APPENDIX 1

Functional Safety Management

Template Procedure

This procedure could be part of a company's Quality Management System (e.g. ISO 9001). It contains those additional practices (over and above ISO 9001) necessary to demonstrate Functional Safety Capability as would be audited by a reviewing body (see Chapter 7).

A large organization, with numerous activities and product types, might require more than one procedure, whereas a small company would probably find a single procedure satisfactory.

Again, the activities covered by a designer and manufacturer of instruments or systems will differ from those of a plant operator, which, in turn, will differ for a functional safety consultant/assessor.

This template has been successfully used by companies in the safety systems integration field and in consultancy firms. It consists of a top-level procedure and eight work practices to cover details of safety assessment (see Annex 1).

The terms used (e.g. Safety Authority, Safety Engineering Manager) are examples only, and will vary from organization; xxxs are used to designate references to in-house company procedures and documents.

This template should not be copied exactly as it reads but tailored to meet the company's way of operating.

Company Standard xxx Implementation of Functional Safety

Contents

1. Purpose of Document
2. Scope
3. Functional Safety Policy
4. Quality & Safety Plan
5. Competencies
6. Review of Requirement and Responsibilities

6.1 Source of the requirement
6.2 Contract or project review
6.3 Assigning responsibilities

Safety Critical Systems Handbook. DOI: 10.1016/B978-0-08-096781-3.10023-9
Copyright © 2011 Dr David J Smith and Kenneth G L Simpson. Published by Elsevier Ltd. All rights of reproduction in any form reserved

7. Functional Safety Specification
8. Life Cycle Activities

8.1 Integrity Targeting
8.2 Random Hardware Failures
8.3 ALARP
8.4 Architectures
8.5 Life-cycle activities
8.6 Functional Safety Capability

9. Implementation
10. Validation

Work Instruction xxx/001 – Random Hardware Failures & ALARP
Work Instruction xxx/002 – Integrity Targeting
Work Instruction xxx/003 – Life Cycle Activities
Work Instruction xxx/004 – Architectures (SFF)
Work Instruction xxx/005 – Rigour of Life Cycle Activities
Work Instruction xxx/006 – Functional Safety Competence
Work Instruction xxx/007 – Functional Safety Plan
Work Instruction xxx/008 – Functional Safety Specification

1 Purpose of document

This standard provides detail of those activities related to setting and achieving specific safety-integrity targets and involves the design, installation, maintenance and modification stages of the life-cycle. Where the activity in question is already catered for elsewhere in the XYZ Ltd quality management system, this document will provide the appropriate cross-reference.

The purpose of this procedure is to enable XYZ Ltd to provide in-house expertise in functional safety such as to meet the requirements of IEC 61508. Since IEC 61508 is not a prescriptive standard the issue is one of providing a risk based "safety argument" that is acceptable to one's regulator/auditor/HSE. A functional safety assessment consists of evidence showing that the areas of the standard have been adequately addressed and that the results are compatible with the current state of the art.

This requires a proactive risk-based approach rather than a slavish adherence to requirements.

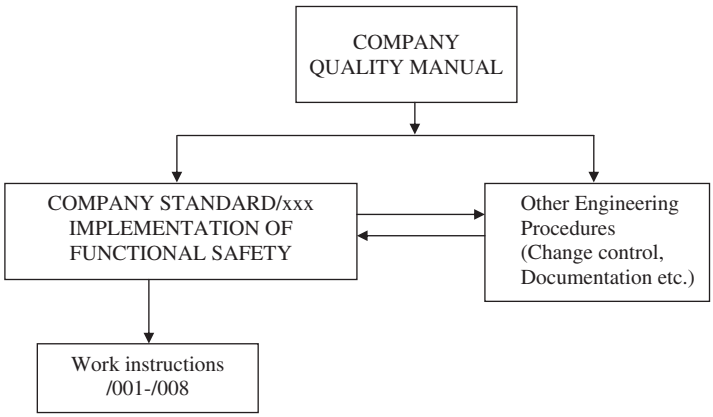
2 Scope

The standard shall apply to all products and documentation designed, produced, installed or supported by XYZ Ltd except where contract requirements specifically call for an alternative.

