THE CASS GUIDE

Guide to Functional Safety Capability Assessment

Accredited Certification to IEC 61508

While every care has been taken in developing and compiling this guidance document to support the CASS scheme, The CASS Scheme Ltd, the contributors and their parent organisations accept no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents except to the extent that such liability may not lawfully be excluded.

These technical schedules and guidelines are intended, as guidance only and any person or body using them should satisfy themselves as to the validity and correctness of their contents. The CASS Scheme Ltd accepts no responsibility for any loss or damage suffered by or to any person, body or thing arising out of the reliance or otherwise by any person or body on the guidance given by these technical schedules and guidelines in the interpretation of IEC 61508 or otherwise.

Where a product bears the CASS mark no assurance or warranty is given by The CASS Scheme Limited that the product is designed to operate to resist Acts of God, Force Majeure or Terrorist action.

Advices, interpretations and opinions are issued for guidance only and The CASS Scheme Limited accepts no liability for any loss or damage suffered by or to any person or thing arising out of the reliance or otherwise by any person or body on such address, interpretations or opinions issued from time to time.

Nothing set out herein shall seek to exclude or limit the liability of The CASS Scheme Limited for death or personal injury.

Marking ***CASS*** on or in relation to a product is a claim by a manufacturer or user that the product has been manufactured or is being used (as appropriate) in accordance with the requirements of the standard. The accuracy of the claim is therefore solely the responsibility of the manufacturer or the user. Enquiries as to the availability of third party certification to support such claims should be addressed to The CASS Scheme Limited in the case of the ***CASS*** certification mark.

CONTENTS LIST

THE CASS GUIDE

GUIDE TO FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

A detailed Contents List is provided at the beginning of each Section.

Intentionally left blank

THE CASS GUIDE

GUIDE TO FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

SECTION ONE

PREFACE

CONTENTS LIST

THE CASS GUIDE

SECTION 1 – PREFACE

Acknowledgements

The guidance presented reflects the views of industry. The CASS Scheme Ltd, wishes to thank the following organisations for their valuable input to the competency scheme.

600 Lathes
ABB
Adranz
AEA Technology
Allbright & Wilson
Association for Instrumentation, Control, Automation (GAMBICA)
Association of British Certification Bodies (ABCB)
BKD Consultants Ltd
British Computer Society (BCS)
Civil Aviation Authority (CAA)
CSE International Ltd
DTI
EECS
Energy Industries Council (EIC)
Engineering Equipment & Material Users Association (EEMUA)
Eutech
Federation of Electronic Industries (FEI)
Fresco Interest Group
Good Automated Manufacturing Forum (GAMP)
Health & Safety Executive (HSE)
HIMA Sella
HM Railway Inspectorate (HMRI)
Honeywell Control Systems Ltd
HSE
ICI Engineering Technology
ICI North Tees
ICS Triplex
Ideo
Industrial Automation & Control Division, Honeywell
Institute of Chemical Engineers
Institute of Measurement & Control
Institute of Railway Signaling Engineers
Institution of Electrical Engineers
Institution of Gas Engineers
IRSE
Jacobs Engineering Ltd
Kvaerner Oil & Gas
Lloyds Register
Machine Tool Technologies Association (MTTA)
Michael Hamlyn Associates
Moore Process Automation Solutions
Motor Industry Research Association (MIRA)
M W Kellogg Ltd
National Engineering Laboratories
National Quality Assurance Ltd
NQA
Pilz
Praxis Critical Systems
Railtrack
Railway Industries Association (RIA)
Rotork Instruments
Safety & Reliability Society
Salem Automation

Shell Expro
SI Process Control Ltd
SIRA Certification Services
Supervisory & Industrial Process Control
Technis (for IgasE & SaRS)
UK Hazards Forum
UKAS
United Kingdom Offshore Operators Association (UKOOA)
Virkonnen
Yokogawa

Preface

This document is presented in three sections. This section (Preface) contains background material relevant to the understanding and application of the CASS Scheme. The second section (Common Schedules) presents the Common Technical Schedules which should be applied to all assessments undertaken under the CASS Scheme Ltd. Technical Schedules which are specific to the conduct of a Functional Safety Capability Assessment are presented in the third section (FSCA TS). Related CASS Guides are listed in Preface : Table 1.

A brief history

Since the mid 1980's industry has placed increasing reliance on programmable safety-related systems, but at the same time concerns have been expressed in many quarters about the risks arising from the increasing use of programmable electronic systems in control and protection.

The initiative for the development of the CASS scheme arose from a series of closely coupled programmes supported by both the DTI (Department of Trade & Industry) and the Health and Safety Executive and implemented over the last twenty years. Pressure increased for research into certification primarily of people, but also discussions centred on certification of products, processes and development organisations. The emphasis was on particular ways of developing software. Industry viewed this as constraining them and not necessarily likely to lead to safer systems. An all sector working party (associated with a DTI sponsored IEE-BCS study) recommended deferring certification pending more research. It also recommended support for the development of IEC 61508, Functional Safety: Safety Related Systems, in order to establish and harmonise best practice across sectors.

1990 saw the launch of the Safety Critical Systems Advanced Technology Programme supported by DTI and EPSRC who wished to open markets in safety-related systems and software. Significant differences between traditional sector-specific approaches to safety management were fragmenting the supply-side, constraining purchasers' choice, and inhibiting diffusion of best practice.

During 1991 the potential for an R&D project specifically addressing conformity assessment and certification was discussed. This led to the approval of the FRESCO (Framework for the Evaluation of Safety Critical Objects) project in 1993 which specifically addressed certification of safety related systems to IEC 61508. FRESCO established an Interest Group for the process industries (FRESCO Interest Group, FIG). This group consisted of end-users, suppliers, design contractors, system integrators and regulators drawn from the UK chemical and pharmaceutical sectors. The Group, augmented by representatives from other industry sectors, recommended development of a conformity assessment scheme-based on IEC 61508.

This recommendation differed from those made earlier in that it was proposed by those who would be assessed rather than those with an interest in assessing others, or those with an interest in promoting particular technical solutions. It was also motivated by business drivers concerned with opening markets, and reducing the cost of compliance, rather than imposition of technical constraints focused on product and system safety or compliance with process standards.

During 1992 the DTI sponsored a study conducted by Coopers and Lybrand, focused on the characteristics of the market for safety-related computer controlled systems. The purpose of the study was to describe how the market was operating, to provide quantification of its key features and to identify any impediments to the effective operation of the market. The study identified that competitive advantage may well accrue to those suppliers who were able to transcend application specific

boundaries whilst maintaining the integrity of their systems. This seemed more likely to be achieved where there exist on a recognised third party testing and validation process, especially for relatively low value products with significant sales potential.

Following the success of FRESCO, in 1996 a further study commissioned by the DTI confirmed the feasibility of developing an accreditable conformity assessment scheme based on IEC 61508.

This led to the CASS project, which commenced in 1998 and was supported by the DTI under its Sector Challenge Programme. It secured strong industry support from all the major UK supply chain trade associations and stakeholder groups, the professional institutions, the Health & Safety Executive and from organisations with strong technical capability in the design and assessment of safety systems. This wide support has provided sound strategic direction, technical input, witnessed dissemination and continuous feedback. The deliverable was the development and conformity assessment scheme for safety-related systems based on the international standard IEC 61508, thereby facilitating the opening of markets, improving UK competitiveness, reducing costs of compliance and improving safety.

Introduction

The main challenges faced by industry are unremitting pressures to reduce costs coupled with shorter product lifecycles, a need for every quicker time to market, and pressure to maximise the use of the asset base. Industry continually strives to improve performance and profitability while maintaining and improving safety. In addition, there is a regulatory and social requirement for safety and reliability.

Against this background, industry is experiencing a revolution in the safety technologies, which themselves continue to rapidly evolve. Increasing reliance is placed on ‘smart’ equipment, integrated control and safety solutions, reusable safety components and sub-systems.

Whilst it is important therefore to fully exploit this modern technology to facilitate improvements in both safety and economic performance, it needs to be undertaken within an overall safety framework. Such a framework includes the use of recognised safety standards and competent assessors, coupled with a credible and industry acceptable conformity assessment regime.

CASS (Conformity Assessment of Safety-related Systems) is the initiative that provides this framework and whose objective is the development of a conformity assessment scheme meeting the requirements of IEC 61508. CASS will open up markets, improve competitiveness, reduce costs of compliance and improve safety.

The CASS Initiative

Certification to IEC 61508 has not been consistent, world-wide. The CASS scheme has been developed by the whole industry, with representatives from all interested sectors, to provide a rigorous and internationally acceptable structure under which consistent certification of safety-related systems can take place.

One of the key features of the CASS scheme is that to encourage European and international recognition it should be operated in accordance with the European and international standards for accreditation. Thus the scheme provides for competition between assessment and certification providers, and even between accreditation authorities, but through the CASS scheme rules, the EN45011 and ISO Guide 65 accreditation standards and international mutual recognition agreements transparency and a ‘level playing field’ can be assured.

CASS is governed by a company limited by guarantee, The CASS Scheme Ltd, that sets and operates the rules of CASS for the benefit of industry, and has Members representing all interested parties.

As a result of certification under the CASS scheme, there will be available on the market, certified equipment and processes available to users of safety systems, in which they can have confidence.

Purpose of CASS

The purpose of the CASS Scheme is to provide a structure so that third party accredited certification bodies can offer conformity assessment certification for safety related products that meets the requirements of IEC 61508. The scope of the scheme will cover all those involved in the design, development, manufacture, implementation, support and application of software components and complete systems, across many sectors. It will cover both off-the-shelf products and application specific products and the operation and maintenance of systems.

The benefits of the scheme are that it will:

- Enhance confidence in the safety of complex E/E/PES systems through the availability of an accredited assessment standard
- Reduce procurement costs by facilitating the re-use of assessed product
- Reduce long term operational and capital costs by facilitating the use of a building 'block approach' using certified components with recognised safety characteristics
- Reduce design and development costs for systems that utilise these components
- Generate increased end-user confidence in current and emerging technologies than can offer flexibility and cost reductions without compromising safety
- Promote international trade in certified equipment by providing manufacturers with independent and internationally recognised endorsement of their product
- Provide a yardstick to national regulatory authorities assessing 'fitness for purpose' and best practice of installed systems
- Generate a pool of assessors recognised as competent to undertake assessments in this field.

CASS relies on formal accreditation to EN45011/ISO guide 65, and will be certified through accredited certification bodies, thus ensuring international credibility and confidence.

Framework of CASS Assessment types

Within CASS there are five assessment types covering:

Type 1 Application independent (Component assessment) - covers the assessment of the functional safety achieved by components or software products that are independent of the application, and sold as a generic product.

Type 2 Application Specific products - covers application specific assessments of electrical, electronic, and programmable electronic systems that have been configured for a given application to perform a specific task. Type 2 is applicable to those organisations who have responsibility for the configuration/integration of components and sub-systems in order to deliver the safety system to the end user.
It has two sub-types:

a. Integrated system assessment is typically for bespoke installations.
b. Sub-system assessment is typically for a part of an integrated system built from supplied components such as input interfaces, logic solver and output interfaces, normally without sensors or actuators.

Type 3 Operations and Maintenance Assessment - covers assessment of operations and maintenance regimes for the safety related system. It is most suited to those organisations who are responsible for the operations and maintenance of the safety system, typically the end user/operator. It includes the policy, procedures, documentation and records of all activities concerned with maintaining functional safety for an installed and operating E/E PES.

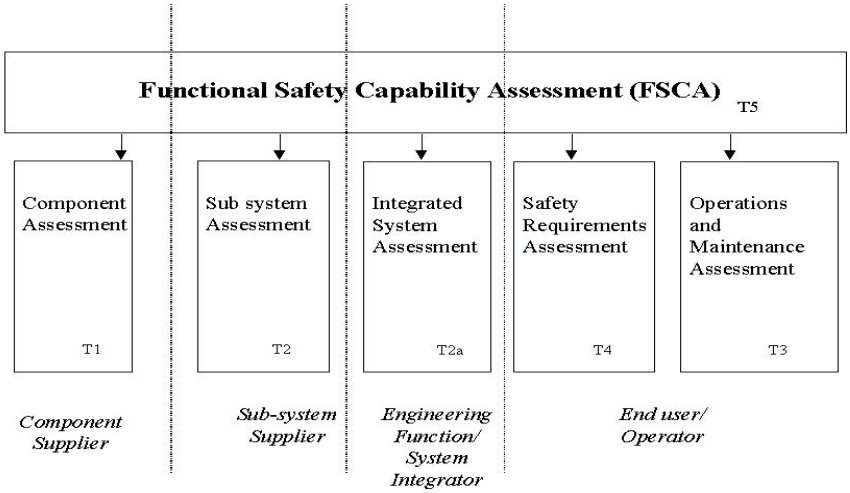
Type 4 Safety Requirements Assessment - covers assessment for the requirements capture, hazard and risk analyses for an application specific safety system. Typically it applies to the operator who is procuring the system.

Type 5 Functional Safety Capability Assessment (FSCA) - is the assessment of an organisation's functional safety capability. It relates to the processes not to individual products and systems, and is common to many sectors such as engineering organisations, end users, system integrators and SME's. Technical schedules and material for assessors is now available, covering Safety Capability Reviews, Safety Capability Audits, and Competence Audits.

A FSCA ensures that there is a management system of policy, processes and procedures which, if followed is capable of producing functional safety systems to a defined Safety Integrity Level (SIL). A FSCA overarches the other assessment types, and demonstrates the capability of delivery. The other four assessment types show approval of a specific product or system.

RELATIONSHIP BETWEEN CASS ASSESSMENT TYPES

Figure 1.



Certification and Scheme Management

Figure 2 provides an overview of the operation of the CASS scheme.

The CASS Scheme is a product/process certification scheme. Certification Bodies will obtain accreditation under EN 45011 to certify CASS from their national accreditation body (e.g. UKAS for the UK). Their scope will be defined according to the experience of their assessors. To ensure a consistent approach internationally, Certification bodies are required to work to the rules of the CASS scheme operated by The CASS Scheme Ltd.

CASS is governed by a company limited by guarantee, The CASS Scheme Ltd, that sets and operates the rules of CASS for the benefit of industry, and has Members representing all interested parties. It has a Governing Body who are responsible for the day to day management of the company.

The CASS Scheme Limited will be responsible for the development of further assessment types and ensuring that the technical schedules fully reflect the needs of industry. In order to achieve these objectives, technical committees and technical development teams will be established.

The feedback loop will be established to ensure that both UKAS and the accredited certification bodies have the opportunity to provide constructive feedback on the actual operation of the scheme.

Accredited certification bodies will operate in accordance with the CASS scheme rules.

Operation of the scheme

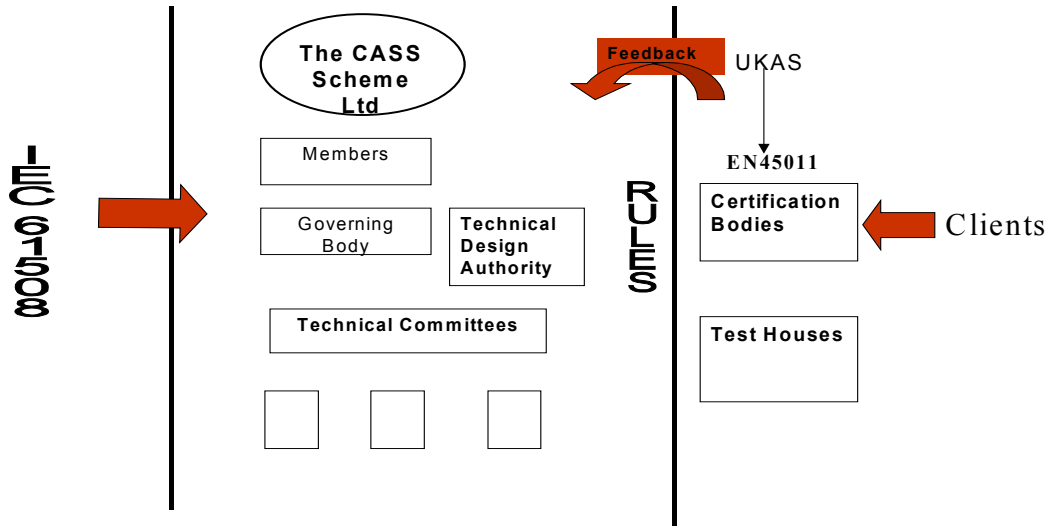


Figure 2.

Assessor competence

CASS assessors will operate through accredited certification bodies and will work to their procedures. Registration as a CASS assessor applies to an individual and need not be tied to employment by a certification body or other employer.

There is one grade of CASS assessor.

In addition the scope of an assessor will be defined by their experience in the industry sector.

The CASS Scheme Ltd will initially co-ordinate the assessor competency process. This will comprise processing the applications, arranging interviews and maintaining a list of registered assessors. Interviews will be conducted by an impartial panel of experts working to defined CASS procedures.

Document Structure of the CASS Scheme

This note outlines the documentation structure for the CASS Scheme documentation.

