope of work. Responsibilities, interfaces and boundaries should be clear in the lifecycle.

The evidence required here will typically be a section in the FSM plan or it may be a separate safety lifecycle document plan. It may be combined with evidence for the following item.

4.5 Documentation structure and content policy

IEC 61508-1 clause 5 specifies requirements for the information that is necessary to support all of the safety lifecycle phases.

Defining a set of safety lifecycle deliverables at the start of a project is a natural way of giving project team members a clear understanding of what they are expected to deliver in the end. The 'functional safety dossier' should be outlined at the beginning of the project rather than being compiled as an afterthought. Eventually, the user will be expected to maintain the system documentation during the operational and subsequent phases.

The initial plan may describe the outputs using vague or generic terms. The plan may be refined as the project is developed. The functional safety deliverables must be individually and specifically identified. It is not acceptable for them to be indistinguishable within a general document management system.

The fundamental requirements for the document management system are that the information must be readily accessible, understandable and current.

The evidence needed here may include:

- reference to the register of safety lifecycle documents;
- reference to the document or information management procedures and system.

The evidence required should show that the documentation policy has been followed in practice on projects, by reference to the project records which are used to track and manage that activity.

4.6 Techniques and measures conformance plan

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

Reference should be made to IEC 61508-2 Annexes A and B, and to IEC 61508-3 Annexes A, B and C in the case of equipment suppliers.

Evidence must be available recording the rationale for selection of techniques, measures and procedures.

The most convenient way to record the selection of techniques and measures is in a tabular form, based on the tables given in IEC 61508-2 and IEC 61508-3. A good worked example is given in IEC 61508-6 Annex E.

The evidence should demonstrate that the techniques and measures that were selected are appropriate for the SIL and have been applied with sufficient effectiveness and rigour.

4.7 Correction action procedure

Formal procedures must be put in place to manage the follow up and resolution of corrective and preventative actions and recommendations. This includes tracking of issues such as deviations and non-conformances. It also includes resolving issues arising from hazard and risk studies, assessments, audits, verification, validation, configuration management, incident reports and analysis.

The evidence required here is with reference to the systems and procedures that are used and to audit or assessment reports that show that they are being used effectively.

4.8 Competence assessment process

Each activity will require competent people to be involved. The level of competency required needs to

be assessed to match the activity and the competency of the people assigned the responsibility for the safety system needs to be assessed. In some cases personnel involved in a safety system will need some level of supervision to competently complete an activity. The matching of competencies required to the people undertaking each task or activity needs to be managed. The owner identifies their competency management system in Part 2 of the FSM Declaration.

The standards IEC 61508 and IEC 61511 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

The evidence required here is that which demonstrates that the defined competency assessment process is followed, by reference to the company records which track that process. It is also required to demonstrate that the individuals fulfilling the defined roles on projects have the appropriate competency, by reference to the project records of the named individuals undertaking the planned roles and responsibilities, and the competencies specified as necessary to fulfil those roles.

Note that Regulators are requiring that safety management is properly covered. Whether or not the owner's business activities are in the UK, the UK's safety authority, the HSE has published an excellent and clear guide to competency management systems which any owner will find helpful. See the HSE guidance - “Managing Competence for Safety Related Systems” July 2007. The document, both parts 1 and 2, are available as a free download from the HSE's website at www.hse.gov.uk

At the time of writing this guidance page it can be found at:

http://www.hse.gov.uk/humanfactors/topics/competence.htm,

but if it has been moved elsewhere on the HSE's website then a search on the title of the competency management system guidance will reveal its location.

The HSE guidance will show what is expected of a competency management system that checks and monitors the competencies of everyone involved in safety instrumented systems and at every stage of their lifecycle.

4.9 Procedure for handling of hazardous incidents and near-misses

Any hazardous incident that occurs or near-miss event cannot be ignored. Lessons need to be learned on every occasion and to make that possible an event should be properly studied and documented. The lessons learned from the event can then be communicated to everyone involved in the safety instrumented system and any corrective action that is necessary can be planned, authorised, managed and implemented.

Even if the system fully responded correctly and no corrective action is needed the near-miss or incident is itself either a demand on the safety instrumented system, or a major test of the effectiveness of the associated procedure which should be documented and can be later compared to the system designer's statement about the frequency or handling of such events.

The owner of the FSM Declaration will document the procedures and systems to be used when responding to hazardous incidents and near misses in Part 2.

The evidence required here is that which demonstrates that the procedure is followed in practice on projects and in operation, by reference to the owner’s operational records designed to track and address these activities.

4.10 Procedure for Operating & Maintenance performance analysis

It is important to understand that this item does not just ask that the owner describes how the safety system is operated and maintained. Within the procedures used for operation and maintenance there needs to be reviews of the work undertaken and analysis of any faults that are detected. Some faults will be equipment faults and some errors may arise from human bad-practice. The review and analysis systems that allow the operations and maintenance to be managed to ensure that the required safety integrity is achieved and maintained have been identified and justified in Part 2.

The evidence required here is that which demonstrates that the defined procedures are employed in practice, by reference to the owners operational records designed to track and monitor this activity.

4.11 Functional safety audit process

Regular functional safety audits are required under the IEC 61508-1 clause 6.2.7.

The standard does not have specific requirements regarding the degree of independence of those undertaking audits, but the degree of independence must be considered and planned. There are specific requirements for independence in functional safety assessment, see item 18 below.