In the case of simple designs, and modifications to existing plant, these activities may be carried using in-house resources and skills. Larger projects may require the use of external resources.

Additional detail (to assist Project Safety Engineers or subcontractors) is supplied in Work Instructions/001 – /008.

The following diagram shows the relationship of relevant procedures:



3 Functional safety policy

Paragraph x of the Quality Manual emphasizes that capability in respect of functional safety is a specific design capability within XYZ Ltd. Some contracts will relate to safety-related applications. Some developments will specifically target safety-integrity conformance as a design requirement.

If the project is deemed to be safety-related then the Project Manager shall appoint an independent Project Safety Assessor. However, a project may be declared sufficiently minor that formal hazard identification is not required and that the remainder of this procedure need not apply. That decision will only be undertaken or ratified by the Company Functional Safety Manager.

In the case of minor modifications this review process is satisfied by means of the impact analysis which shall be recorded on the change request.

4 Quality & safety plan

Every project shall involve a Quality & Safety Plan which is the responsibility of the Project Manager. It will indicate the safety-related activities, the deliverables (e.g. Safety-Integrity assessment report) and the competent persons to be used. The Project Manager will consult the competency register and will review the choice of personnel with the Safety Authority.

The tasks are summarized in Section 5 of this standard. Minimum SR items required in the Quality & Safety Plan are shown in WI/007.

See also Appendix 7 of this book

5 Competencies

The HR department will maintain a "safety-related competence register" containing profiles of those individuals eligible to carry out functional safety assessment and design tasks. Periodically the Managing Director and Functional Safety Manager will review the list.

The list will be updated from:

Individuals' attendance at relevant off-the-job courses
Records of SR experience from each project (on-the-job training) (Project Managers will provide this information to the Personnel Manager)
Details of new employees or contractors.

Sample entry in the competency register

See Chapter 2 Figure 2.5 of this book

Examples of specific jobs involving SR competencies include:

Functional Safety Manager

The FSM will provide the company's central expertise in functional safety. He/she will have substantial experience in functional safety assessment and will be thoroughly conversant with IEC 61508 and related standards.

Safety Authority:

This role requires the ability to bring to a project all the expertise necessary to define functional safety requirements and to carry out the assessments. He/she will communicate between disciplines on functional safety issues. The individual may not possess all the skills involved but is required to understand sufficient of the methodology to be able to manage the process of sub-contracting all or parts of the work. In other words, the competency to make valid judgments of the subcontracted work is of the essence. A minimum of one day's "off the job" training with a competent course-provider is required. He/she shall resolve conflicts with his/her other roles in the project by liaising with the Company Functional Safety Manager.

Functional Safety Auditor

Functional Safety Audits are carried out by a person other than the Safety Authority for a project. He/she will have received the XYZ Ltd training course on Functional Safety. He/she will have had experience of at least one Safety-Integrity Assessment.

Lead Project Engineer

A Lead Project Engineer shall have a basic understanding of the requirements of IEC 61508 such as might be obtained from a one-day appreciation course.

For each project, the Project Manager (assisted by the Safety Authority) shall consult the competence register to decide who will be allocated to each task. In the event that a particular competence(s) is not available then he will discuss the possible options involving training, recruitment or subcontracting the task with the Managing Director.

Each individual on the competency register will participate in an annual review (generally at the annual appraisal) with his/her next level of supervision competent to assess this feature of performance. He/she will also discuss his/her recent training and experience, training needs, aspirations for future SR work.

6 Review of requirements and responsibilities

6.1 Source of the requirement

There are two circumstances in which an integrity target will arise:

> Arbitrary Requirement from a client with little or no justification/explanation
> An integrity target based on earlier, or subcontractor, assessments. In the event of this being greater than SIL 1, derived from some risk graph technique, then XYZ Ltd should attempt to ratify the result by means of quantified risk targeting.

6.2 Contract or project review

Where a bid, or invitation to tender, explicitly indicates a SR requirement (e.g. reference to IEC 61508, use of the term safety-critical, etc.) then the Sales Engineer will consult a Safety Authority for advice.