MAIN TITLE	SUB TITLE	COMMENTS
The CASS Scheme Ltd.	CASS Memoranda of Association	Registered with Companies House
	CASS Articles of Association	Registered with Companies House
	CASS Scheme Rules	Registered with Companies House
	Overview of Assessor Comptency	Contained in The CASS Assessor Framework
	Assessor Registration & Interview Process	Contained in The CASS Assessor Framework
	Guidance for Interviewers	Contained in The CASS Assessor Framework
	Accredited Certification Body Requirements	Contained in The CASS Assessor Framework
	CASS Scheme overview	
COMM CASS Scheme Common Schedules	Chapter 1 : Common Schedules Assessment Procedures	**Contained in this document**
	Chapter 2 : Common Schedules Assessment techniques	**Contained in this document**
	Chapter 3 : Common Schedules Guidance notes	**Contained in this document**
	Chapter 4 : Glossary	**Contained in this document**
FSCATS CASS Scheme Technical Schedules for Functional Safety Capability Assessments (FSCA)	Chapter 1 : FSCA Schedules Mapping tables	**Contained in this document**
	Chapter 2: FSCA Schedules Assessment criteria	**Contained in this document**
	Chapter 3: FSCA Schedules Assessment modules	**Contained in this document**
	Chapter 4: FSCA Schedules Targets of evaluation	**Contained in this document**
CASS Scheme Technical Schedules for Application Specific Assessments (Type 2)		To be launched
CASS Scheme Technical Schedules for Operations and Maintenance Assessments (Type 3)		To be launched
CASS Scheme Technical Schedules for Components (Type 1)		To be launched
CASS Scheme Technical Schedules for Safety Requirements (Type 4)		To be launched

Assessment Model Structure

The overall assessment model structure is shown below in figure 3:

Overall Assessment Model Structure

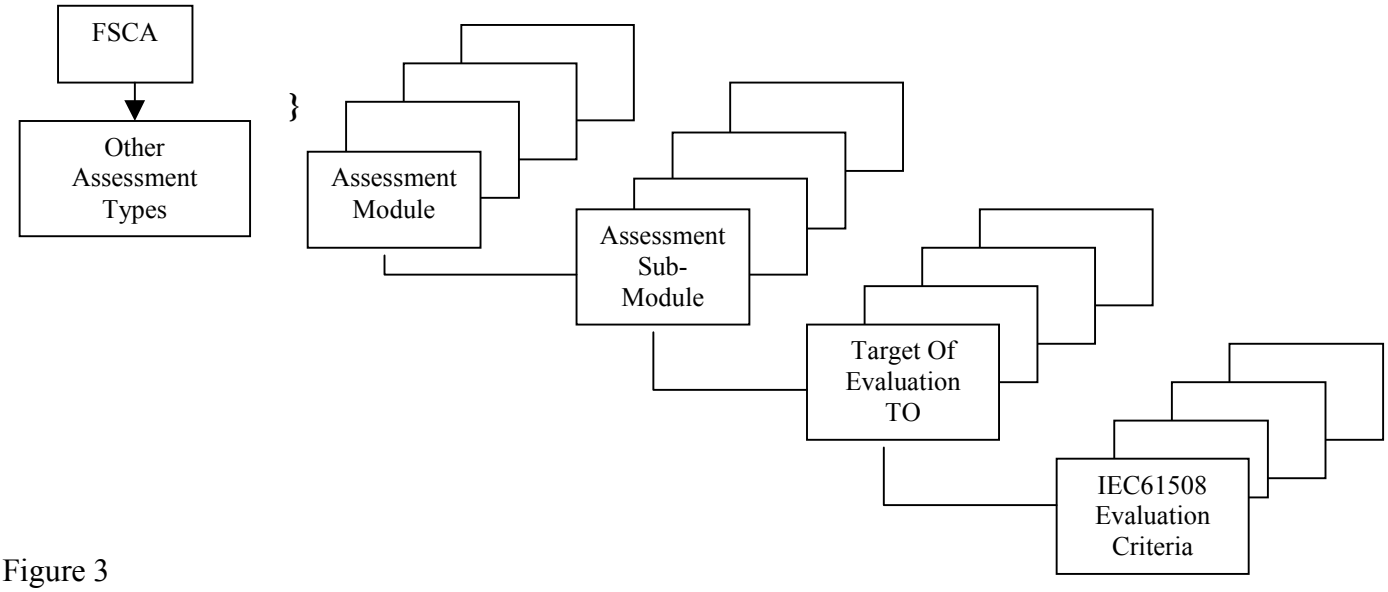


Figure 3

Each CASS assessment type follows the same structure where the assessment is divided into sub-modules. Each sub-module is further divided into Targets of Evaluation (TOE), where each TOE has evaluation criteria against IEC 61508.

The detailed description of the breakdown for FSCA is shown in Section 3 (FSCATS), Chapter 3.

Intentionally left blank

THE CASS GUIDE

GUIDE TO FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

SECTION TWO

COMMON SCHEDULES

CONTENTS LIST
CASS - COMMON SCHEDULES

CASS - COMMON SCHEDULES
CHAPTER 1 : ASSESSMENT PROCEDURES

1.1 INTRODUCTION

This chapter defines the assessment process and the procedures that an assessor is to follow for a CASS assessment.

IMPORTANT NOTE:

In the assessment procedures, items in **bold** are mandatory requirements of the CASS scheme, items in normal typeface are recommendations of the CASS scheme and items in *italics* are guidance material only.

1.2 SCOPE

The procedures described here are applicable to all types of CASS assessments. Acknowledgement is given to the DTI/SERC sponsored project Framework For The Evaluation of Safety Critical Objects (FRESCO) especially deliverable 'Development of the FRESCO technical approach', ref 5261/FDL/1, issue 1.0, May 1996. Much of the material here builds on deliverables produced by the FRESCO project.

1.3 CASS ASSESSMENT PROCEDURES

The CASS common assessment procedures are provided in CAP 01 to CAP 17 below.

1.3.1 LIST OF ASSESSMENT PROCEDURES

Procedure Number	Procedure name
01	CASS assessment process model
02	Establishing assessment requirements
03	Specifying a CASS assessment
04	Planning a CASS assessment
05	Performing a CASS assessment
06	Concluding a CASS assessment
07	Mapping document checks
08	Reviewing Assessment module reports
09	Preliminary Assessment reports
10	Final Assessment reports
11	Raising non-compliances and observations
12	Recognising current certifications
13	Metrics
14	On-going assessments
15	Assessment report format
16	CASS Certificates
17	Assessment Scope

1.3.2 LIST OF DOCUMENTS TO BE PRODUCED

Report	Procedure	Format
Assessment plan	CAP 04	Not specified
Preliminary assessment report	CAP 09	CAP 15
Final assessment report	CAP 10	CAP 15

The last two documents include findings from each assessment module.

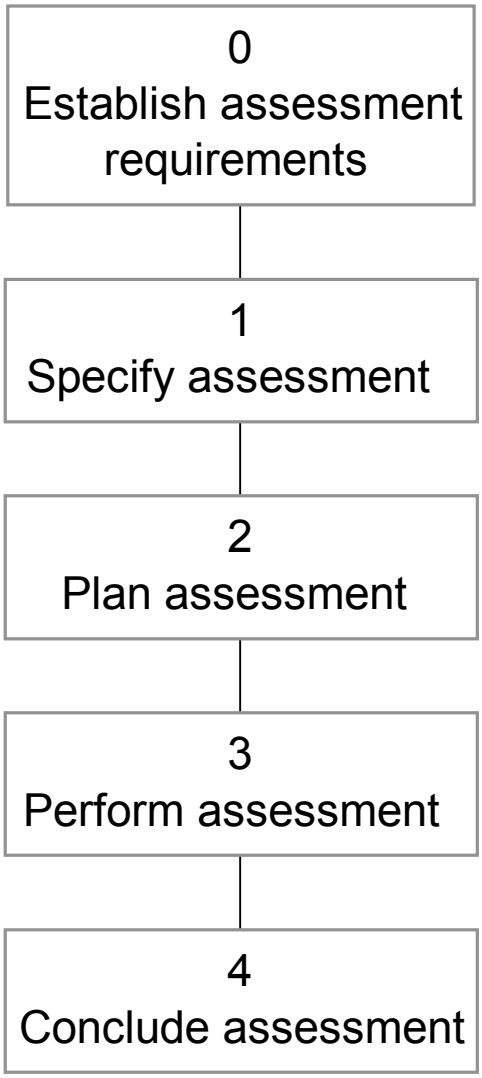
CAP01 CASS ASSESSMENT PROCESS MODEL

1. This procedure shows the overall process diagram of a CASS assessment.

2. It is the top-level road map to the main activities and deliverables of a CASS assessment. It cross references the other CASS assessment procedures contained in this manual to show where they are applicable in the assessment process. It does not describe the details of the assessment techniques or the assessment modules to be used.

CAP01 CASS ASSESSMENT PROCESS MODEL

ASSESSMENT PROCESS MODEL



CAP01 CASS ASSESSMENT PROCESS MODEL

CROSS REFERENCE TABLE OF ASSESSMENT PROCESSES TO RELATED PROCEDURES

PROCESS	RELATED PROCEDURES	
	NUMBER	TITLE
0. Establish assessment requirements	CAP02 CAP17	Establishing assessment requirements Assessment scopes
1. Specify assessment	CAP03 CAP14	Specifying a CASS assessment Resubmission assessments
2. Plan assessment	CAP04 CAP07 CAP12	Planning a CASS assessment Mapping document checks Recognising current certifications
3. Perform assessment	CAP05 CAP08 CAP09 CAP11 CAP15	Performing a CASS assessment Reviewing assessment module reports Preliminary assessment reports Raising non-compliances and observations Assessment report format
4. Conclude assessment	CAP06 CAP10 CAP13 CAP15 CAP16	Closing a CASS assessment Final Assessment reports Metrics Assessment report format Certificates

CAP02 ESTABLISHING ASSESSMENT REQUIREMENTS

PURPOSE
To ensure the client requirements for assessment are defined, understood and agreed

NB: This procedure contains no mandatory provisions for CASS assessment providers. It is expected that, for a mature assessment scheme, the client requirements will be fully defined at the point of requesting a CASS proposal.

INPUTS
Draft client requirements

OUTPUTS
Assessment requirements
Mapping document
Request for a CASS Assessment

ACTIVITIES

1. Analyse the draft requirements so the following are understood:

a) the reasons for requesting the assessment;
b) the CASS assessment type;
c) whether the assessment should address any non-safety issues such as security, economic or environmental requirements;
d) applicable regulations or laws are defined;
e) any special issues affecting the conduct of the assessment such as confidentiality; legal ownership or security concerns;
f) the required integrity level of the safety functions;
g) for CASS assessment types other than FSCA, relevant details about the E/E/PES to be assessed, e.g. its application domain.

2. Document these into definitive requirements if not already done so.

3. Receive or prepare the Mapping document for the assessment. This must clearly indicate the relationships between client documents/records and CASS components. It may be presented as lists or as cross reference tables and should be to an adequate level of detail.

4. Agree the assessment requirements with the client.

NB: It is expected that in the majority of cases these activities will involve a site visit to conduct/agree the analysis and mapping.

CAP03 SPECIFYING A CASS ASSESSMENT

PURPOSE

To define the scope of the assessment and assessment criteria to be applied.

INPUTS

Assessment requirements
Assessment module definitions
CASS criteria
Mapping document

OUTPUTS

Assessment specification

ACTIVITIES

NB: The assessment provider's own commercial procedures should also be followed.

1. Receive and control the client's Request for Assessment and Assessment requirements.

2. Check that the assessment requirements are complete and consistent and identify any missing information that will be needed to prepare a proposal.

3. Confirm that the assessment provider is not involved as a consultant, or otherwise, in the design, manufacture, installation or supply of any E/E/PES specified on the application form. This may involve:

a) checking the relevant internal records;
b) checking with other relevant departments within the assessment provider;
c) enquiring with the client.

4. The guiding principle is that the assessment provider must be a disinterested party as far as the results of conformity assessment are concerned. In particular the assessment provider must not have been involved in its design or development.

5. If this principle is contravened, the applicant should be informed that a proposal cannot be submitted at this time. The applicant can be referred to an alternative assessment organisation.

6. If a decision to proceed is made, **appoint a Lead Assessor** who is to be responsible for the assessment.

CAP03 SPECIFYING A CASS ASSESSMENT

7. Define the Assessment specification from the Assessment requirements and the Assessment module definitions.

8. This must include the exact scope of the assessment - see CAP 17.

NB: The role of the assessment specification is to clearly define the criteria to be applied and the client system they will be applied to. Rather than list the criteria, they will be defined by the Assessment modules as these list the objects to be assessed and hence the individual criteria to be applied. It should not deal with the documentation supplied or attempt to plan the assessment.

CAP04 PLANNING A CASS ASSESSMENT

PURPOSE

To produce a Safety Assessment plan that documents the procedures and resources to be used to evaluate against the assessment specification.

To produce a CASS proposal that meets the client requirements

INPUTS
Mapping document
Assessment specification
Assessment techniques
Assessor competencies
Assessment module definitions

OUTPUTS
Outline Safety Assessment plan
Detailed Safety Assessment plan

ACTIVITIES

1. Analyse the specified Assessment module definitions with the mapping document to determine the assessment techniques to be used. This should take account of pre-defined assessment modules and techniques where relevant.

2. Produce an outline Safety Assessment plan by:

a) Producing a work breakdown structure which partitions the assessment into separate tasks based around Assessment module definitions. Please note that on some assessments it will be preferable to assess the modules/sub-modules in a different order to that suggested in the description of the assessment modules. This re-ordering will be at the discretion of the Lead Assessor.

b) **Determine the most appropriate Assessment technique(s) to be applied.**

c) **Assign assessment team based on Assessor competencies** especially with respect to the Safety Integrity Level of the E/E/PES.

d) Produce an assessment schedule based on the work breakdown structure, the availability of resources (including assessment team, assessment tools and computers).

e) Identify key milestones in the assessment schedule.

3. Where the E/E/PES development is not yet complete, access to the development plan and schedule will be required to produce the Safety Assessment plan.

CAP04 PLANNING A CASS ASSESSMENT

4. Review and agreement by the client of the outline Safety Assessment Plan. This is to ensure access to the required client information and staff is possible.

5. Rework outline Safety Assessment plan into the detailed Safety Assessment Plan to eliminate any duplication of assessment activities. **Review and issue the detailed Safety Assessment plan.**

CAP05 PERFORMING A CASS ASSESSMENT

PURPOSE

To obtain results from evaluating the assessee material against the criteria in the Assessment specification using the techniques and tools planned in the assessment plan

INPUTS
Assessment plan
Assessment tools
Assessee material
Assessment module definitions

OUTPUTS
Assessor logs
Assessment module reports
Preliminary Assessment report

ACTIVITIES

1. **Manage the information supplied by the client**. This may involve formal configuration management and should account for client confidentiality requirements

2. **Apply the assessment criteria using the techniques and tools defined in the Assessment plan. See CAP11 for details of how to raise non-compliances and observations.**

3. Manage the data produced by assessment activities. This includes Assessor Logs and the preparation of Assessment module reports

4. Manage the tools used for the assessment

5. **Where site visits are necessary for assessment actions the activities should be subject to the same controls including protection of client confidentiality**.

6. All assessment findings should be reviewed by at least one person not directly involved in the assessment action concerned.

7. **Prepare and review the Preliminary Assessment report.**

CAP06 CONCLUDING A CASS ASSESSMENT

PURPOSE

To review and issue the Final Assessment report and to dispose of assessment data.

INPUTS
Preliminary Assessment report

OUTPUTS
Final Assessment report
CASS Certificates
Assessment metrics

ACTIVITIES

1. **Issue the Preliminary Assessment report to the client**.

2. Obtain client comments on the report and include these in a specific section in the report.

3. **If there are no major non-compliances, prepare a CASS certificate**.

4. **Review and issue the Final Assessment report to the client**.

5. **Prepare required metrics of the assessment and issue to The CASS Scheme Ltd.**

6. Close down assessment by returning, archiving or disposing of client supplied information as necessary.

CAP07 MAPPING DOCUMENT CHECKS

1. The Lead Assessor checks the supplied Mapping Document according to:

a) Whether of not the assessment is FSCA
b) For non-FSCA, whether documentation has been supplied with the request for CASS assessment
c) For non-FSCA, whether the E/E/PES development is complete or not.

EITHER FSCA, OR (for non-FSCA) SYSTEM DOCUMENTATION SUPPLIED WITH APPLICATION, DEVELOPMENT COMPLETE.

2. If the Mapping Document has not been supplied with the Request, the client should be asked for a completed table or a visit made to complete one.

The Lead Assessor checks that:

a) the supplied documents match up with the references given in the Mapping Document table
b) **the supplied documents relate to the Functional Safety Management System or E/E/PES version specified on the application form;**
c) **the Mapping Document table is accurate in so far as entries in the table are correct (the completeness of the entries in the table should not be considered at this stage).**

3. The Lead Assessor should sign and date the Mapping Document table to indicate that the above checks have taken place.

4. If there are too many anomalies with the supplied documentation arising from the checks to prevent the assessment progressing, the client will be informed of this fact and corrective action suggested.

NON-FSCA, NO SYSTEM DOCUMENTATION SUPPLIED WITH APPLICATION, DEVELOPMENT COMPLETE.

5. A site visit will be necessary to check the documentation to be supplied.

6. If the Mapping Document has not been supplied with the Request, the client should be asked for a completed table or this can be completed during the site visit.

CAP07 MAPPING DOCUMENT CHECKS

7. The purpose of the visit, from the assessment providers point of view, is to check the sources of evidence for satisfaction of the assessment criteria. Hence the client will need to make available all relevant documentation during the visit.

8. **During the visit, the Lead Assessor should perform the checks outlined above.** Any remaining visit time should be spent ascertaining the general quality of the documentation and discussing the assessment with the client.

9. The Lead Assessor should sign and date the Mapping Document table to indicate that the above checks have taken place.

10. If there are too many anomalies with the supplied documentation arising from the checks to prevent the assessment progressing, the client will be informed of this fact and corrective action suggested.

NON-FSCA, SYSTEM DEVELOPMENT NOT YET COMPLETE.

11. A site visit will be necessary to check the documentation to be supplied.

12. If the Mapping Document has not been supplied with the Request, the client should be asked for a completed table or this can be completed during the site visit.

13. The purpose of the visit, from the assessment providers point of view, is to check the sources of evidence that will be generated by the development for satisfaction of the assessment criteria. Hence the client will need to make available all relevant planning and procedural documentation during the visit.

14. **During the visit, the Lead Assessor should perform the checks outlined above on any extant documentation.** The Lead Assessor should then discuss E/E/PES development and assessment with the client, with a view to ascertaining the future schedule of client deliverables. It must be clear what is expected of the client during the remainder of the assessment, particularly in terms of documentation yet to be produced.

15. The Lead Assessor should sign and date the Mapping Document table to indicate that the above checks have taken place.

16. If there are too many anomalies with the supplied documentation arising from the checks or with the schedule of future deliverables to prevent the assessment progressing, the client will be informed of this fact and corrective action suggested.

17. For further guidance on mapping see Common Schedules Chapter 3.9

CAP08 REVIEWING ASSESSMENT REPORTS

1. This Procedure describes the procedures to be followed when reviewing a preliminary or final Assessment Report.

2. **It is the responsibility of the Certification Body to arrange a review of the preliminary and final Assessment Reports in accordance with the assessment provider's quality manual** by a person other than the author of the Report. Note that it is not the responsibility of the reviewer to repeat the assessment especially where this would involve extensive checking. Instead, it is expected that the reviewer will check the adequacy of the evidence that the assessor provides.

3. The reviewer should use the following review criteria.

a) The report is internally consistent and understandable.

b) The references to assessed documents are correct and complete.

c) Where criteria are said to pass or fail and specific instances are given to support the claim, the evidence is accurate and complete and any arguments used are valid.

d) Where criteria are said to pass or fail and this judgement is supported by sampling, the sample used is reasonable and the correct conclusions have been drawn from the sample.

4. If the consequences and necessary corrective actions for failed criteria are recommended then these recommendations shall be consistent with the circumstances of the assessment. Such recommendations must not amount to design consultancy.

5. The reviewer should examine the failed criteria in relation to each other and also in relation to failed criteria arising from other assessment modules, with a view to identifying common causes of failure. Any such common causes should be reported to the Lead Assessor who will make the whole assessment team aware of them, so that they might guide further assessment.

6. **Any comments the reviewer has should be recorded and implemented by the assessor, after discussion if necessary**. Any disagreements should be arbitrated in accordance with EN45011 requirements. When the review is complete, and the Assessment Report changed as necessary, the Lead Assessor should sign and date the Report.

CAP09 PRELIMINARY ASSESSMENT REPORTS

1. This procedure describes the content and reviewing of a CASS Preliminary Assessment Report

2 It is the responsibility of the Lead Assessor to produce the Preliminary Assessment Report.

3 The Preliminary Assessment Report should be written according to the format given in CAP 15. It will contain the following information:

- **Title;**
- **Contents page;**
- **Introduction;**
- **Type and scope of assessment;**
- **Assessment techniques;**
- **Assessment findings**
- **Conclusions**
- **Recommendations**

4 The Report should be reviewed and authorised by the Assessment Manager to ensure consistency of presentation and judgement, and by the Lead Assessor, at least in respect of those parts of the Report which were not produced by the Lead Assessor. The review may include other Assessors who are not directly involved in the assessment.