The evidence required here is that which demonstrates that the defined audit process is employed in practice, by reference to audit reports.

4.12 Modification process for safety-related systems

Safety depends on the safety instrumented function operating fully and correctly on demand. Any alteration to the safety function needs to be addressed by fully defined procedures which are appropriate for the SIL of the safety function. The owner of the FSM Declaration will have identified and justified in Part 2 the systems and procedures used to ensure that all proposed changes are fully assessed prior to implementation and, when implemented, the entire process is fully managed and that each safety loop is fully tested.

The evidence required here is that which demonstrates that the defined procedures are employed in practice, by reference to the owner's operational and project records designed to track, audit, and monitor this activity. The evidence will include reference to the procedures that apply and to typical examples of documentation used to manage the modification process.

The evidence must clearly show that the impact assessment specifically considers impact on functional safety. That means consideration of changes that affect hazards and demand rates as well as changes that affect approved functional safety documentation such as specifications and drawings. For instance a change to a BPCS process set point or alarm setting to increase throughput may increase the demand rate on a related safety function. The evidence must demonstrate appropriate review and authorisation for all changes.

4.13 Procedures for maintaining information on hazards with respect to Safety-Related Systems or to the Safety Instrumented Function

There needs to be a procedure that assigns responsibility for collecting and maintaining accurate information on hazards and hazardous events, the safety functions and the safety-related systems.

This information is necessary to support items 9 and 10 above.

The evidence required here is that which demonstrates that the defined procedures are employed in practice.

Reference should be made to the procedure and to typical examples of reports that are produced in compliance with the procedure.

4.14 Configuration management procedures

Configuration management applies to hardware devices such as sensors and final elements as well as to logic solvers. The configuration includes the specific make and model of a device, its version, firmware version and its range, settings and calibration. For a valve it might include the trim selection or the speed control settings.

During development, modification, and maintenance of the safety instrumented function it is important that unauthorised components or software do not enter service. Changes to configuration must be strictly controlled and authorised.

Management of the construction and configuration will be documented and justified by the owner in Part 2. The system documented will also show at what point the system is first applied and how it is initiated. The procedure will then show how each component of the safety instrumented function can be identified uniquely and how no component of software can enter service that has not been authorised for use with the safety instrumented function.

The evidence required here is that which demonstrates that the defined procedures are employed in practice, by reference to the owners operational and project records designed to track, audit, and monitor this activity.

4.15 Procedures for provision of training and information for the emergency services

For some safety instrumented functions the emergency services may be involved, e.g. after the plant has been made safe in order to restore the plant to a stage in which maintenance and operation can safely restart.

Whenever the involvement of the emergency services is a possibility the owner will have identified the systems and procedures in place for training and working with the emergency services in Part 2. The owner will also have indicated the frequency of re-training events and meetings for information exchange.

The evidence required here is that which demonstrates that the defined procedures are employed in practice, by reference to the owners operational records designed to track and monitor this activity.

4.16 Functional Safety Management - Formal Reviews

The general requirement in IEC 61508-1 clause 6.2.1 is for ‘ensuring that functional safety is achieved and demonstrated in accordance with the objectives and requirements of this standard’. Clause 6.2.16 requires that the management activities are ‘implemented and monitored’. This requirement is very similar to the requirement for management review in ISO standards relating to quality management and risk management.

Formal review by management is an essential element in Duty of Care. Evidence must be provided of a procedure or process of regular formal reviews by the owner. The owner must be able to demonstrate that reasonable and effective steps have been taken to comply with the appropriate standards and practices.

Typical evidence would be management signatures indicating acceptance of functional safety audit and functional safety assessment reports.

4.17 Supplier assessment process

IEC 61508-1 clause 6.2.17 and IEC 61511-1 clause 5.2.5.2 stipulate similar requirements: ‘Suppliers providing products or services to an organization having **overall responsibility for one or more phases** … shall have an appropriate quality management system’.

Evidence is required to show that suppliers and service providers such EPCM contractors, design contractors and system suppliers have appropriate and effective quality systems. That evidence must include evidence of audit to show that the systems are effective and with specific regard to functional safety.

4.18 Functional safety assessment

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 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.

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

- **Framework**: Effective planning and management, covering all of the requirements of the standards
- **Foundation**: Complete and clear safety requirements specifications, based on credible and comprehensive risk assessments
- **Follow-through**: Traceability of the design, implementation, validation and operation back to the requirements and to the planning.

The purpose of the assessment is to provide feedback to management, demonstrating that these 3 elements are in place and are effective.

The assessment must also consider the systematic capability of the team and of the system components to show that systematic integrity has been achieved. This can be demonstrated through assessment of the techniques and measures that were actually used.

Functional safety assessment is usually achieved through a coordinated series of functional safety audits. It is much more than just a set of audits because it considers the overall effectiveness of the safety systems, not just compliance to procedures and standards.

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

The scope of each supplier and contractor is limited. They can usually only audit or assess 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 safety system.

Regular assessments must also be made during the operational life of the plant, and also after modifications to the plant that affect safety systems.

The requirement for functional safety assessment can be found in IEC 61508, clause 8. Assessors need to have some degree of independence. Requirements for independence are given in IEC 61508 Part 1 clauses 8.2.15 to 8.2.18.

The evidence for this item will be the completed functional safety assessment reports together with evidence of how recommendations have been followed up and resolved.