All contracts (prior to acceptance by XYZ Ltd) will be examined to ascertain whether they involve safety-related requirements. These requirements may be stated directly by the client or may be implicit by reference to some standard. Clients may not always use appropriate terms to refer to safety-related applications or integrity requirements. Therefore, the assistance of the Safety Engineering Manager will be sought before a contract is declared not safety-related.

A project or contract may result in there being a specific integrity requirement placed on the design (e.g. SIL 2 of IEC 61508). Alternatively, XYZ Ltd may be required to advise on the appropriate integrity target in which case/002 will be used.

6.3 Assigning responsibilities

For each project or contract the Project Manager shall be responsible for ensuring (using the expertise of the Safety Authority) that the safety-integrity requirements are ascertained and implemented.

Each project will have a Safety Authority.

The Project Manager will ensure that the FS activities (for which he carries overall responsibility to ensure that they are carried out) called for in this standard (and related procedures) are included in the project Quality & Safety Plan and the life-cycle techniques and measures document. Specific allocation of individuals to tasks will be included in the Quality and Safety Plan. These shall include:

Design & implementation tasks
Functional safety assessment tasks
Functional safety audits.

The Project Manager will ensure that the tasks are allocated to individuals with appropriate competence. The choice of individual may be governed by the degree of independence required for an activity, as addressed in section 10 of this standard.

7 Functional safety specification

Every project shall involve a Functional Safety Specification. This is outlines in WI/008.

See also Chapters 2 and 4 of this book

8 Life-cycle activities

The IEC 61508 standard essentially addresses six areas:

Integrity targeting
Random hardware failures
ALARP
Architectures (safe failure fraction)
Life-cycle activities
Functional safety competence.

The life-cycle activities are summarized in this section They are implemented, by XYZ Ltd, by means of The Quality Management System (to ISO 9001 standard) by means of this standard and the associated Functional Safety Procedures (/001-008).

8.1 Integrity targeting

This is addressed in Chapter 2 of this book. The company choice of risks etc. will be described here

SIL 3 targets may sometimes be required but, for reasons of cost, additional levels of protection will be suggested. SIL 4 targets will always be avoided since they involve unrealistic requirements and can be better engineered by having additional levels of protection.

SIL targeting shall be carried out by using a quantified risk approach rather than any rule based risk graph methodology. In the event of an existing risk graph based assessment the

Company Functional Safety Manager shall advise that a risk based approach is necessary for functions indicated as greater than SIL 1 and will provide Company expertise in that area.

8.2 Random hardware failures

This involves assessing the design, by means of reliability analysis techniques, to determine whether the targets can be met. Techniques include fault tree and logic block diagram and FMEA analysis, redundancy modeling, assessments of common cause failure, human error modeling and the choice of appropriate component failure rate data. Reliability assessment may also be used to evaluate potential financial loss. The process is described in/001 (Random hardware failures).

8.3 ALARP (As Low As Reasonably Practicable)

This involves testing risk reduction proposals when the assessment of random hardware failures indicates that the target has been met but not by sufficient margin to reduce the risk below the broadly acceptable level.

It is necessary to decide whether the cost and time of any proposed risk reduction is, or is not, grossly disproportionate to the safety benefit gained. This requires that a cost per life (or non-injury) saved criterion is in place. The process is described in/001 (Random hardware failures).

8.4 "Architectures"

In the context of IEC 61508 the term "architectures" refers to the safe failure fraction parameter (or 2_H data route) for which there are SIL-related requirements. It involves establishing, for each piece of safety-related instrumentation, the fraction of failures which are neither unrevealed nor hazardous. The process is described in/004 (Architectures & safe failure fraction).

8.5 Life-cycle activities

In some cases existing safety assessments will have been based on only Integrity targeting, Random hardware failures, ALARP and Architectures (safe failure fraction). The Company Functional Safety Manager should advise that this represents only a part of the spectrum of functional safety assessment.

Where the Company Functional Safety Manager has made the decision to include an assessment of life-cycle rigor then the activities necessary to demonstrate conformance to a SIL target are summarized, in tabular form, in/005 – Life-cycle activities. Reference to the evidence which satisfies each requirement will be entered in the tables. Justifications for alternatives or for "not applicable" status will be entered in the same way.