5 The reviewers should use the following review criteria.

a) The report is internally consistent and understandable.

b) The report is precise, avoiding the use of value judgements and qualifying adjectives.

c) The reporting style is objective and formal.

d) The references to assessed documents are correct and complete.

e) The report fulfils the requirements of the Assessment specification.

f) That all non-compliances reported in the Assessment Module Reports are included in the Assessment Report

CAP09 PRELIMINARY ASSESSMENT REPORTS

6 If the consequences and necessary corrective actions for failed criteria are recommended then these recommendations are consistent with the circumstances of the assessment.

7 Any comments the reviewers have should be recorded and implemented by the Lead Assessor, after discussion if necessary. When the review is complete, and the Report changed as necessary, the Assessment Manager should sign and date the report.

8 One copy of the Report will be sent to the client to allow them the opportunity to comment on its factual accuracy. The client should be informed that the assessment is based on submitted documents and that any comments should be confined to that scope. Typically a period of two weeks will be allowed for the submission of comments.

CAP10 FINAL ASSESSMENTS REPORTS

1 This Procedure gives guidance concerning the construction of the Final Assessment Report from the Preliminary Assessment Report and the client's comments, if any, on the Preliminary Assessment Report.

2 It is the Lead Assessor's responsibility to produce the Final Assessment Report.

3 The Final Assessment Report should have exactly the same structure as the Preliminary Assessment Report, except that it will contain additional sections as shown below:

a) Client comments
b) CASS certificate

4 The Lead Assessor should consider each of the client's comments and, if necessary, alter the Assessment Report accordingly. For each comment, the Lead Assessor should either record the changes made or the reasons why no change has been made. It may be appropriate to include the reasons in the Assessment Report. It may also be appropriate to inform the client why certain changes have not been made as requested.

5 The Lead Assessor should review the Conclusions and recommendations of the Final Assessment Report, after due consideration of whether or not the criteria are satisfied.

6 Where no major non-compliances have been raised, insert a CASS certificate against the assessment criteria (specified in the assessment scope) that were used.

7 Where major non-compliances have been raised, defer a CASS certificate (see CAP 16) until corrective action has been demonstrated during a resubmission assessment.

8 The Final Assessment Report should be reviewed by the Assessment Manager. In particular, the following review criteria should be used:

a) the response to each of the client's comments;
b) the overall findings of the assessment;
c) the date of the report correct;
d) the total number of pages correctly given on each page;
e) the table of contents updated correctly;
f) the summary of non-compliances changed, if necessary

9 Any comments the Assessment Manager has should be recorded and implemented by the Lead Assessor, after discussion if necessary. **When the review is complete, and the Report changed as necessary, the Lead Assessor and Assessment Manager should sign off the Report.**

CAP10 FINAL ASSESSMENTS REPORTS

10 One copy of the authorised Final Assessment Report should be sent to the client. If the client system has failed the Assessment, the client's attention should be drawn to the resubmission procedure. If the client wishes to appeal against the findings of the Final Assessment Report then attention should be drawn to the Appeals Procedure.

11 In particular, Re-submissions (see CAP 12) within three months of the date of publication of the Final Assessment Report will only entail re-assessment to the extent required to clear the non-compliances, unless other changes have occurred. The following forms should also be sent to the client:

a) An assessment of the extra work needed for re-assessment
b) A copy of a blank Mapping Document table

CAP11 RAISING NON-COMPLIANCES AND OBSERVATIONS

1. Two main aspects to assessment are those of existence and adequacy. These relate to whether the characteristic required by a criterion is actually present and, even if it is, that it is appropriately and adequately addressed.

2. Evaluating individual criteria

Evaluating against an individual criterion results in one of four types of finding. These will be referenced to the applicable clause of the criteria document used.

a) **Compliance**
this is where there is positive evidence that the criterion has been satisfied.

b) **Observation**:
this is where there is insufficient evidence for or against a criterion. It indicates either that there is a potential problem which cannot be unequivocally identified as a non-compliance or that the evidence may be found in future audits or document reviews. Observations are used to remind the assessor of some aspect of the assessment that will be checked at a later date.

c) **Minor non-compliance**:
this is where the evidence for a criterion is inadequate but where lack of evidence does not seriously compromise safety integrity. It is raised where there is evidence that the relevant feature of the client system generally meets the criterion but minor lapses have occurred. It indicates a product weakness typically manifested by isolated random examples of individual criteria not being met.

d) **Major non-compliance**:
this is where there is complete absence or inadequacy of evidence to meet the criterion. It is a deficiency which places safety integrity at risk and is usually a clear finding of features not properly established, not implemented or not being maintained.

Examples might be:
i) the absence of E/E/PES features specifically required by the assessment criteria;
ii) E/E/PES features which do not correctly address the requirements of the assessment criteria;
iii) the absence of design features which have a direct bearing on safety;
iv) major omission in the Functional Safety Management System.

CAP11 RAISING NON-COMPLIANCES AND OBSERVATIONS

3. Evaluating a ToE

A ToE is assessed by reviewing the individual criteria results and evaluating the overall result as one of the following:

a) Pass
this is where there are only positive findings or a small number of minor non-compliances.

b) Fail
this is where one or more major non-compliances have been raised or there are a number of minor non-compliances with, taken together, in the assessor's judgement constitute a major non-compliance.

c) Inconclusive
this is where the supplied documentation does not provide sufficient evidence for assessment against the criteria. It is typically raised where the number of observations mitigate against reaching a definitive evaluation result.

4. Evaluating an Assessment module result

The outcome of each Assessment module is assessed by reviewing the individual criteria results and evaluating the overall result as one of the following.

a) Pass
this is where there are only positive findings or a small number of minor non-compliances. Note that no non-compliances are allowed for a product assessment.

b) Fail
this is where one or more major non-compliances have been raised or there are a number of minor non-compliances with, taken together, in the assessor's judgement constitute a major non-compliance.

CAP12 RECOGNISING CURRENT CERTIFICATIONS

1. This procedure is to be followed if a client requests that current certifications or assessment reports from other schemes be taken into account during the assessment.

2. The Lead Assessor should obtain details of the existing certification including precisely what it was awarded to and for what is was awarded. This will then be passed to the Assessment Manager who will decide whether the certification can reasonably exempt the client from some or all of the assessment.

3. The Assessment Manager should consider the following criteria for deciding this:

a) the certification has been recognised by The CASS Scheme Ltd as from an equivalent assessment scheme;
b) the certification is for the same E/E/PES (for application-specific assessments);
c) the certification is for the same application;
d) the certification was against the same or equivalent criteria;
e) the certifying body complies with the EN45000 series of standards, or their equivalent.

4. The Assessment Manager shall record the exemption and report this to the CASS Executive for future comparative reference. The following minimum information shall be recorded:

a) current date
b) name of certificate issuing body
c) description of scope of certification
d) its number and date
e) any endorsements or exceptions
f) identification of the E/E/PES or Functional Safety Management System awarded the certificate
g) identification of the E/E/PES or Functional Safety Management System submitted for assessment
h) the Assessment modules being used for the assessment
i) details of the exemptions granted (i.e. which Assessment modules will not be evaluated)

CAP13 METRICS FOR APPLICATION-SPECIFIC ASSESSMENTS

1. This procedure describes the measurement information that should be recorded during a CASS Assessment. The purpose is to enable improvement of the whole assessment process.

2. It is the responsibility of the Lead Assessor to record the following information at the end of the assessment. This will mean the information will need recording for each Assessment module evaluation. Care should be taken to protect client and assessor confidentiality.

3. **It is the responsibility of the Assessment Manager to report that measurement information required by The CASS Scheme upon completion of the Assessment.** Note that this is a subset of the measurements shown below.

MEASUREMENT INFORMATION

Description of E/E/PES assessed system, including application sector
Size of system:
- **Number of I/O channels**
- **Number of processors**
- **Number of lines of source code (excluding comments)**
- **Percentage of system that is COTS**

Estimate of total size of system documentation assessed
- **Number of A4 pages**
- **Number of separate drawings**

Estimated/actual effort of assessment
- Number of man-days spent by assessors and client

Estimated/actual delivery date
- Date of issue of Final Assessment Report

Assessment type
Assessment team
- **Assessment provider**
- **Number of assessors**
- **Names of assessors**

Tools used
- **Number of assessment tools**
- **Names of assessment tools**

Assessment outcome
- **Description of assessment outcome**
- **Number of CASS certificate issued**

CAP14 ONGOING ASSESSMENTS

1. Introduction

This procedure gives guidance for assessments that are performed after an initial assessment. The types of on-going assessment are:

a) Surveillance assessment
b) Renewal assessment
c) Re-submission assessment.

The purpose, scope, timing, applicability and guidance for each of these assessments is given below. All on-going assessments are specified, planned, performed and concluded by following the basic assessment process model defined in CAP01.

2. Surveillance Assessment

Surveillances are to check the continued success and effectiveness of the process assessed. They have a reduced scope and depth with respect to the Initial Assessment by covering certain key aspects of the process, changes to the process structure and investigation of any open non-compliance or observations.

Surveillances are applicable to:
Functional Safety Capability Assessments (Type 5);
Operation and Maintenance Assessments (Type 3).

Surveillances are performed annually.

2.1 Guidance For Functional Safety Capability Surveillance Assessments.

a) Only the assessment modules: Functional Safety Audit and Competence Audit are performed.
b) It is mandatory to check the implementation and records for the following TOEs: 'Functional Safety Management System - Formal Reviews' and 'Corrective Action Procedure'.
c) It is mandatory to check any changes to the procedures defining the Functional Safety Management System in particular to the TOE: 'Organisation and Responsibilities'.
d) A sample check of each changed safety lifecycle activity should be done to its successful implementation.
e) A sample check of the remaining safety lifecycle activities should be done to confirm the overall continuing successful operation of the Functional Safety Management System. It is not necessary to sample each of these activities.
f) Open non-compliances and observations from previous assessments should be reviewed.

CAP14 ONGOING ASSESSMENTS

2.2 Guidance For Operation And Maintenance Surveillance Assessments.
TO BE DONE.

3. RENEWAL ASSESSMENT

Renewals are to reaffirm the operation and effectiveness of the process assessed. They have a similar scope to the Initial Assessment but require less depth of investigation as the process will be known and understood by the assessor. Renewals will cover all aspects of the process and will also include any changes to the process structure and investigation of any open non-compliance or observations.

Renewals are applicable to:
Functional Safety Capability Assessments (Type 5);
Operation and Maintenance Assessments (Type 3);
Component Assessments (Type 1) - production aspects only.

Renewals are performed triennially.

3.1 Guidance For Functional Safety Capability Renewal Assessments.

a) All the Functional Safety Capability assessment modules are performed.
b) It is mandatory to check each of the FSCA TOEs.
c) It is mandatory to check any changes to the procedures defining the Functional Safety Management System.
d) A check of each changed safety lifecycle activity should be done to confirm its successful implementation.
e) A check of each of the remaining safety lifecycle activities should be done to confirm the overall continuing successful operation of the Functional Safety Management System. Although each activity should be checked the sampling can be reduced based on previous successful performance of the activity.
f) Open non-compliances and observations from previous assessments should be reviewed.

3.2 Guidance For Operation And Maintenance Renewal Assessments.
TO BE DONE.

CAP14 ONGOING ASSESSMENTS

4. RESUBMISSION ASSESSMENT

Re-submissions are where the client has specifically addressed major non-compliances raised during a previous CASS assessment and requires the product or process to be reassessed. They have a reduced scope in that only the activities relevant to the non-compliances are checked. They will however cover all aspects relevant to the correction of the non-compliance and any preventive actions arising from this.

Re-submissions are applicable to all CASS assessment types.

Re-submissions are performed within 3 months of the major non-compliance being raised.

4.1 Guidance For Re-submission Assessments.

a) The corrective action for each non-compliance should be reviewed, verified and recorded.
b) For process assessments it is mandatory to check any revised or new procedures arising from the corrective action.

CAP15 ASSESSMENT REPORT FORMAT

1. This format is intended for the Preliminary and Final Assessment Reports.

TITLE

2. The standard title is 'Report on the Assessment of *xyz*'. The date of issue and a unique identification reference is stated and is repeated on each page of the report. The report is paginated with the total number of pages indicated on each page.

3. The name, signature and title of the Lead Assessor conducting the assessment and of the Assessment Manager are also inserted on the title page.

4. A Copyright notice will be included on the title page.

CONTENTS

INTRODUCTION

5. State the name and address of Assessment provider and indicate any accreditation of the provider.

6. State the name and address of the client and include the reference and date of the relevant Request for a CASS Assessment.

7. State that the report may not be reproduced whole, or in part, without written permission from the Assessment provider.

SCOPE OF ASSESSMENT

8. Identify exactly the name and version(s) of the system under assessment and the operating environments for which assessment is sought, including, for example, hardware and software platforms, and constraints on E/E/PES use (e.g. not in pharmaceutical applications).

9. Indicate the submission information inspected, usually by reference to a full list containing titles, identifiers, revision numbers and dates in an Annex.

10. List the assessment modules used for the assessment.

CAP15 ASSESSMENT REPORT FORMAT

11. List the existing certificates and reports which have resulted in exemptions, together with details of the exemptions.

ASSESSMENT TECHNIQUES

12. List the names of the assessors who performed the assessment.

13. Record the assessment techniques used.

14. List the names and versions of any assessment tools that were used.

SUMMARY OF ASSESSMENT FINDINGS

15. Record the date(s) of the assessment.

16. Summarise the non-compliances raised in each section of the assessment indicating the numbers found and the areas found deficient. Where no deficiencies were found, state that this is the case. Details of the non-compliances will be found in the internal Assessment Module Reports prepared by individual assessors.

CONCLUSIONS AND RECOMMENDATIONS

17. State the degree to which the client system has met the Assessment criteria.

CLIENT COMMENTS (final report only)

18. Include client comments raised on the Preliminary Assessment Report.

19. Indicate which comments have not been incorporated with reasons.

CERTIFICATE

20. Where no major non-compliances have been raised, include a certificate for the client system.

DETAILS OF ASSESSMENT FINDINGS

21. **There should be one Annex per assessment module. For each one, detail every non-compliance, observation or finding arising from the individual Assessment Modules**

CAP16 CASS CERTIFICATE FORMAT

1. This procedure describes the preparation of a CASS Certificate.

2. It is the responsibility of the Lead Assessor to prepare a CASS certificate. It is reviewed and approved by the Assessment Manager.

3. For a FSCA assessment, the certificate must contain the following information.

a) **CLIENT: address as per assessment Request.**

b) **ASSESSMENT CRITERIA: state the assessment standard(s) and the associated CASS criteria that were applied**.

c) **QUALIFICATIONS:** If minor non-compliances were raised then state that "permitted minor deviations from the assessment criteria are detailed in Assessment Report xyz".

d) **DATE OF ISSUE**: typically, same as the Assessment Report.

e) **CERTIFICATE NUMBER**: unique identifier of the certificate; typically, same as the Assessment Report.

f) **Functional Safety Management System and associated scope**

For a product assessment, the certificate must contain the following information.

g) **CLIENT: address as per assessment Request**

h) **E/E/PES: unique identified used for the E/E/PES**

i) **DESCRIPTION: brief description of intended use of the E/E/PES**

j) **OPERATING ENVIRONMENT: description of the required hardware/software operating environment, specific constraints on use and/or a reference to more detailed description in the Assessment Report**

k) **ASSESSMENT CRITERIA: state the assessment standard(s) and the associated CASS criteria that were applied**.

l) **QUALIFICATIONS:** If minor non-compliances were raised then state that "permitted minor deviations from the assessment criteria are detailed in Assessment Report xyz"

m) **DATE OF ISSUE**: typically, same as the Assessment Report

CAP16 CASS CERTIFICATE FORMAT

n) **CERTIFICATE NUMBER**: unique identifier of the certificate; typically, same as the Assessment Report

Typical example certificates are attached.

SPECIMEN CERTIFICATION STATEMENTS FOR CASS ASSESSMENT TYPES

SPECIMEN– FUNCTIONAL SAFETY CAPABILITY ASSESSMENT (TYPE 5)

CERTIFICATE OF APPROVAL
(SPECIMEN)

This is to certify that the Functional safety capability of:

Bravo Safety Systems Ltd.
1a, Poplar Walk
Croydon CR0 2AJ
United Kingdom

has been assessed with satisfactory results in accordance with the relevant requirements of the CASS scheme

The Functional Safety Management System is applicable to:
The specification, development and installation of programmable electronic shutdown systems for use in bulk chemical processing applications

ASSESSMENT CRITERIA: IEC 61508-1: 1998(part only),
IEC 61508-2: 1999
IEC 61508-3: 1998

ASSESSMENT MODULES APPLIED:
FUNCTIONAL SAFETY CAPABILITY incorporating all subordinate assessment modules. For detailed description, see assessment report R28073, issue 1.0, 29 April 1999.

Date: 29 April 1999 Certificate Number: 28073

SPECIMEN APPLICATION SPECIFIC ASSESSMENT (TYPE 2b)- SUB-SYSTEM

CERTIFICATE OF CONFORMITY
(SPECIMEN)

This Certificate is issued to:

Bravo Safety Systems Ltd.
1a, Poplar Walk
Croydon CR0 2AJ
United Kingdom

to declare the undernoted system has been assessed with satisfactory results in accordance with the relevant requirements of the CASS scheme

E/E/PES:
PLC SD001 version 1.0.3 with components listed in the Assessment Report.

DESCRIPTION:
Programmable electronic sub-system for a diverse emergency shutdown system for liquid fertiliser production plant

OPERATING ENVIRONMENT:
Organofox-2 production line at Alpha Chemical Co. liquid fertiliser plant. For detailed description, see assessment report R28072, issue 1.0, 29 April 1999.

ASSESSMENT CRITERIA: IEC 61508-2: 1999
IEC 61508-3: 1998

ASSESSMENT MODULES APPLIED:
SUB-SYSTEM incorporating all subordinate assessment modules. For detailed description, see assessment report R28072, issue 1.0, 29 April 1999.

Date: 29 April 1999 Certificate Number: 28072

SPECIMEN APPLICATION SPECIFIC ASSESSMENT (TYPE 2a) - INTEGRATED SYSTEM

CERTIFICATE OF CONFORMITY
(SPECIMEN)

This Certificate is issued to:

Alpha Chemical Co.
1, Poplar Walk
Croydon CR0 2AJ
United Kingdom

to declare the undernoted system has been assessed with satisfactory results in accordance with the relevant requirements of the CASS scheme

E/E/PES:
ESD ORG2-001, version 2.1 with sub-systems and components listed in the Assessment Report.

DESCRIPTION:
Diverse emergency shutdown system for liquid fertiliser production plant.

OPERATING ENVIRONMENT:
Organofox-2 production line. For detailed description, see assessment report R28071, issue 1.0, 29 April 1996.

ASSESSMENT CRITERIA: IEC 61508-1: 1998 (part only),
IEC 61508-2: 1999
IEC 61508-3: 1998

ASSESSMENT MODULES APPLIED:
INTEGRATED SYSTEM incorporating all subordinate assessment modules. For detailed description, see assessment report R28071, issue 1.0, 29 April 1999.

Date: 29 April 1999 Certificate Number: 28071

CAP 17 CASS ASSESSMENT SCOPES

1. INTRODUCTION

A CASS scope of approval has several uses:

a) Defines the activities to be assessed
b) Enables appropriate CASS assessor team selection
c) Defines exactly what has been approved
d) Defines the location of the activities (important for accreditation requirements)
e) Informs customers of CASS clients exactly what is covered by the approved Functional Safety Management System
f) Used by CASS clients to advertise the extent of the approval.

2. STRUCTURE OF SCOPES

A FSCA scope includes the following elements:

a) the assessment standard(s), currently IEC 61508;
b) the locations covered by the FSCA
c) the activities performed
d) the products or services provided
e) any clarifications and limitations to the scope

For CASS assessment types other than FSCA, it would contain:

a) identification of the E/E/PES by description; version number and any other relevant configuration information;
b) identification of the application environment which the E/E/PES is operating in (application dependent assessments only).

All scopes should list the Assessment modules that the E/E/PES will be assessed against.

All these elements should be clearly stated on the CASS certificate.

Scope statements should be consistently structured; be grammatically correct and be coherent. They should always be consistent with the scope of the CASS scheme and the assessment standard (currently IEC 61508). They must reflect the Functional Safety Management System under assessment and the activities actually covered during assessment.

Notes:

a) All the locations and the activities at those locations must be listed. For complex multi-site assessments these may be listed on a separate schedule.
b) The main activities referenced in the Safety Lifecycle are preferred where possible.
c) Generic terms for products should be used or trade names. A full list of all the products is not normally needed.
d) Service descriptions should reflect those stated in the clients Functional Safety Policy.

CAP 17 CASS ASSESSMENT SCOPES

e) 'Clarifications and limitations' are to make clear any restrictions on the approval which might reasonably be taken as included e.g. maximum integrity level of supplied systems.

3. FORMAT AND EXAMPLES

Scope statements should be formatted as follows:

ACTIVITY + PRODUCT /SERVICE + CLARIFICATION/LIMITATION

Examples are:

"The specification, design, installation and commissioning of programmable electronic shutdown systems for the petrochemical industry to a maximum target safety integrity of level 3"

"The independent verification of safety related software using static analysis tools for the transport and nuclear sectors"

"The specification, design, assembly and delivery of electronic and programmable electronic safety related systems for all industrial sectors"

CASS - COMMON SCHEDULES
CHAPTER 2 : ASSESSMENT TECHNIQUES

2.1 INTRODUCTION

This chapter contains procedures for applying techniques during a CASS assessment.

2.2 SCOPE

The procedures contained in this document are for use by CASS assessors and should be used in conjunction with IEC 61508, particularly the guidance in part 7.

General assessment techniques such as document inspection, audit visit and test witnessing are described in this issue of the document.

Future issues will cover detailed assessment techniques required by IEC 61508 for safety assessments. These include (brackets are the relevant sections of IEC 61508 part 7):

a) checklists (section B.2.5);
b) decision/truth tables (section C.6.1);
c) software complexity metrics (section C.5.14);
d) failure analysis for which the following techniques can be used
   - cause consequence diagrams (section B.6.6.2)
   - event tree analysis (section B.6.6.3)
   - fault tree analysis (section B.6.6.5)
   - failure modes effects and criticality analysis (section B.6.6.4)
   - monte-carlo simulation (section C.6.6)
e) common cause failure analysis (section C.6.3);
f) reliability block diagrams (section C.6.5).

Appropriate techniques should be selected according to the Safety Integrity Level. Guidance on this selection is given in the table below:

Assessment technique	SIL 1	SIL 2	SIL 3	SIL 4	Notes
Document inspection	HR	HR	HR	HR	
Process audit	HR	HR	HR	HR	
Test witnessing	R	R	HR	HR	Not for FSC Assessments (Type 5)
Checklists	R	R	R	R	
Decision/truth tables	R	R	R	R	Not for FSC Assessments (Type 5)
Software complexity metrics	R	R	R	R	Not for FSC Assessments (Type 5)
Cause consequence diagrams	R	R	HR	HR	Not for FSC Assessments (Type 5)
Event tree analysis	R	R	HR	HR	Not for FSC Assessments (Type 5)
FMECA	R	R	HR	HR	Not for FSC Assessments (Type 5)
Common cause failure analysis	R	R	HR	HR	Not for FSC Assessments (Type 5
Reliability block diagram	R	R	R	R	Not for FSC Assessments (Type 5

2.3 DOCUMENT INSPECTION

Document Inspection is a detailed review of planning, design or test documentation to determine whether there is conformance to the applicable assessment criteria. This technique is applicable to all types of assessment.

2.3.1 TIMING

This technique applies at any time during the lifecycle when formal documentation has been produced. Any type of document can be subject to this review including those stored electronically.

2.3.2 PLANNING

The Lead Assessor shall identify the document(s) to be inspected. The specific criteria against which the document will be inspected are also identified.

The Lead Assessor shall identify a suitable Assessor to perform the inspection. This Assessor will be from the assessment team unless specific knowledge is required which is not covered by the assessment team personnel.

The Lead Assessor shall issue an instruction to the Assessor to perform the inspection. This instruction shall contain:

a) identification of the document to be inspected;
b) the date and time for the inspection to be completed;
c) the estimated effort to be expended;
d) the specific criteria against which the document will be inspected.
e) how the findings of the inspection are to be recorded;
f) any process measurement data to be recorded.

2.3.3 INSPECTION

The Lead Assessor shall monitor the progress of the inspection reporting any problems or delays to the Assessment Manager.
The Assessor shall inspect the document against the specified criteria and record findings, non-compliances and observations. The document shall also be inspected for general issues like spelling, compatibility with other documents and understandability.

2.3.4 REPORTING

A document inspection report shall be prepared detailing the general purpose, scope and adequacy of the document. Any non-conformances against the specific criteria shall be noted with a cross-reference to where the non-conformance is located in the document.

Any process measurement data required shall be recorded after the document inspection report has been completed.

2.3.5 RECORDS

The following records shall be kept as part of the assessment record:
a) instruction to perform the document review;
b) assessor notes;
c) any non-compliances;
d) document inspection report.

2.4 PROCESS AUDIT

A Process Audit is a systematic and independent examination to determine whether safety activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve their objectives. This technique is appropriate for all types of audit.

2.4.1 TIMING

This technique can be applied at any time during the development lifecycle.

2.4.2 PLANNING

The Lead Assessor shall nominate the audit visit team.
An agenda shall be prepared to include, as a minimum:
a) the date and time of the audit visit;

b) the audit team;
c) any logistical needs;
d) the purpose and scope of the audit;
e) a proposed daily schedule.

This agenda shall be sent to the client.
Audit checklists to aid in the collection of evidence shall be prepared.

2.4.3 THE VISIT

An opening meeting shall be held at the start of the visit to confirm with the client:
a) the purpose and scope of the audit;
b) the practicality of the audit agenda;
c) the procedure for raising and agreeing non-compliances;
d) the reporting method.

Evidence shall then be collected and any deviations noted. It may be necessary to reschedule part of the audit as the audit progresses depending on what is found. Any changes to the agenda must be communicated to the client.

At the end of the audit visit, a closing meeting shall be held. This closing meeting shall include, as a minimum:
a) a summary of the general adequacy of the process;
b) any non-compliances and areas of concern, together with dates of corrective actions;
c) what happens next (including contact names and numbers).

2.4.4 REPORTING

An audit report shall be prepared detailing the general purpose, scope and findings of the audit.

Any process measurement data required shall be recorded after the audit report has been completed.

2.4.5 RECORDS

The following records shall be kept as part of the audit record:
a) audit agenda;
b) checklists;
c) assessor notes;
d) non-compliances;
e) audit report.

2.5 TEST WITNESSING

Test Witnessing is an independent examination to determine whether testing activities comply with planned arrangements and whether these arrangements are implemented

effectively and are suitable to achieve the test objectives. This technique is appropriate for all types of audit.

2.5.1 TIMING

This technique can be applied at any time during the testing lifecycle. However, it is more usual to perform test witnessing in the latter stages of the testing lifecycle.

2.5.2 PLANNING

The Lead Assessor shall nominate an assessor to take responsibility for the test witnessing. A timetable for the test witnessing shall be produced and shall include as a minimum:

a) the date, time and duration of the test;
b) any logistical needs;
c) resources required from the client to support the test witnessing;
d) purpose and scope of the tests;
e) the test plan/procedures(s) to be witnessed;
f) the schedule of tests.

This timetable shall be submitted to the client.
Audit checklists shall be prepared in order to aid the collection of evidence. Any non-conformances or follow-ups requested from previous audits should be clearly marked. Applicable test plans and procedures shall be reviewed to ensure familiarity when the test witnessing takes place.

2.5.3 PROCEDURE

An opening meeting shall be held at the start of the visit to confirm with the client:

a) the purpose and scope of the test witnessing;
b) the practicality of the test timetable;
c) the procedure for raising and agreeing non-compliances;
d) the reporting method.

The witnessing shall be performed according to the schedule. Any deviations from the schedule shall be recorded.

The test shall be observed and clarification sought on unclear areas, stopping the test if necessary. The conduct of the test shall also be observed, including the preparation of test logs and recording of faults.

The following information shall be recorded during the test witnessing:

a) the staff involved in the test;
b) any possible areas of weakness in the test procedure;
c) any positive evidence which contributes to the test procedure satisfying the assessment criteria;
d) the assessor's name;

e) date and location of the test witnessing.

At the end of the audit visit, a closing meeting shall be held. This closing meeting shall include, as a minimum:
a) a summary of the general adequacy of the testing;
b) any non-compliances and areas of concern, together with dates of corrective actions;
c) what happens next (including contact names and numbers).

2.5.4 REPORTING

A test witness report shall be prepared detailing the general purpose, scope and findings of the witnessing.

Any process measurement data required shall be recorded after the test witness report has been completed.

2.5.5 RECORDS

The following records shall be kept as part of the test witness record:
a) test witnessing timetable;
b) checklists;
c) witness notes;
d) non-compliances;
e) test witness report.

CASS - COMMON SCHEDULES
CHAPTER 3 : GUIDANCE

3.1 INTRODUCTION

This chapter contains guidance on the CASS Scheme.

3.2 SCOPE

The guidance contained in this document is to help organisations to achieve conformance to IEC 61508 using the CASS scheme and should be used in conjunction with IEC 61508, particularly part 7.

3.3 OVERVIEW OF ASSESSMENT TYPES

This section outlines the CASS 'assessment types'. Its primary purpose is to explain the rationale behind the relationship of assessment types to safety life-cycle phases, supply chain, EN45000 standards and competencies.

3.3.1 SOURCES/NOTES

Section 4 of the CASS User Requirements Specification defines the basic assessment types.

Each assessment type is explained using a 'base case' model which assumes a 'typical' assessment situation for the case. This is done only for explanation purposes only as it is expected that a variety of cases will arise and have to be dealt with.

3.3.2 CONCEPT OF THE V MODELS

In order to provide a wide spectrum of readers with the rationale for the selection of assessment types a series of 'V models' have been constructed (see Common Schedules: Figure 3.1). These are discussed below.

Whilst IEC 61508 provides a comprehensive safety life-cycle model with related methods and techniques it does not attempt to map the life-cycle to the concept of a typical industry supply chain. This is understandable as the standard is generic in nature. However, in presenting the CASS assessment types to a wide industry audience it is clear that some mapping of the assessment types to the concept of a supply chain is necessary, hence the CASS 'V model' concept which provides a relationship of safety life cycle to typical supply chains. This helps provide guidance to those organisations seeking assessment as to the most appropriate assessment types for their specific role(s) within the supply chain and/or system(s) developed, delivered and maintained. Mapping of IEC 61508 phases to the 'V model' assists organisations in determining, fairly easily, which specific phases impact upon their scope of supply and responsibilities, so assisting in their understanding and implementation of the standard.

During development of the CASS technical deliverables other closely related material has been developed within the industry, such as the IEE/BCS Safety, Competency and Commitment Guidelines. The CASS 'V model' concept provides an appropriate mechanism for mapping these core safety practitioner competencies to the 61508 life cycle phases.

In consultation with UKAS the 'V model' concept has been further enhanced to map the appropriate EN 45000 accreditation standards to the assessment types.

Common Schedules Figure 3.1 introduces the basic CASS 'V model'. It represents a typical industry (generic) supply chain model mapped to the traditional safety development life-cycle model.

A typical supply chain consists of an end user organisation whom both specify the system and also have responsibility for maintaining the system within an operations and maintenance regime. The actual maintenance activities and tasks may be sub-contracted but the end user or process owner still retains ultimate responsibility for the safety of the equipment under control (EUC).

Within many industry sectors engineering design contractor organisations have a significant role to play in total plant and safety systems engineering. In some cases these engineering activities may be implemented by the end user's own engineering functional group or external system integrators. The responsibility covers the integration and/or configuration of the end-to-end safety-related system consisting of sensors, logic solver and actuators. Such systems are application dependent.

The safety-related system consists of a number of sub-systems which can be sourced from a number of different sub-system suppliers, hence the horizontal partition 'sub-system supplier'. These sub-systems have typically been subjected to some configuration and are therefore application dependent

Finally at the lowest horizontal level those organisations supplying application independent components are represented.

CASS defines five basic assessment types:

a) Component assessment, often referred to as *application independent* and *proprietary (Type 1)*
b) Application specific system assessment, often referred to as application dependent (Type 2)
c) Operations and maintenance assessment of a specific safety related system (Type 3)
d) Safety requirements assessment (Type 4)
e) Functional safety capability assessment (Type 5)

Application specific assessment is further sub-divided into:

a) Integrated system assessment (Type 2a)
b) Sub-system assessment (Type 2b)

The concept of an organisational assessment of functional safety management is catered for by the Functional Safety Capability Assessment (FSCA) and is applicable to all organisations within the supply chain.

The O&M assessment (Type 3) is most suited to those organisations who are responsible for the operations and maintenance of the safety system, typically the end -user/operator or in some circumstances, engineering design contractors.

Application Specific assessments are applicable to those organisations who have responsibility for the configuration/integration of components and sub-systems in order to deliver the safety related system to the end user.

This leads to a mapping of the supply chain model to CASS assessment types. See Common Schedules Figure 3.2.

The ability to map the IEC 61508 life cycle phases to both the supply chain and CASS assessment types is beneficial in that it assists those organisations in preparing for a CASS assessment. In particular identifying and mapping the *'targets of evaluation'* to IEC 61508 phases and relating these targets to the assessment type selected.

It also enables an organisation to more easily relate its roles and responsibilities within the supply chain, possibly sector specific, to the phases of the standard and hence identify the activities and deliverables it is expected to undertake and provide. See Common Schedules Figure 3.3.

The IEE/BCS Safety, Competency and Commitment guideline has identified a set of twelve competency functions which map to IEC 61508. These core competency functions are:

a) C1 Corporate Functional Safety Management (CFM)
b) C2 Project Safety Assurance Management (PSM)
c) C3 Safety-Related System Maintenance (SRM)
d) C4 Safety-Related System Procurement (SRP)
e) C5 Independent Safety Assessment (ISA)
f) C6 Safety Hazard and Risk Analysis (HRA)
g) C7 Safety Requirements Specification (SRS)
h) C8 Safety Validation (SV)
i) C9 Safety-Related System Architectural Design (SAD)
j) C10 Safety-Related System Software Realisation (SSR)
k) C11 Safety-Related System Hardware Realisation (SHR)
l) C12 Human Factors Safety Engineering (HF).

An integral part of any CASS assessment is an assessment of individual and team competencies.

To assist organisations in interpreting the HSE competency functions in relation to their own organisational competency models and understanding the relationship of the twelve

competency functions to CASS assessment types the following model is provided. See Common Schedules Figure 3.4.

In developing the CASS assessment schedules it is important to cover the *rigour of assessment*. This is a key determinant in ensuring that sufficient objectivity and repeatability is built into the scheme to enable a consistent approach to the actual assessment process, the development of the technical schedules and the assessment results.

There are a number of key factors to be addressed in developing the CASS approach to *rigour of assessment* (see Common Schedules Chapter 3.10).

It is important to position management of functional safety as defined in IEC 61508 and the related CASS assessment, FSCA in the context of other international management certification standards.

The key management standards are ISO 9001, ISO 14000, BS 7799, ISO 8800. Common Schedules Figure 3.5 below serves to illustrate the dominant relationship between ISO 9001 and IEC 61508. ISO 9001 forms the basis for quality management systems.

Descriptions of the specific CASS assessment types follow.

3.3.3 FUNCTIONAL SAFETY CAPABILITY ASSESSMENT (TYPE 5)

Also known as:
Safety audit, safety assessment,

Purpose of assessment:
To assess the adequacy and effectiveness of the functional safety capability of an organisation for developing and supplying E/E/PES for given application(s).

Target Of Evaluation
The functional safety management capability of the organisation. Scope includes the policy, procedures, documentation and records for all activities concerned with functional safety for the given application area. This includes the competence assessment process that the organisation has in place to ensure competency of staff involved in functional safety activities.

Typical applicant:
Any organisation involved in any of the functional safety lifecycle activities i.e. in creating, using or disposing of E/E/PES safety related systems. This includes:
a) Owner/operators who specify, procure and operate such systems;
b) System integrators and design contractors who develop, supply and/or install application specific systems;
c) Component suppliers who develop and supply off-the-shelf products for use in E/E/PES safety systems.

Typical Lifecycle phases to be assessed

IEC 61508-1 Clause 6: Management of functional safety
Sample of lifecycle phases
IEC 61508-2 Sample of phases
IEC 61508-3 Sample of phases

A FSCA is scoped to assess only those lifecycle phases that the organisation performs and wishes to claim capability for. This focus ensures the FSCA is appropriate to the organisation's activities and checks the organisation's understanding of how those activities fit within the overall safety lifecycle.

A FSCA will be further scoped to make clear the other issues affecting the assessment. For example a system integrator will need to specify the Safety Integrity Level of the systems involved; the use of common proprietary platforms on which the systems are implemented and the teams/departments that are developing these systems.

Assessment techniques
Process Audit;
Document inspection;
Checklists as appropriate.
The primary role of FSCA is to ensure that a management system for functional safety exists and is adequate. The secondary role is to check that it is effectively implemented by sampling evidence of this on specific systems or projects. This sampling will check the work products produced by the phases but it must be stressed that the assessment will not **repeat** lifecycle activities especially where those activities themselves involve checking work products e.g. the organisation's verification process.

FSCA establishes the basic capability of an organisation to perform safety lifecycle activities and is, thus, a crucial basis for the remaining CASS assessment types. A successful FSCA will have confirmed that the underlying functional safety processes and procedures are defined, adequate and in use. In this way a FSCA allows the other CASS assessments to focus on the safety system (product) attributes rather than on the processes used. The relationship between FSCA and the other CASS assessment types is shown in fig. 3.7.

Applicable EN standard for accreditation of certification bodies

EN 45011

3.3.4 APPLICATION SPECIFIC ASSESSMENTS (TYPE 2)

Two subtypes of Application Specific Assessment are described. These are:
a) Integrated System Assessment (Type 2a)
b) Subsystem Assessment (Type 2b)

They lead to product certification of the safety related system itself.

It is difficult to make an exact definition of the various system types (i.e. integrated system, sub-system, component etc.). The definitions here are for guidance only and will be revisited as necessary following experience with scoping and performing CASS assessments.