Operations and Maintenance involve key activities which impact on the achievement of the functional safety targets. Specific items include:

Implementation of the correct proof test intervals as per the assessments
Recording all proof tests and demands on SIS elements.

8.6 Functional safety capability

8.6.1 Audit

The company has an ISO9001 QA audit capability and shall carry out at least one audit per annum of the implementation of this procedure.

8.6.2 Changes

Control of modifications is an important aspect and requires that all change request documents specifically identify changes as safety-related or NOT safety-related. The change request document will contain a "safety-related/not safety-related" option, a space to record the impact of the change. This judgement must be ratified by the Safety Authority.

8.6.3 Failures

Failure/defect/hazardous incident recording requires that each is identified as safety-related or NOT safety-related. This judgement must be ratified by the Safety Authority.

8.6.4 Placing requirements onto suppliers

Instrumentation and field devices

There is a need to place a requirement upon OEM suppliers defining the hazardous failure modes together with an integrity (e.g. SIL or SFF) requirement.

System integrators

Where a safety-related sub-system (e.g. F&GDS or ESD) is procured then a "Functional Safety Specification" shall be placed on the system-integrator (i.e. supplier). It will state the hazardous failure modes (e.g. Fail to respond to a pressure input) and provide integrity targets to be demonstrated by the supplier. The integrity targets should be expressed (for each hazardous failure mode) either as SIL levels or as specific failure rates or probability of failure on demand.

8.7 Functional safety assessment report

Throughout the life-cycle there should be evidence of an ongoing assessment against the functional safety requirements. The assessment report should contain, as a minimum:

- Reason for the assessment
- Hazard and risk analysis if appropriate
- Definition of the safety-related system and its failure modes

- Calculation of target SIL
- Reliability models and assumptions, for example down times and proof test intervals
- Failure data sources and reliability calculations
- Findings of the qualitative assessment of life-cycle activities
- A demonstration of rigor such as is described in Appendix 2 of this book
- Appropriate independence.

9 Implementation

During design, test and build, defects are recorded on "Defect Reports". During Site installation and operations they are recorded on "Incident Reports", which embrace a wider range of incident.

Problems elicited during design review will be recorded on form xxxx. Failures during test will be recorded as indicated in STD/xxx (factory) and PROC/xxx (Site).

All defect reports will be copied to the Functional Safety Manager, who will decide whether they are SR or not SR. He will positively indicate SR or not SR on each report. All SR reports will be copied to the Safety Authority, who will be responsible for following up and closing out remedial action.

All SR incident reports, defect reports and records of SR system demands will be copied to the XYZ Ltd Functional Safety Manager, who will maintain a register of failures/incidents. A 6-monthly summary (identifying trends where applicable) will be prepared and circulated to Project Managers and Technical Authorities and Safety Authorities.

10 Validation

Validation, which will be called for in the Quality & Safety Plan and is specified in section 7.4a) of this standard, will involve a Validation Plan. This plan will be prepared by the Safety Authority and will consist of a list of all the SR activities for the Project, as detailed in this standard and related procedures.

The Safety Authority will produce a Validation Report which will remain active until all remedial actions have been satisfied. The Safety Authority and Project Manager will eventually sign off the report, which will form part of the Project File.

Annex A

Notes on the Second-level Work Instructions 001-008

Work Instruction xxx/001 – Random Hardware Failures & ALARP

Will describe techniques to be used (see Chapters 5 and 6 and Appendix 4 of this book).

Work Instruction xxx/002 – Integrity Targeting

Will describe techniques and targets to be used (see Chapter 2 of this book).

Work Instruction xxx/003 – Life Cycle Activities

Will capture the tables from Chapters 2, 3,4 and 8 of this book.

Work Instruction xxx/004 – Architectures (SFF)

Will describe the rules from Chapters 3 and 8 of this book.

Work Instruction xxx/006 – Functional Safety Competence

Will provide the tasks and register format – see Chapter 2 of this book.

Work Instruction xxx/007 – Functional Safety Plan

See Appendix 7 of this book.

Work Instruction xxx/008 – Functional Safety Specification

See Chapters 3 and 4 of this book.