3.3.4.1 INTEGRATED SYSTEM ASSESSMENT (TYPE 2A)

Also known as:
Integrated system assessment ; Application Dependent assessment, Design/Integration assessment, installed system assessment.

Purpose of assessment:
To assess the functional safety achieved by a specific E/E/PES that has been configured for a given application in order to perform a required task.

Target Of Evaluation
Integrated system close to installation or recently installed. Scope normally includes all sub-systems comprising the integrated system and all elements of those sub-systems (sensors, programmable electronics, actuators etc.). **The end to end system in its working environment is the scope of these assessments.**

These integrated systems are typically *installations*, physically large or involve multiple CPU's that are specially designed for the application, i.e. bespoke. Examples are:

a) High Integrity Protection Systems (HIPS)
b) Emergency Shutdown Systems (ESD)
c) Fire and Gas systems
d) Burner management systems
e) Anti-lock braking systems
f) Automatic Warning Systems (AWS)
g) Distributed Control Systems (DCS)
h) Supervisory Control and Data Acquisition (SCADA) systems.

A 'standardised' product that has been built into a specific architecture and configured for the application would also come into this category.

Typical applicant:
Engineering Design Contractor

Lifecycle phases to be assessed
IEC 61508-1
4 Overall Safety Requirements*
5 Safety Requirements Allocation*
7 Overall safety validation planning
8 Overall installation and commissioning planning
12 Overall installation and commissioning
13 Overall safety validation
IEC 61508-2 All phases
IEC 61508-3 All phases
(* = Boundary check only)

Assessment techniques*
Document inspection
Process Audit
Test witnessing
Checklists
Decision/truth tables
Software complexity metrics
Failure analysis
Common cause failure analysis
Reliability block diagrams
(*= selected according to SIL and whether software is to be assessed)

Factors affecting the base case
Applicant may have subcontracted the entire procurement to a prime subcontractor
Integrated system is a long term legacy system
No application software needed to be developed, only data configuration files

Applicable EN standard for accreditation of certification bodies

EN 45011

3.3.4.2 SUB-SYSTEM ASSESSMENT (TYPE 2B)

Also known as:
Supplied system assessment; Application Dependent assessment, Design/Integration assessment,

Purpose of assessment:
To assess the functional safety achieved by a specific E/E/PES that has been configured for a given application in order to perform a required task.

Target Of Evaluation
Part of an integrated system, normally without the sensors or actuators. Scope is a sub-system of the final installed system comprising such components as the input interfaces, logic solver and output interfaces. This is **not** typically the end to end system in its working environment but an integration of components that is supplied separately and then installed into the plant or process.

Typical applicant:
Design contractor/system supplier who has developed and supplied the sub-system

Lifecycle phases to be assessed
IEC 61508-1 None
IEC 61508-2 All phases
IEC 61508-3 All phases

Assessment techniques*
Document inspection
Process Audit
Test witnessing
Checklists
Decision/truth tables
Software complexity metrics
Failure analysis
Common cause failure analysis
Reliability block diagrams
(*= selected according to SIL and whether software is to be assessed)

Factors affecting the base case
Applicant may supply the full end to end system and overlap with the Integrated System case.
Sub-system is a large integration of components in its own right.
No application software needed to be developed only data configuration files

Applicable EN standard for accreditation of certification bodies

EN 45011

3.3.5 COMPONENT ASSESSMENTS (TYPE 1)

Components are characterised by such terms *as application independent* and *proprietary.* Examples are:

a) proprietary general purpose equipment
b) PLC's
c) smart instruments
d) signal acquisition boxes
e) stand-alone shutdown systems
f) TMR PLC's
g) Commercial Off The Shelf (COTS) systems
h) shrink-wrapped software
i) other proprietary software.

There is one basic type of Component Assessment which leads to product certification of the component itself.

Also known as:
Application Independent; Product Assessment; Type Approval

Purpose of assessment:
To assess the functional safety achieved by a specific component intended for a set of applications in order to perform a required task.

Target Of Evaluation
Single E/E/PES or individual component that is sold as a generic product. Can be:
hardware only e.g. sensor, non-programmable ESD
hardware and software e.g. PLC, programmable ESD
software only e.g. software sold as a generic product and used in safety related PES.

Typical applicant:
Component manufacturer or supplier who has developed the component.
Equipment vendor or Value Added Retailer who sells on components.

Lifecycle phases to be assessed

IEC 61508-2
E/E/PES safety requirements specification
E/E/PES safety validation planning
E/E/PES design and development**
E/E/PES operation and maintenance procedures
E/E/PES integration*
*E/E/PES safety validation**
(* = not for single item components)
(** = to include factory production arrangements)

IEC 61508-3
Software safety requirements specification
Software safety validation planning
Software design and development**
PE integration (hardware/software)**
Software operation and modification procedures
Software safety validation
(** = to include software replication arrangements)

Assessment techniques*
Document inspection
Process Audit
Test witnessing
Checklists
Decision/truth tables
Software complexity metrics
Failure analysis
Common cause failure analysis
Reliability block diagrams
(*= selected according to SIL and whether software is to be assessed)

Factors affecting the base case

Applicant may not be developer or manufacturer.
Component is a 'low complexity' system.
Component is a set of individual items from a product line.

Applicable EN standard for accreditation of certification bodies

EN 45011

3.3.6 OPERATION AND MAINTENANCE ASSESSMENTS (TYPE 3)

There is one basic type of O&M assessment which leads to certification of the operation and maintenance process for a given E/E/PES.

Also known as:
Service monitoring Assessment, In service support assessment.

Purpose of assessment:
The assess the adequacy and effectiveness of the operation and maintenance process of an organisation for operating, maintaining, repairing and modifying a E/E/PES for a given application.

Target of evaluation
The operation and maintenance process of the organisation. Scope includes the policy, procedures, documentation and records for all activities concerned with maintaining functional safety for an installed and operating E/E/PES.

Typical applicant.
Plant operator
Installation owner

Lifecycle phases to be assessed
IEC 61508-1
6: Overall operation and maintenance planning
14: Overall operation, maintenance and repair
15: Overall modification or retrofit
IEC 61508-2 None
IEC 61508-3 None

Assessment techniques
Document (procedures) review
Process Audit

Factors affecting the base case
Applicant may not be the plant operator.
Applicant contracts out O&M to a third party

Applicable EN standard for accreditation of certification bodies

EN 45011

Selected on the basis of an assessment of the operations and maintenance system as applied to the specific safety system under maintenance. Could also apply to a number of similar safety-related systems.

3.3.7 SAFETY REQUIREMENTS ASSESSMENT (TYPE 4)

Also known as:
Hazard and risk analysis assessment; safety requirements capture assessment

Purpose of assessment:
To assess the overall safety requirements and associated hazard and risk analyses for an application specific E/E/PES.

Target Of Evaluation
Safety requirements specification and hazard and risk process.

Typical applicant:
Owner/operator who has procured/is procuring the application specific system.

Lifecycle phases to be assessed
IEC 61508-1
2: Overall scope definition
3: Hazard and risk analysis
4: Overall safety requirements
5: Safety requirements allocation
IEC 61508-2 None
IEC 61508-3 None

Assessment techniques
Document inspection
Process Audit
Checklists
Decision/truth tables
Failure analysis
Common cause failure analysis
Reliability block diagrams

Factors affecting the base case
Applicant may have subcontracted the entire procurement to a prime subcontractor
Hazard & risk analysis was not responsibility of applicant
Application specific system is a long-term legacy system

Applicable EN standard for accreditation of certification bodies

EN 45011

Figure 3.1 - Basic V Model

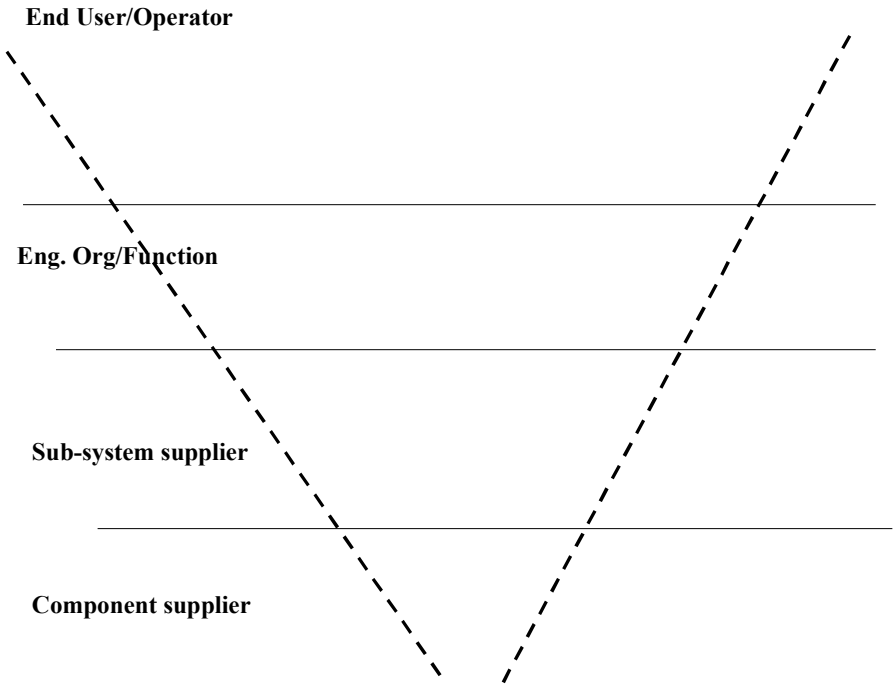


Figure 3.2 - Supply chain mapping to CASS assessment types

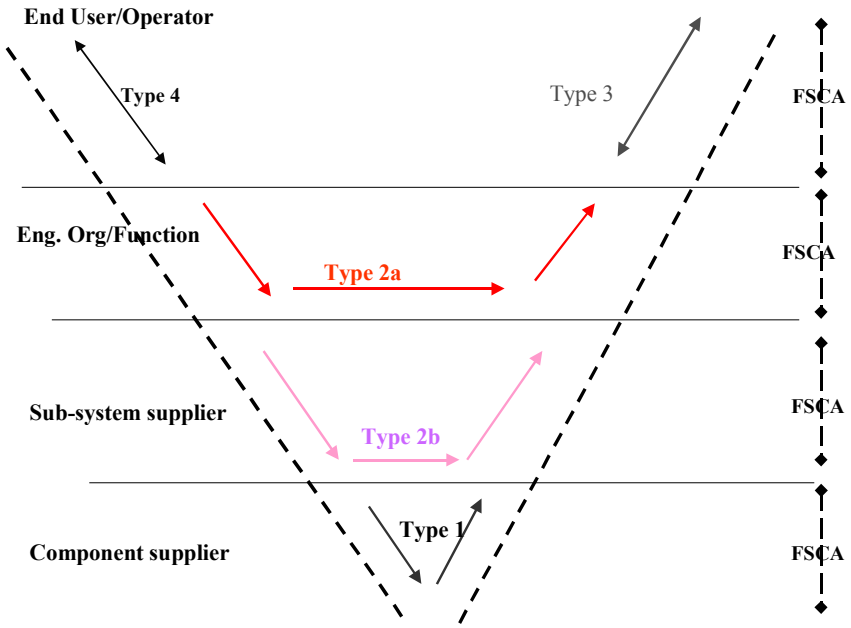


Figure 3.3 - Mapping of 61508 phases to CASS assessment types

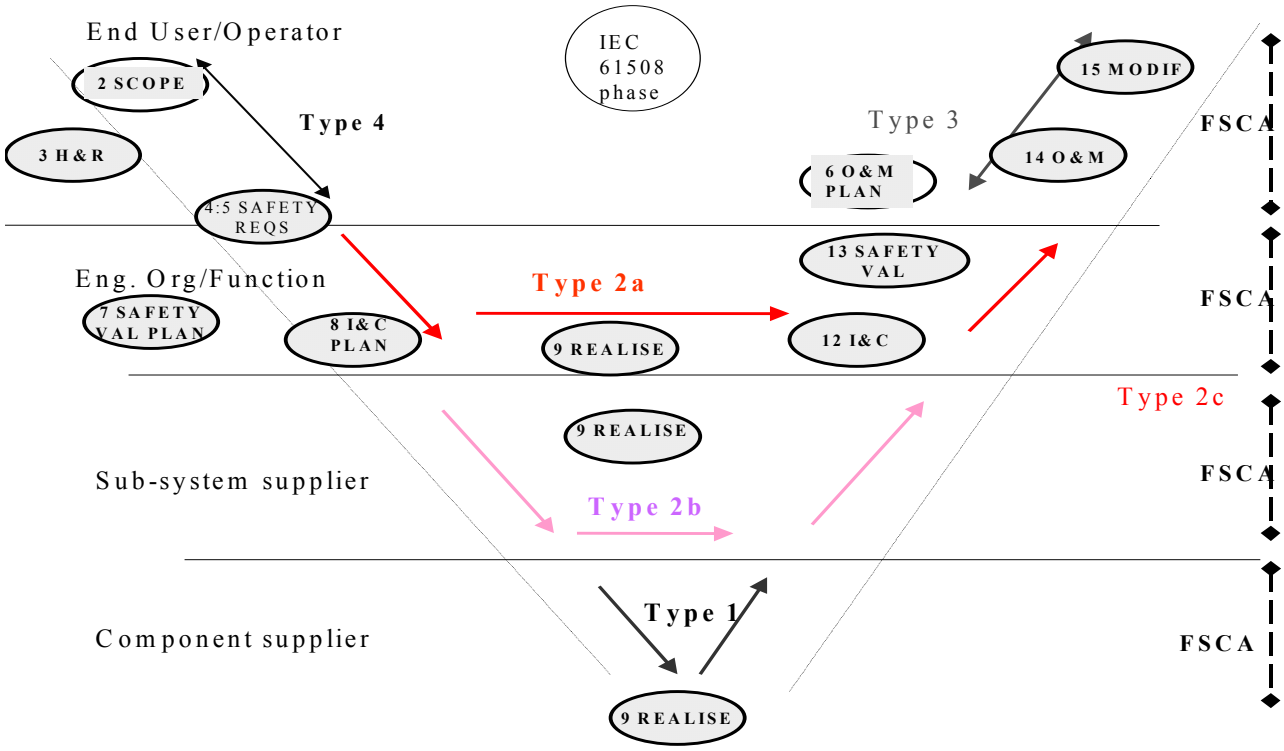


Figure 3.4 - Mapping of core competencies

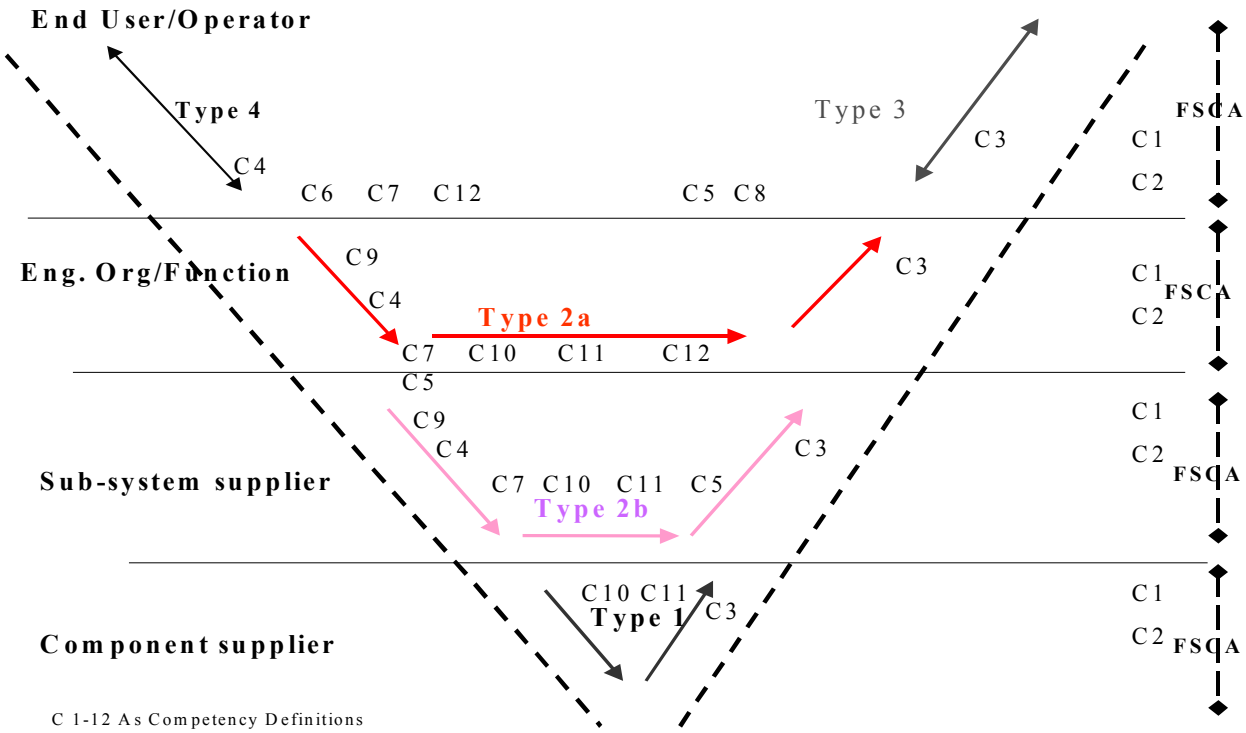


Figure 3.5 : Current Management Systems

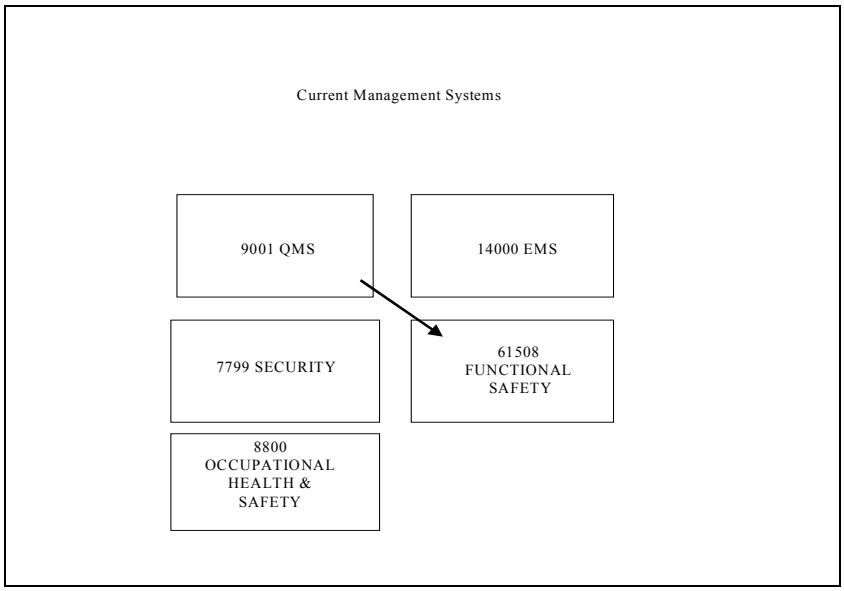
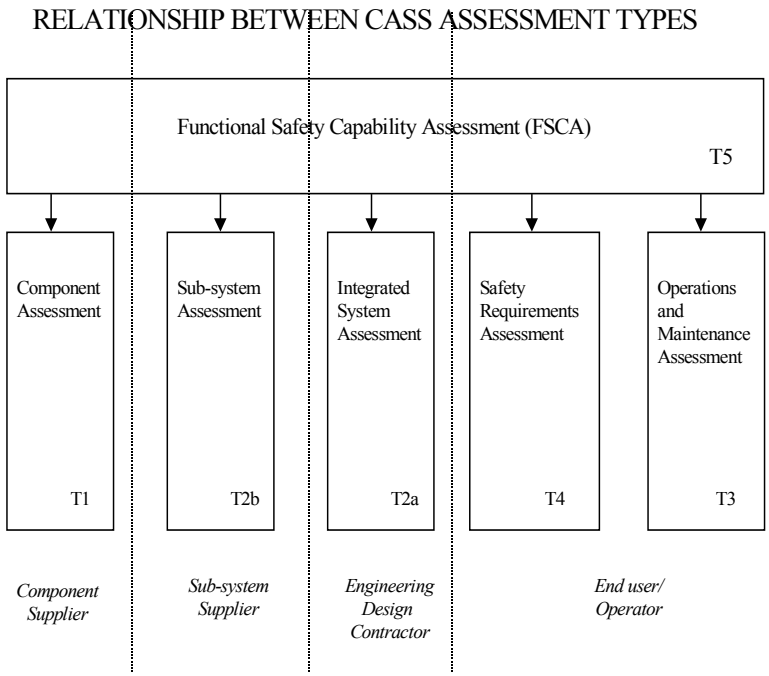


Figure 3.6: Relationship between CASS assessment types



3.4 GUIDANCE FOR CONTROL SYSTEMS

This section provides guidance and clarification on control systems within the context of IEC 61508.

3.4.1 CONTROL SYSTEMS WHICH ARE NOT DESIGNATED AS 'SAFETY-RELATED', AND WHERE THERE IS NO OTHER E/E/PE SAFETY-RELATED SYSTEM PROVIDING PROTECTION

If failure of the control system does not lead to a hazardous situation or does not cause a demand on an E/E/PE safety-related system, then IEC 61508 does not specifically apply (although the principles of the standard could be applied if a high integrity system is required for other reasons, e.g. to protect against economic loss).

In situations where failure of the control system does lead to a hazardous situation, and where there is no other safety-related system providing protection, then the probability of a hazard occurring (due to a failure of the control system) in a specified period of time, t, is determined by the rate at which the control system fails to danger. Assuming a constant dangerous failure rate, λ_d, and provided that $\lambda_d t << 1$ then the probability of a hazard occurring, P_h, is given by:

$$P_h = \lambda_d t$$

The view of IEC 61508 (IEC 61508-1, 7.5.2.4) is that a dangerous failure rate for a control system of less than 10^{-5} per hour should not be claimed unless the system has been designed and implemented according to IEC 61508. Therefore, the lowest probability of a hazard which can be claimed associated with the failure of a control system which is not regarded as safety-related and implemented according to IEC 61508 is 10^{-5} per hour, which is roughly equal to 10^{-1} per year. This probability is only likely to result in a tolerable risk for the most minor of consequences (e.g. an injury which will heal and leave no permanent impairment).

The conclusion of the above is that where the failure of a control system can lead to a greater consequence than a reversible injury, then the control system should be designated as 'safety-related' and should be designed and implemented according to IEC 61508 or there should be second system which operates to prevent the hazard occurring on failure of the control system. Such a second system is often referred to as a 'protection system'.

3.4.2 CONTROL SYSTEMS WHICH ARE NOT DESIGNATED AS SAFETY RELATED AND WHERE THERE IS ANOTHER E/E/PE SAFETY-RELATED SYSTEM PROVIDING PROTECTION.

The requirements in this case are set out in IEC 61508-1, 7.5.2.4:

"Where failures of the EUC control system place a demand on one or more E/E/PE or other technology safety-related systems and/or external risk reduction facilities, and where the

intention is not to designate the EUC control system as a safety-related system, the following requirements shall apply:

a) the dangerous failure rate claimed for the EUC control system shall be supported by data acquired through one of the following:
— actual operating experience of the EUC control system in a similar application,
— a reliability analysis carried out to a recognised procedure,
— an industry database of reliability of generic equipment; and
b) the dangerous failure rate that can be claimed for the EUC control system shall be not lower than 10-5 dangerous failures per hour; and
c) NOTE 1 The rationale of this requirement is that if the EUC control system is not designated as a safety-related system, then the failure rate that can be claimed for the EUC control system shall not be lower than the higher target failure measure for safety integrity level 1 (which is 10-5 dangerous failures per hour - see table 3).
d) all reasonably foreseeable dangerous failure modes of the EUC control system shall be determined and taken into account in developing the specification for the overall safety requirements; and
e) the EUC control system shall be separate and independent from the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.
f) NOTE 2 Providing the safety-related systems have been designed to provide adequate safety integrity, taking into account the normal demand rate from the EUC control system, it will not be necessary to designate the EUC control system as a safety-related system (and, therefore, its functions will not be designated as safety functions within the context of this standard). In some applications, particularly where very high safety integrity is required, it may be appropriate to reduce the demand rate by designing the EUC control system to have a lower than normal failure rate. In such cases, if the failure rate is less than the higher limit target safety integrity for safety integrity level 1 (see table 3) then the control system will become safety-related and the requirements in this standard will apply."

The reason for this restriction on what can be claimed for a control system which is not designated as safety-related, is to prevent unrealistic claims being made for the performance of the control system in order to ease the requirements (i.e. reduce the required risk reduction) relating to the safety-related system.

3.4.3 CONTROL SYSTEMS WHICH ARE DESIGNATED AS 'SAFETY-RELATED'

In most situations, a control system acts to provide more or less continuous control (e.g. level control, temperature control). A failure of the control system will lead to some deviation from the intended operating conditions. In situations where this deviation is hazardous, and where the probability associated with the tolerable risk is below 10^{-1} per year, then it will be necessary to regard the control system as being 'safety-related' and to design and implement it according to IEC 61508.

In such situations, the system is, in effect, implementing a safety function operating in the high demand / continuous mode of operation and therefore the target failure measure is

expressed in terms of the dangerous failure rate per hour rather than as a probability of failure on demand.

The target failure measure is derived directly by considering the failure rate associated with the tolerable risk, rather than by deriving it in terms of risk reduction. This is not well explained in IEC 61508-1, which requires that risk reduction is specified for each hazardous event (IEC 61508-1, 7.5.2.2). In fact, the process of deriving the target failure measure in terms of risk reduction, as specified in IEC 61508-1, is appropriate for safety functions operating in the low demand mode of operation (e.g. protection functions which operate 'on demand'), but is not directly applicable to safety functions operating in the high demand / continuous mode of operation.

3.5 IS A PRODUCT SAFETY-RELATED?

This section seeks to identify the principles that are required to be addressed when giving consideration to assessing if a product or application has any bearing on the safety of operation of that product or process.

3.5.1 PRINCIPLES

Before one can judge if a product is safety related, two aspects must be considered:
a) what is a product? and,
b) what is safety?

A product can be an item or unit which provides an intrinsic function and which can be distributed and/or purchased as a usable entity. Equally, a product can be a collection of such items that together form a larger product or system that provides a collection of functions that are specific to that system. In addition, a product may be purely software. This could be in the form of 'shrink wrapped' software or it may be bespoke application software.

For a definition of safety, one dictionary defines Safety as including each of the following:

a) being uninjured,
b) being out of danger,
c) keeping secure,
d) avoiding risk.

Bringing these aspects together provides a basis for answering the above question.

A further question to consider is how does one determine if an application is safety related?

In order to further consider the questions raised in the preceding section, one should approach this in a top-down approach; considering the issue of Applications first then follow with products.

3.5.2 APPLICATIONS

An application which can subject one or more of an operating company's employees, any member of the general public or any significant aspect of the environment to any risk that offers some element of danger, should that application malfunction or fail to operate in some prescribed way, then that application is safety related. The degree to which it is related to safety can be determined by the undertaking of the provisions discussed in the standard IEC 61508.

A useful source of introductory material to this aspect of safety is available from The Health and Safety Executive in a video open learning package entitled "Safety and Computer Control".

3.5.3 PRODUCTS

Products can involve both hardware and software components and it must be recognised that each of these components can have a dramatic impact on the level of safe operation that can be guaranteed for a given product.

For a product to be safe then all possible forms of failure of that product must be identifiable, predictable, unambiguous and consistently repeatable. This applies to all of the above definitions of product that are discussed in Section 2 and can be a combination of both hardware and software in their make-up.

Where a product is a composite of other products, i.e. a system, then the interactive effects of a possible failure of one product upon one or more of the other products involved in the composite must be also identifiable, predictable, unambiguous and consistently repeatable. If such a combination also involves some form of human intervention then this must be adequately monitored by the system to ensure that any failure in the human operation is both detected and the effects isolated.

Guidance on the considerations and approaches to take to ensure that any "product" which is deemed to be safety related meets these requirements, are fully discussed in the standard IEC 61508.

3.6 CHARACTERISATION OF SAFETY RELATED SUBSYSTEMS

3.6.1 BACKGROUND

This section discusses the way in which sub-systems (such as sensors, programmable logic controllers (PLCs) within an electrical / electronic / programmable (E/E/PE) electronic safety-related system should be characterised so as to allow the designer or integrator of an E/E/PE safety-related system meet the requirements of IEC 61508-2. It is in response to actions raised at CASS Technical Team meetings.

3.6.2 DEFINITIONS

The following definitions are included in IEC 61508-4:

1 ***System*** *- set of elements which interact according to a design, where an element of a system can be another system, called a sub-system, which may be a controlling system or a controlled system and may include hardware, software and human interaction.* (ref. IEC 61508-4, 3.3.1)

2 ***Electrical / electronic / programmable electronic system*** *- system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices.* (ref. IEC 61508-4, 3.3.3)

3 ***Safety-related system -*** *designated system that both:*

— *implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and*
— *is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions* (ref. IEC 61508-4, 3.4.1)

The term electrical / electronic / programmable electronic safety-related system, although that is forms part of the title of IEC 61508-2, is not explicitly defined. However, it can be taken to mean an E/E/PE system which comes within the definition of a safety-related system.

IEC 61508-2 includes the following requirement and supporting explanatory note:

"*The design shall be based on a decomposition into sub-systems with each sub-system having a specified design and set of integration tests (see 7.4.7).*
NOTE 1 A sub-system may be considered to comprise a single component or any group of components. A complete E/E/PE safety-related system is made up from a number of identifiable and separate sub-systems, which when put together, implement the safety function under consideration. A sub-system can have more than one channel. See 7.4.7.3." (ref. IEC 61508-2, 7.4.2.11)

Additionally, IEC 61508-2 introduces the concept of a safety-related sub-system:

"All sub-systems which are used by one or more safety functions shall be identified and documented as safety-related sub-systems." (ref. IEC 61508-2, 7.4.2.11)

In summary, E/E/PE safety-related systems implement complete safety functions (and therefore must be considered to include everything from sensor to final actuator) and sub-systems can be considered as any group of components within the system.

3.6.3 REQUIREMENTS OF IEC 61508-2

In general, the requirements in IEC 61508-2 relate to E/E/PE safety-related *systems*. However, in order that the system requirements can be met, the following specific requirements are placed on *sub-systems*:

Classification of sub-systems as 'Type A' or 'Type B' (IEC 61508-2, 7.4.3.1.2, 7.4.3.1.3)
Architectural constraints (IEC 61508-2, 7.4.3.1.4)
Diagnostic test interval (IEC 61508-2, 7.4.3.2.3 to 7.4.3.2.5)
Identification of safety-related sub-systems (IEC 61508-2, 7.4.7.2)
Information (specification) requirements (IEC 61508-2, 7.4.7.3, 7.4.7.4)
Proven-in-use criteria (IEC 61508-2, 7.4.7.5 to 7.4.7.12)

3.6.4 CHARACTERISATION OF SUB-SYSTEMS

In order that sub-systems can be integrated into the E/E/PE safety-related system in such a way that satisfies the E/E/PE Safety Requirements Specification, then any safety-related sub-system has to be characterised, or specified, in such a way that the relevant information and data is available as inputs to the E/E/PE safety-related system design process. The data and information that is required is listed in IEC 61508-2, 7.4.7.3:

"*The following information shall be available for each safety-related sub-system (see also 7.4.7.4):*

a) a functional specification of those functions and interfaces of the sub-system which can be used by safety functions;
b) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are detected by diagnostic tests (see 7.4.7.4);
c) the estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are undetected by diagnostic tests (see 7.4.7.4);
d) any limits on the environment of the sub-system which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures;
e) any limit on the lifetime of the sub-system which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures;
f) any periodic proof test and / or maintenance requirements;
g) the diagnostic coverage derived according to annex C (when required, see note 1)

h) the diagnostic test interval (when required, see note 1);

NOTE 1 Items g) and h) above relate to diagnostic tests which are internal to the sub-system. This information is only required when credit is claimed for the action of the diagnostic tests performed in the sub-system in the reliability model of the E/E/PE safety-related system (see 7.4.3.2.2).

i) any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;

NOTE 2 Items b) to i) are needed to allow the probability of failure on demand, or the probability of failure per hour of the safety function to be estimated (see 7.4.3.2.2)

NOTE 3 Items b), c), g), h) and i) are only required as separate parameters for sub-systems such as sensors and actuators which may be combined in redundant architectures to improve hardware safety integrity. For items such as logic solvers which will not themselves be combined in redundant architectures in the E/E/PE safety-related system, it is acceptable to specify performance in terms of probability of failure on demand, or probability of dangerous failure per hour taking into account items b), c), g), h) and i). For such items it will also be necessary to establish the proof test interval for failures which are undetected.

j) all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the sub-system as applied in the E/E/PE safety-related system, determined according to annex C;

k) the hardware fault tolerance of the sub-system;

NOTE 4 Items j) and k) are needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints (see 7.4.3.1)

l) any limits on the application of the sub-system which should be observed in order to avoid systematic failures;

m) the highest safety integrity level that can be claimed for a safety function which uses the sub-system on the basis of:

— measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the sub-system (see 7.4.4.1 and 61508-3, 7.4),

— the design features which make the sub-system tolerant against systematic faults (see 7.4.5.1);

NOTE 5 This is not required in the case of those sub-systems which are considered to have been proven-in-use (see 7.4.7.5).

n) any information which is required to identify the hardware and software configuration of the sub-system in order to enable the configuration management of the E/E/PE safety-related system in accordance with IEC 61508-1, 6.2.1.

o) *documentary evidence that the sub-system has been validated."*

It is this information which forms the characterisation of a safety-related sub-system for the purposes of IEC 61508-2. In principle, this characterisation can be applied to any sub-system, regardless of the complexity or whether or not the sub-system was designed specifically for safety-related application. For example, it could be applied to a complex sub-system such as a programmable logic controller or to a simple component. In the latter case it is most likely that the component would, in effect, be claimed as "proven-in-use" according to IEC 61508-2, clauses 7.4.7.5 to 7.4.7.12 and the characterisation would comprise no more than the standard set of data required for any general purpose component.

3.7 SUB-CONTRACTING ACTIVITIES WITHIN IEC 61508

3.7.1 PURPOSE

This section discusses how sub-contracting activities are covered by the standard. For many large, multi-national organisations, sub-contracting parts of a project to organisations, potentially in different parts of the world, is a standard practice.

3.7.2 61508 PART 1 – OVERALL ACTIVITIES

In terms of management activities, Part 1 of the standard should be considered. Sub-contracting is not explicitly mentioned in the standard, but the terms suppliers and manufacturers are used frequently.

The standard uses the term, 'Responsible for Life-cycle phase or activity' in several clauses of Part 1. This indicates that an activity may be performed by individuals, organisations or teams other than those who have responsibility for the activity.

The important reference seems to be Part 1, Clause 6.2.5

"Suppliers providing products and services to an organisation having overall responsibility for one or more phases of the overall, E/E/PES or software safety lifecycles shall deliver products or services as specified by that organisation and shall have an appropriate quality management system"

This tells us that the responsible organisation is required to specify the activity or service to be produced, which may include defining standards to be used or specifying checks that need to be conducted before acceptance of the service or product.

The supplying organisation shall have an appropriate quality management system. The term appropriate is interesting, as this can be interpreted in different ways. In the context of safety systems, it would be reasonable to expect the sub-contracting company to have policy, procedures and processes that would support the safety activity.

Another clear requirement is specified in Part 1, clause 6.2.1h. This states that:

" The organisation or individual that have overall responsibility for a phase of the lifecycle…. shall specify procedures for ensuring that applicable parties involved in any of the activities are competent to carry out the activities…."

This indicates that the responsible organisation shall have a process for ensuring that sub-contractor organisations or individuals are competent for the activities they are performing.

3.7.3 61508 PART 2 – E/E/PES

There is no obvious guidance in Part 2 for the use of sub-contractors. Suppliers and manufacturers are mentioned, but only in the context of making available the results of the safety validation testing (7.7.2.6) and maintaining a system to initiate changes as a result of defects being detected and informing users of the need for modification (7.8.2.2).

3.7.4 61508 PART 3 – SOFTWARE REQUIREMENTS

In Part 3 there are several clauses that discuss the relationship between the software supplier and the user. Clearly, this could be viewed as a sub-contracting arrangement.
Clause 7.4.2.1 states that responsibility for conformance with the software design and development clause can rest with the supplier alone, the user alone, or with both.
Clause 7.4.3 discusses the division if responsibilities for compliance with the software design and development clause depending upon the architecture and language variability.
Clause 7.4.4 discusses the division of responsibilities for compliance with the clause on requirements for support tools and programming languages depending upon the language variability.
Clause 7.4.5 discusses the requirements for detailed design and development. The responsibility for conformance will depend upon the nature of the software development.
In all these clauses, there is specific guidance to assist in the allocation and documentation of responsibilities. The exact division of responsibilities shall be documented during safety planning.

3.7.5 CONCLUSIONS AND DISCUSSION

The important concept that clarifies the issue is ‘responsibility’. Responsibility can pass to different organisations throughout the complete lifecycle. If we envisage the ‘V’ model, responsibility could pass from the End User / operator who specifies the requirement to the Engineering organisation, who may design the system, to the sub-system supplier, who may supply a standard package, then back up to Engineering organisation to install / commission the system the back to the End User to operate and maintain the system.

At any stage in this process, work could be sub-contracted out. This could be the end-user sub-contracting out the Hazard analysis to a specialist consultancy at the front end of the ‘V’ model, to the Engineering contractor sub-contracting out packages of work to several different integration / installation companies.

Throughout all of these complex interactions, it should be clear who is responsible for the activities in that phase and the responsible organisation must specify the activities and any standards that apply to the sub-contractor. It is also clear that the responsible organisation should have processes and procedures in place to ensure that the sub-contracting organisation is competent to perform the tasks that are allocated to them. Finally, the sub-contracting organisation should operate an appropriate Quality Management system. If a safety activity is being performed, it is not unreasonable to expect this QMS to include aspects of a FSCA.

3.8 NON-COMPLIANCES: WHAT THEY MEAN AND HOW TO DEAL WITH THEM

The objective of an assessment is to verify that a product or organisation complies with specified criteria. Compliance is demonstrated with objective evidence that all criteria are met.

A non-compliance is generally recorded if:

a) there is objective evidence that a criterion is not met, or
b) there is insufficient objective evidence that a criterion is met.

If a non-compliance is recorded, the possible courses of action will depend on the nature of the assessment. For product conformity assessment, only complete compliance is acceptable.

The options are:
a) produce evidence of compliance, either by modifying the product to comply with the criteria or by providing additional objective evidence that the existing product complies, or
b) change the specified criteria to a level which the product can meet.

For example, if the original criteria stated that the product must function correctly over a temperature range of -30°C to +50°C and it was shown to function only in the range -10°C to +30°C, this limitation might be acceptable.

In the case of organisation conformity assessment a limited degree of non-compliance might be tolerable if:
a) the number and severity of the non-compliances was not such as to raise doubts about the capability of the organisation to carry out its functions satisfactorily, and
b) the organisation undertook to rectify the non-compliances within an acceptable period of time.

Evidence of rectification must be provided and will be verified by the assessor.

A feature of organisation conformity assessment is that the organisation is subject to periodic audits and re-assessments. Evidence of compliance with the specified criteria is gathered over time as the organisation develops and adapts to its business environment. The satisfactory rectification of non-compliances can be verified during the auditing process.

Product conformity assessment may relate to one particular product for one specified installation or may be applied to a product type which the supplier may replicate for a number of different users and installations. In the latter case, evidence will be required to provide confidence that the production system will produce products conforming to the assessed type. One method is to assess and audit the production organisation for conformity with a relevant standard such as ISO 9002. Non-conformances raised during such a process would be dealt with as for the organisation assessment described above.

Further guidance on this topic is given in CASS Assessment Procedure CAP 11.

3.9 MAPPING – PURPOSE AND PERFORMANCE

This section gives guidance on the purpose of the mapping procedure. Also included is guidance on what information is required to be included in a mapping matrix.

3.9.1 INTRODUCTION

Before a CASS assessment can be undertaken, it is first necessary to establish the scope of the task. Although this activity is the responsibility of the client requesting the assessment, it may be that the client requires assistance in this process. In such cases, the client may seek suitable support from an external consultant with appropriate expertise, or from a CASS assessor. It is acceptable for the same person to scope and perform a CASS assessment.

At the highest level, the client must identify both the type of assessment which is required, and the integrity level which is applicable. In addition, a systematic analysis should be carried out to determine the detailed scope of the assessment. The aim of this analysis is to determine the correspondence between the client documentation and the documentation required by IEC 61508. The assessment criteria for a CASS assessment, which are based on the requirements of IEC 61508, are outlined in Section 2 of the "Technical Schedules for Application Specific Assessments".

It is recommended that this analysis should be carried out by establishing a mapping between the appropriate elements of the client's documentation and a particular "target of evaluation" (TOE). The CASS TOEs, which are detailed in Section 4 of the "Technical Schedules for Application Specific Assessments", represent a set of identifiable objects which can themselves be mapped onto the requirements of IEC 61508. However, not all of the TOEs will be applicable for all types of assessment, and only a sub-set of those identified for each class of assessment will be relevant in any specific case. It is the responsibility of the client requesting the assessment, therefore, to determine which TOEs are relevant to the required assessment and which elements of the available documentation can be identified with these TOEs. This mapping is still necessary if the client documentation was developed according to sector-specific standards based upon IEC 61508 or its predecessors (e.g. IEC 61508, SC65A).

3.9.2 PURPOSE

Definition of the scope of the assessment and the identification of mappings between client documentation and the CASS TOEs (and hence to the relevant requirements of IEC 61508).

3.9.3 RESPONSIBILITY

This activity is the responsibility of the client requesting a CASS assessment, with support from outside consultants or assessors as necessary.

3.9.4 INPUTS

Application specific assessments may be carried out both for final installations and for sub-systems. It is recognised that the latter may be at a wide range of levels between individual components and installed or fully integrated systems.

In many cases, therefore, clients requesting application specific assessments may be dependent on suppliers who are providing elements of both the product and the associated safety management system. If so, it may be appropriate for these suppliers to be assessed independently, so that the results of their assessments can be offered as part of the supporting documentation provided by the client requesting assessment at a higher level of integration. The degree of independence required for such assessments is defined in IEC 61508 and depends upon such factors as the Safety Integrity Level of the system, novelty of the application etc.

In some cases, however, this may not be practicable, so the client requesting assessment may need to draw more directly on the suppliers' documentation in order to meet the requirements of the CASS TOEs.

The required inputs for application specific assessments are outlined below:

a) Project specifications, plans, reviews and reports, engineers' log books and any relevant documentation (e.g. certificates or supporting information) for bought-in components and sub-systems.

b) List of TOEs relevant to the required type of application specific product assessment (i.e. integrated system or sub-system, and the nature of the technology deployed), and their purpose (e.g. software module test specification).

The requirements for both of these types of assessment are essentially the same, although they will differ in detail.

3.9.5 ACTIVITIES

The tasks which the client must carry out to scope the assessment are as follows:

1) Identify the integrity level of the product to be assessed. If this is impractical, a target SIL may be used instead.
2) Identify the class of application specific assessment required (ie. integrated system, or sub-system).
3) Consider whether any existing certificates might reduce the amount of assessment required.
4) Define the scope of assessment (in terms of TOEs to be assessed).
5) Identify the corresponding company or supplier documentation.
6) Record the references, locations and mapping of these documents to the review objects in a summary table (or set of tables if appropriate).
7) Identify any missing features (relative to the descriptions of the TOEs).

3.9.6 OUTPUTS

The information required by the assessors in order to undertake an application specific assessment is listed below.

a) The type of assessment requested.
b) The integrity level which is applicable.
c) An appropriate set of completed mapping matrices (see Annexes A and B of this document), selected as appropriate to the type of technology and the nature of the assessment. These tables will detail the mapping to CASS TOEs by providing:
   a relevant list of the TOEs to be assessed;
   the corresponding client documents;
   the location of the documents for review;
   notes on any missing features.

The notes on any missing features are considered to be particularly important, as they will identify any shortfalls which may need to be addressed before an assessment can be completed.

Recording the location of the documentation is also useful, especially if this information is normally distributed around a number of different sites or organisations. This information can then be quoted by the assessor to ensure that all of the relevant documentation is available at a single location when the review is scheduled to take place.

3.10 ASSESSMENT RIGOUR AND SAMPLING

This note outlines a framework for achieving rigour in CASS assessments. Two aspects of rigour are defined and used to determine the CASS approach to this issue:

- rigour of assessment
- rigour of evidence.

3.10.1 RIGOUR OF ASSESSMENT (ROA)

This relates to the correctness, repeatability and confidence level of assessment decisions. This rigour is dependent upon the assessor and the assessment method.

	ROA Requirement	**CASS approach**	**Remarks/References**
1.1	Use of competent assessors.	Scheme definitions for assessor competence. Scheme procedures for assuring competence (e.g. training course, interview, exam)	IEE/BCS study.
1.2	Use of independent assessors.	Scheme rules for non-involved 3rd party assessors. Scheme guidance on self-certification routes	61508-1,§8
1.3	Defined assessment procedures.	Define a common assessment process that is always followed	Common Schedules Chapter 1, defined
1.4	Defined assessment techniques	Define work instructions for specific assessment techniques. Provide guidance on application of techniques in different situations e.g. sampling levels (see section 3.10.3)	Common Schedules Chapter 2,
1.5	Selection criteria for techniques	Define criteria for selecting techniques.	61508-3, Table A10
1.6	V&V of assessment process	Scheme rules for peer review of assessment reports. Scheme rules for monitoring assessments. Scheme rules for role of Technical Design authority	Common Schedules Chapter 1

3.10.2 RIGOUR OF EVIDENCE (ROE)

This relates to the exactness with no deviation of the evidence that is produced in accordance with 61508. This rigour depends upon the clarity and precision of the requirements in the standard.

	ROE Requirement	CASS approach	Remarks/References
2.1	Separate Targets of Evaluation into 'basic' and 'graded' types.	Indicate in tables as appropriate.	'Basic' means the evidence is unaffected by ROE factors. 'Graded' means the evidence is dependent upon ROE factors. Section 4 of specific assessment type schedules
2.2	Identify 61508 requirements that are unclear (undefined, ambiguous or subjective).	Provide CASS 'clarification' or 'definition' for such requirements on Basic TOEs. Provide CASS 'interpretation' for such requirements on Graded TOEs.	
2.3	Identify factors affecting Rigour of Evidence	These factors are: • SIL • Complexity • Novelty • Consequence of failure • Nature of the hazard • Technology used • System size and distribution • Number of development teams	61508-1, §4
2.4	Provide mechanism to classify overall degree of ROE given the factors	Technical guidance providing a scale for each factor and a technique to combine them.	

3.10.3 SAMPLES

Samples must be chosen such that all of the following elements are covered by the assessment.

a) Each of the applicable FSCA TOEs.
b) Each of the applicable safety lifecycle phases.
c) Each of the locations at which safety lifecycle activities are performed.

Similarly where there are activities within the scope of the assessment that cover different application sectors; different technology types; different products and services, then each of these different elements must also be included in the sample taken.

3.10.3.1 DEPTH OF SAMPLING

Within the framework of the above coverage, evidence must be sampled by the assessor until the evaluation of compliance or not can be made. For some areas this may be 100% sample e.g. the TOE Functional Safety Policy whereas for others it may be a much smaller sample of the total number of objects e.g. Software Module Test Reports.

The following Rigour of Evidence factors should be taken into account when selecting samples.

a) Target Safety Integrity Level
b) Complexity
c) Novelty
d) Consequence of failure
e) Nature of the hazard
f) Technology type used
g) System size and distribution
h) Number of development teams.

Higher sample levels will be needed where one or more of these factors has a significant impact.

Sample levels may also need adjusting during the assessment if problems are found with a specific activity, e.g. Safety Validation Planning. Further samples of that activity should be taken until a firm judgement can be made as to compliance or not.

3.10.3.2 PROJECT BASED ACTIVITIES

Where activities are project-based, a number of approaches are possible. These are:

a) trace forward through the entire project from the earliest lifecycle phase to the last applicable phase;
b) trace backwards through the project investigating how the phase outputs were produced and verified;
c) check one phase in a number of projects.

Note that whole project sampling may not be effective if projects have long timespans or if the Functional Safety Management System has only recently been established. Similarly

where a number of projects are sampled, it is more efficient to check adjacent lifecycle phases as this reduces the time needed to brief the CASS assessor about the overall objectives and status of the project.

Acknowledgements to 'The TickIT Guide' 12 Jan 1998, issue 4.0.

CASS - COMMON SCHEDULES
CHAPTER 4 : GLOSSARY

4.1 INTRODUCTION

This chapter provides definitions and references to definitions for terms used in CASS assessments.
This is done:

a) indirectly by reference alone to IEC 61508-4 where the full definition of the term can be found;
b) directly by explicit definition of the terms and a reference to the source standard for the definition.

4.2 GLOSSARY

Term	Definition	Source
Animation		IEC 61508-4
Architecture		IEC 61508-4
Channel		IEC 61508-4
Common cause failure		IEC 61508-4
Configuration	Functional and physical characteristics of a product as defined in technical documents and achieved in the product.	ISO 10007
Configuration control	Activities comprising the control of changes to a configuration item after formal establishment of its configuration documents.	ISO 10007
Configuration identification	Activities comprising determination of the product structure, selection of configuration items, documenting the configuration item's physical and functional characteristics including interfaces and subsequent changes, and allocating identification characters or numbers to the configuration items and their documents.	ISO 10007
Configuration management		IEC 61508-4
Conformity assessment	Any activity concerned with determining directly or indirectly that relevant requirements are fulfilled Note 1. Typical examples of conformity assessment activities are sampling, testing and inspection, evaluation, verification and assurance of conformity (suppliers declaration, certification), registration, accreditation and approval as well as their combinations.	EN 45020 (ISO/IEC Guide 2:1996)
Cots	Commercial Off The Shelf. See Proprietary.	
Covert		IEC 61508-4

Term	Definition	Source
Criterion	a means or standard of judging	
Dangerous failure		IEC 61508-4
Dependent failure		IEC 61508-4
Detected		IEC 61508-4
Diagnostic coverage		IEC 61508-4
Diagnostic test interval		IEC 61508-4
Diversity		IEC 61508-4
Document	A structured amount of information for human perception, that can be interchanged as a unit between users and/or systems	ISO 8613-1
Dynamic testing		IEC 61508-4
Effectiveness (performance)	1. The ability of an item to meet a service demand of given quantitative characteristics 2. The accuracy and completeness with which users achieve specified goals	1. IEC 50(191) 2. ISO 9241-11
Electrical/electronic/programmable electronic (e/e/pe)		IEC 61508-4
Electrical/electronic/programmable electronic system (e/e/pes)		IEC 61508-4
Equipment under control (euc)		IEC 61508-4
Error		IEC 61508-4
euc control system		IEC 61508-4
euc risk		IEC 61508-4
External risk reduction facility		IEC 61508-4
Failure		IEC 61508-4
Failure mode	The effect by which a failure is observed	BS4778-3.1: 1991
Fault		IEC 61508-4
fault avoidance		IEC 61508-4
fault tolerance		IEC 61508-4
Function	Elementary operation performed by the system which, combined with other elementary operations (system functions), enables the system to perform a task.	BS 61069-1
functional safety		IEC 61508-4
functional safety assessment		IEC 61508-4
functional safety audit		IEC 61508-4
functional unit		IEC 61508-4
hardware safety integrity		IEC 61508-4
harm		IEC 61508-4
hazard		IEC 61508-4
hazardous event		IEC 61508-4
hazardous situation		IEC 61508-4

Term	Definition	Source
human error		IEC 61508-4
impact analysis		IEC 61508-4
implied needs	In a contractual environment, needs are specified, whereas in other environments, implied needs should be identified and defined	ISO 8402: 1994
independent department		IEC 61508-4
independent organisation		IEC 61508-4
independent person		IEC 61508-4
interactive system	Combination of hardware and software components that receive input from and communicate output to a human user in order to support his or her performance of a task	[ISO 13407]
limited variability		IEC 61508-4
logic system		IEC 61508-4
low complexity e/e/pe safety-related system		IEC 61508-4
mistake		IEC 61508-4
mode of operation		IEC 61508-4
modification (of an item)	The combination of all technical and administrative actions intended to change an item.	IEC 50(191)
module		IEC 61508-4
necessary risk reduction		IEC 61508-4
operator	The person or persons given the task of installing, operating, adjusting, maintaining, cleaning, repairing or transporting machinery	BS 292-1
other technology safety-related system		IEC 61508-4
overt		IEC 61508-4
programmable electronic		IEC 61508-4
programmable electronic system (pes)		IEC 61508-4
proof test		IEC 61508-4
proprietary	Legally made only by a person or body of persons having special rights	.
prototype	A model or preliminary implementation suitable for evaluation of system design, performance, and production potential; or for better understanding or determination of the requirements.	ISO / IEC 2382-20: 1990
quality	The totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs	ISO 8402
quality system	The organisational structure, responsibilities, procedures, processes and resources for implementing quality management.	BS 4778-2: 1991
random hardware failure		IEC 61508-4
reasonably foreseeable misuse		IEC 61508-4

Term	Definition	Source
redundancy		IEC 61508-4
redundancy	In an item, the existence of more than one means for performing a required function.	IEC 50
reliability (performance)	The ability of an item to perform a required function under given conditions for a given time interval.	IEC 50(191)
requirement	1: A condition or capability needed by a user to solve a problem or achieve an objective 2: A condition or capability that must be met or possessed by a system or a system component to satisfy a contract, standard, specification or other formally imposed documents	IEE 610.12
revealed		IEC 61508-4
risk		IEC 61508-4
safe failure		IEC 61508-4
safe state		IEC 61508-4
safety		IEC 61508-4
safety function		IEC 61508-4
safety functions requirements specification		IEC 61508-4
safety integrity		IEC 61508-4
safety integrity level (sil)		IEC 61508-4
safety integrity requirements specification		IEC 61508-4
safety lifecycle		IEC 61508-4
safety requirements specification		IEC 61508-4
safety-related software		IEC 61508-4
safety-related system		IEC 61508-4
simulation	The use of a data processing system to represent selected behavioural characteristics of a physical or abstract system	ISO / IEC 2382-20: 1990
software		IEC 61508-4
software lifecycle		IEC 61508-4
software module		IEC 61508-4
software safety integrity		IEC 61508-4
software safety integrity level		IEC 61508-4
source code	Computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler or other translator.	IEEE 610.12
specification	The document that prescribes the requirements with which the product or service has to conform	ISO 8402
system		IEC 61508-4

Term	Definition	Source
system testing	Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.	IEEE 610.12
systematic	Methodical, according to plan and not casually or at random	
systematic failure		IEC 61508-4
systematic safety integrity		IEC 61508-4
target failure measure		IEC 61508-4
task	The smallest indivisible part of an activity when it is broken down to a level best understood an performed by a specific user	BS 4778-3.1: 1991
test harness		IEC 61508-4
tolerable risk		IEC 61508-4
undetected		IEC 61508-4
unrevealed		IEC 61508-4
usability	The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.	ISO 9241-11
user	The individual interacting with the system	ISO 9241-10
user documentation	Documentation describing the way in which a system or component is to be used to obtain desired results.	IEEE 610.12
validation		IEC 61508-4
verification		IEC 61508-4

THE CASS GUIDE

GUIDE TO FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

SECTION THREE

TECHNICAL SCHEDULES FOR FUNCTIONAL SAFETY CAPABILITY ASSESSMENT (FSCA TS)

CONTENTS LIST
FUNCTIONAL SAFETY CAPABILITY ASSESSMENT
-TECHNICAL SCHEDULES

CASS - FSCA TS

CHAPTER 1 : MAPPING TABLE

1.1 INTRODUCTION

References to this document - Functional Safety Capability Assessment, Technical Schedules - are abbreviated to FSCA TS.

The mapping table is used to document the mappings between client documentation and the CASS Targets of Evaluation (TOES) (and hence to the relevant requirements of IEC 61508).

FSCA TS Annex A contains a list of TOEs relevant to all FSC assessments.

FSCA TS Annex B contains a list of TOEs that will be relevant only if the applicable life-cycle phase is appropriate to the assessment scope. The TOEs in FSCA TS Annex B are checked on a sample basis only.

Note: A list of applicable life-cycle phases appropriate to the scope of the company business should already be defined.

CASS - FSCA TS

CHAPTER 2 : ASSESSMENT CRITERIA

2.1 INTRODUCTION

This section identifies for the assessor those clauses within IEC 61508 which are relevant to a Functional Safety Capability Assessment (FSCA).

2.2 CLAUSES RELEVANT FOR FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

The following clauses of IEC 61508 are relevant to a FSCA.

IEC 61508 Part 1 clause 6 – applied to all FSCAs irrespective of scope

IEC 61508 Part 1 clause 8 (Functional Safety Assessment) – the CASS process assessments i.e. the Functional Safety Capability Assessment should include the organisation's approach to FSA as part of the audit check.

IEC 61508 Parts 1, 2 and 3 – the remaining clauses applied to FSCA only as relevant to the declared scope of life-cycle activities for the organisation under assessment.

CASS - FSCATS

CHAPTER 3 : ASSESSMENT MODULES

3.1 INTRODUCTION

This document contains definitions of the assessment modules for FUNCTIONAL SAFETY CAPABILITY assessments.

Each assessment module provides instructions and guidance for the assessment of the Targets of Evaluation (TOEs) and any related activities. The assessment criteria to apply are defined in **FSCATS** Chapter 2; the mapping of criteria to TOEs is in **FSCATS** Chapter 4; and the assessment techniques to use are referenced in the Assessor Notes in **FSCATS** Chapter 4, and addressed in detail in **CASS Scheme Common Schedules,** Chapter 2: Common Schedules - Assessment techniques.

3.2 SCOPE

The modules contained in this document are for use by CASS assessors; they are for a FUNCTIONAL SAFETY CAPABILITY assessment.

The current contents define:

a) the assessment modules needed for the functional safety capability assessment.
b) the mapping of top level assessment modules to sub-modules.
c) the structure and content of Overall sub-modules and Related Activity sub-modules.

3.3 MAPPING OF ASSESSMENT MODULES TO SUB-MODULES

Each CASS Assessment Module consists of a number of Sub-Modules.

Each Sub-Module consists of an assessment of a number of TOEs.

Table 3.1 FUNCTIONAL SAFETY CAPABILITY ASSESSMENT - Mapping of Assessment Modules

Module	Sub-Module
Functional Safety Capability	Safety capability review Safety capability audit Competence audit

3.4 ASSESSMENT MODULE DESCRIPTIONS

3.4.1 INTRODUCTION

This Section defines the top level assessment modules that are performed as part of a Functional Safety Capability assessment.

3.4.2 MODULE: FUNCTIONAL SAFETY CAPABILITY

3.4.2.1 OBJECTIVES

Confirm the adequacy and effectiveness of the functional safety management process of an organisation for developing, supplying, operating &/or maintaining safety-related E/E/PES for given application(s).

3.4.2.2 TARGETS OF EVALUATION

The targets of evaluation of this module are specified in the Sub-modules.

3.4.2.3 OTHER REQUIRED INPUTS

Other inputs are specified in the Sub-modules.

3.4.2.4 ASSESSOR NOTES

Perform the sub-modules:

- Safety capability review
- Safety capability audit
- Competence audit

Note that the sub-module ‘Safety Capability Review’ is normally performed before ‘Safety Capability Audit’. However, these modules may be performed in reverse order at the Lead Assessor’s discretion.

3.5 SUB-MODULE DESCRIPTIONS

3.5.1 INTRODUCTION

This Section defines the sub-modules that are performed as individual elements of Functional Safety Capability Assessment.

Evidence of adequate implementation of functional safety policy and procedures is required. Sample inspection of other TOEs produced by the client will be required to confirm this.

3.5.2 SUB-MODULE: SAFETY CAPABILITY REVIEW

3.5.2.1 OBJECTIVES

- To ensure that the Functional Safety Management system is defined and appropriate to the organisation's claimed capability for functional safety activities.

3.5.2.2 TARGET(S) OF EVALUATION

Note that not all TOEs will be applicable to all FSCAs. The mapping procedures (FSCA TS Chapter 1) will identify life-cycle phases appropriate to the scope of the organisation's business and therefore the TOEs applicable to the FSCA.

Functional Safety Management System
Functional Safety Policy
Organisation and Responsibilities
Identification of relevant life-cycle phases
Documentation structure and content policy
Techniques and Measures conformance plan
Corrective action procedure
Procedure for handling of hazardous incidents
Procedure for O&M performance analysis
Functional safety audit process
Modification process for Safety related systems
Procedures for maintaining information on hazards with respect to Safety-Related Systems
Configuration management procedures
Procedures for provision of training and information for the emergency services
Functional Safety Management System - Formal Reviews
Supplier Assessment Process
Functional Safety Assessment.

3.5.2.3 OTHER REQUIRED INPUTS

None

3.5.2.4 ASSESSOR NOTES

1. The main technique for this work package is Document Inspection.

2. The assessor needs to ensure that all the elements of a functional safety management system relevant to the organisation are in place and suitably defined. A functional safety management system should only be considered compliant provided that there is a positive safety culture to support its effective application (see FSCA TS Annex D).

3. Safety policy, procedures and practices are normally defined by documenting the relevant information. Where other means are used then the technique Process Audit may be needed to check that the procedure or practice is adequately defined.

4. EXCLUSION: The competence assessment process is not checked as part of this sub-module as is the target of a separate sub-module in its own right.

3.5.3 SUB-MODULE: SAFETY CAPABILITY AUDIT

3.5.3.1 OBJECTIVES

- To ensure that the Functional Safety Management system is effectively implemented

3.5.3.2 TARGET(S) OF EVALUATION

Note that not all TOEs will be applicable to all FSCAs. The mapping procedures (FSCA TS Chapter 1) will identify life-cycle phases appropriate to the scope of the organisation's business and therefore the TOEs applicable to the FSCA.

Functional Safety Management System
Functional Safety Policy
Organisation and Responsibilities
Identification of relevant life-cycle phases
Documentation structure and content policy
Techniques and Measures conformance plan
Corrective action procedure
Procedure for handling of hazardous incidents
Procedure for O&M performance analysis
Functional safety audit process
Modification process for Safety related systems
Procedures for maintaining information on hazards with respect to Safety-Related Systems.
Configuration management procedures
Procedures for provision of training and information for the emergency services
Functional Safety Management System - Formal Reviews
Supplier Assessment Process
Functional Safety Assessment.

Sample of Overall TOES (where relevant)
Sample of E/E/PES TOEs (where relevant)
Sample of Software TOEs (where relevant)

3.5.3.3 OTHER REQUIRED INPUTS

None

3.5.3.4 ASSESSOR NOTES

1. The main techniques for this work package is Process Audit.

2. Evidence of adequate implementation of functional safety policy and procedures is required. Sample inspection of other TOEs produced by the client will be required to confirm this.

3. Evidence of an established and effective Quality Management System will reduce the degree of sampling that is required. (Certification of the Quality Management System to acceptable National or International Standards by a recognised authority will provide evidence in this respect).

4. EXCLUSION: The competence assessment process is not checked as part of this sub-module as it is the target of a separate sub-module in its own right.

3.5.4 SUB-MODULE: COMPETENCE AUDIT

3.5.4.1 OBJECTIVES

- To ensure that the Functional Safety Management System competence assessment process is defined and implemented to ensure that parties involved in safety life-cycle activities are competent to perform those activities.

3.5.4.2 TARGET(S) OF EVALUATION

Competence assessment process

3.5.4.3 OTHER REQUIRED INPUTS

Safety Policy
Safety Procedures
Safety Plans
Organisation training plan
Organisation training records
Corrective Action Process.

3.5.4.4 ASSESSOR NOTES

1. The main techniques for this work package are Document Inspection and Process Audit.

2. The assessor should check that the Competence Assessment process of the organisation is defined and consistent with the stated Safety Policy.

3. The assessor should check that the Competence Assessment process is effectively implemented through sample inspection of the records arising from the process. In particular that any identified shortfalls in competence are addressed through appropriate corrective action.

4. The assessor should refer to specific CASS guidance on interpreting the IEC 61508 requirements for competence.

5. The Annex C at the end of the FSCA Technical Schedules contains a set of checklist questions to help guide the CASS assessor.

CASS - FSCATS

CHAPTER 4 : TARGETS OF EVALUATION

4.1 INTRODUCTION

This section provides, for the assessor, specific guidance on the identifiable deliverables or 'assessable objects' associated with those clauses within IEC 61508 which are relevant to a Functional Safety Capability Assessment (FSCA). These deliverables are termed Targets of Evaluation (TOEs).

4.2 MAPPING OF TARGETS OF EVALUATION TO IEC 61508 CLAUSES

4.2.1 MAPPING OF FSCA TOES TO IEC 61508 CLAUSES

Version used: IEC 61508-1:1998

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
1.	Functional Safety Management System	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 (1/6.1.1) The activities specified as a result of 1/6.2.1 shall be implemented and progress monitored	**1/6.2.1** **1/6.2.2** **Evidence from the relevant sub-clauses 1/6.2.1 a) to p) as listed below**	Calls for the following sub clauses which 'should' be considered. Needs to be tailored to business scope and relevant life-cycle phases.
2.	Functional Safety Policy	The policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organisation to ensure a culture of safe working;	**1/6.2.1 a)** **Figs 2,3,4, Table 1, and 1/6.2.1.c as framework.**	There should be a top-level policy statement that reflects the safety goals and objectives of the organisation.

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
3.	Organisation and Responsibilities	Identification of the persons, departments and organisations who perform or review safety life-cycle activities and allocation of responsibilities for those activities. To ensure that all those specified as responsible for management of functional safety activities are informed of the responsibilities assigned to them	**1/6.2.1 b)** **1/6.2.4** **Figs 2,3,4, and 1/ Table 1**	Assessment should verify that the allocation of responsibilities is documented, and covers all of the scope of the assessee activities. This may be presented in: - Organisation Chart - Project Safety Plan This includes where relevant, licensing authorities or safety regulatory bodies. For guidance on level of rigour for this TOE against SIL - refer to TOE 8 for competence of staff in technical positions.
4.	Identification of relevant life-cycle phases	The overall, E/E/PES or software safety life-cycle phases to be applied;	**1/6.2.1 c)** **Figs 2,3,4, and 1/ Table 1**	Should demonstrate understanding of where the assessee activities fit in the overall life-cycle. This could be included as part of the safety plan procedure/ work instruction.

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
5.	Documentation structure and content policy	The way in which information is to be structured and the extent of the information to be documented.	**1/6.2.1 d)** **1/5.0**	
6.	Techniques and Measures conformance plan	The selected measures and techniques used to meet the requirements of a specified clause or sub-clause;	**1/6.2.1.e)** **(see parts 2, 3 and 6)**	This is evidence of a policy in place which pre-defines a general approach by which the assessee intends to comply with the requirements of those clauses. This may include guidelines on the appropriate techniques and measures. See specific TOES for guidance of rigour against SIL
7.	Corrective action procedure	the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations arising from: — hazard and risk, — functional safety assessment, — verification activities, — validation activities, — configuration management;	**1/6.2.1 g)** **Evidence from the relevant sections:** **1/6.2.1o, 1/7.4, 1/7.8, 1/7.14, 1/7.16, 1/7.18, 1/8.0** **Parts 2 and 3** **Figs 2,3,4 and 1/Table 1 as framework.**	

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
8.	Competence assessment process	To define procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety life-cycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified: — the training of staff in diagnosing and repairing faults and in system testing, — the training of operations staff, — the retraining of staff at periodic intervals;	**1/6.2.1 h)** **Figs 2,3,4 and 1/Table 1 as framework.**	**1/Annex B** provides guidelines on the competence requirements of those involved in any overall, E/E/PES or software safety life-cycle activity. Organisation training plan and training records should be reviewed. The IEE/BCS Competency Study may be used as guidance for appropriate competency criteria, and is the basis of the FSCA TS Annex C at the end of the FSCA Technical Schedules: '**Competency Assessment Process Checklist**' which provides further detail and discussion on this topic. Some grading can be inferred from the competency level, but no firm guidelines yet available to match SIL against level of competency

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
9.	Procedure for handling of hazardous incidents.	To define procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;	**1/6.2.1 I)**	Safety logs should be reviewed.
10.	Procedure for O&M performance analysis	To define procedures for analysing operations and maintenance performance. In particular procedures for: — recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which detect recurring faults, — assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system;	**1/6.2.1 j)** **Figs 2,3,4 and 1/Table 1 as framework.**	This TOE is only relevant to organisations performing O&M activities Fig 7 provides example of operations and maintenance activities model. Fig 8 provides example of O&M management model. No guidance on level of rigour for this TOE against SIL – could be linked with the competency of reviewers and authorisers of modifications

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
11.	Functional safety audit process	To define requirements for periodic functional safety audits in accordance with this sub-clause including: — the frequency of the functional safety audits, — consideration as to the level of independence required for those responsible for the audits, the documentation and follow-up activities;	**1/6.2.1 k)**	Assessee should justify the level of independence of those conducting the audits. Audit timetable, audit reports and actions should be reviewed. Guidance given in 1/Tables 4, 1/Table 5 on levels of independence on FSA against SIL
12.	Modification process for Safety related systems	To define the procedures for initiating modifications to the safety-related; To define the required approval procedure and authority for modifications;	**1/6.2.1 l);** **1/6.2.1 m)** **Figs 2,3,4 and 1/Table 1 as framework.** **1/7.16.2.2**	Assessee should demonstrate that modification procedures have been properly planned. Assessor should verify modification request has been properly documented and authorised. There is no direct guidance, but assessor should verify the competence level of the checker / approver

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
13.	Procedures for maintaining information on hazards with respect to Safety-Related Systems.	To define the procedures for maintaining accurate information on potential hazards and safety-related systems;	**1/6.2.1 n)**	Assessor should review the Hazard and Risk Analysis Report.
14.	Configuration management procedures	To define the procedures for configuration management of the E/E/PE safety-related systems during the overall, E/E/PES and software safety life-cycle phases; in particular the following should be specified: — the stage at which formal configuration control is to be implemented, — the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software), — the procedures for preventing unauthorised items from entering service;	**1/6.2.1 o)** **Figs 2,3,4 and 1/Table 1 as framework.** **See also Part 3 – 6.2.3 : Software configuration management**	NOTE: For more details on configuration management see references [45] and [46] in annex C. [45] ISO 10007: 1995, *Quality management – Guidelines for configuration management.* [46] ISO/IEC DIS 12220-2, *Information technology software processes – Software configuration management*
15.	Procedures for provision of training and information for the emergency services.	To provide training and information for the emergency services.	**1/6.2.1 p)**	Note that requirement of this sub-clause may not be mandatory in all cases. Training records should be reviewed (if appropriate).

TOE Ref.	FSCA TOEs **Target of Evaluation**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
16.	Functional Safety Management System - Formal Reviews	To ensure that requirements for functional safety management are formally reviewed by the organisations concerned, and agreement reached.	**1/6.2.3**	General requirement for formal review and decision making procedures relating to clause 6.2.1. Minutes of review meetings and Review documents will be assessed.
17.	Supplier Assessment Process	To ensure that suppliers providing products or services to an organisation having overall responsibility for one or more phases of the safety deliver products or services as specified by that organisation and have an appropriate quality management system.	**1/6.2.5**	Appropriate quality management system may be through certification to recognised national or international standards e.g. ISO 9001. Supplier audit reports, QMS certificates, supplier CASS assessment may be reviewed. No guidance on level of rigour for this TOE against SIL – see Technical note on use of sub-contractors (CASS Common Schedules).
18.	Functional Safety Assessment	To ensure that an organisation's approach to dealing with the Functional Safety Assessment requirements of IEC 61508 has been adequately reviewed.	**1/8.1** **1/8.2**	

4.2.2 MAPPING OF OVERALL (PART 1) TOES TO IEC61508 CLAUSES

Version used: IEC 61508-1:1998

TOE Ref.	OVERALL (Part 1) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
1.	Overall Safety Life-cycle	To structure the development of the overall project into defined phases and activities that will allow the functional safety of the overall project to be developed, maintained, verified etc.	**1/7.1** **1/Figure 2** **1/Table 1**	
2.	Concept Documentation	To develop a level of understanding of the Equipment Under Control (EUC) and it's environment (physical, legislative etc.) to enable other safety life-cycle activities to be carried out satisfactorily.	**1/7.2** **1/ Table 1 [1]**	
3.	Fully Installed E/E/PES	To implement all the requirements of the **Overall Installation Plan**	**1/7.13.2.1** **1/Table 1 [12]**	N/A for guidance of TOES against SIL
4.	Fully Commissioned E/E/PES	To implement all the requirements of the **Overall Commissioning Plan**	**1/7.13.2.3** **1/Table 1 [12]**	N/A for guidance of TOES against SIL
5.	Overall Installation &Commissioning Records	To report the results of the overall installation & commissioning activities	**1/7.13.2.2** **1/7.13.2.4** **1/Table 1 [12]**	N/A for guidance of TOES against SIL
6.	Overall Scope Definition Documents	To determine the boundary of the overall project and determine the scope of the hazard & risk analysis. E.g. process, environmental hazards etc.	**1/7.3** **1/Table 1 [2]**	
7.	Overall Safety Plan	To outline when, how and by whom specific phases within the **Overall Safety Life-cycle** shall be performed.	**Management Of Functional Safety: 1/6.2.1 b) to p)**	

TOE Ref.	OVERALL (Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
8.	Hazard & Risk Analysis Report	To report the results of the hazard and risk analysis throughout the overall life-cycle	**1/7.4** **1/Table 1 [3]**	
9.	Overall Safety Requirements Specification	To specify the overall safety requirements in terms of the **Safety Functions Requirements** and the **Safety Integrity Requirements** for all safety related systems and external risk reduction facilities in order to achieve the required functional safety for the project.	**1/7.5** **1/Table 1 [4]**	
10.	Safety Requirements Allocation Report	To report on: a) the allocation of each safety function and it's associated safety integrity requirement to the designated safety system or external risk reduction facility b) the allocation of a **Safety Integrity Level (SIL)** to each safety function.	**1/7.6** **1/Tables 2 & 3** **1/ Table 1 [5]** **1/Figure 6**	
11.	Overall Safety Validation Plan	To define the steps/procedures for the overall safety validation of the E/E/PE safety related systems against the **Overall Safety Requirements Specification.**	**1/7.8** **1/Table 1 [7]**	
12.	Overall Operation and Maintenance Plan	To define the steps/procedures for operating & maintaining the E/E/PE safety related systems to ensure the required functional safety of the overall system is maintained during operation & maintenance	**1/7.7** **1/Figure 8** **1/Table 1 [6]** **1/Figure 7**	

TOE Ref.	OVERALL (Part 1) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	**Comments**
13.	Overall Installation & Commissioning Plan	To define the steps/procedures for installing & commissioning the E/E/PE safety-related system in a controlled manner to ensure the required functional safety is achieved	**1/7.9 1/7.9.2.1 1/7.9.2.2 1/Table 1 [8]**	
14.	E/E/PE safety-related systems: realisation phase deliverables	To create the E/E/PE safety-related systems conforming to the **E/E/PES Safety Requirements Specification**	**1/7.10 Parts 2 & 3**	**See E/E/PES & Software TOEs**
15.	Other technology safety-related systems: confirmation of realisation phase deliverables	To confirm delivery of all other technology safety-related systems which have been specified as part of the overall safety system	**1/7.11**	**No 61508 requirements. Show evidence of delivery against Overall Safety Requirements Specification**
16.	External Risk Reduction facilities: confirmation of realisation phase deliverables	To confirm delivery of all external risk reduction facilities which have been specified as part of the overall safety system	**1/7.12**	**No 61508 requirements. Show evidence of delivery against Overall Safety Requirements Specification**
17.	Overall Safety Validation Records	To report the results of the overall safety validation against the **Overall Safety Requirements Specification**	**1/7.14 1/Table 1 [13]**	N/A for guidance of TOES against SIL
18.	Overall Operation, Maintenance & Repair Records	To report the results of any operation, maintenance & repair activities	**1/7.15 1/Table 1 [14]**	N/A for guidance of TOES against SIL

TOE Ref.	OVERALL (Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
19.	Overall Modification & Retrofit Records	To report the results of any modification & retrofit activities, indicating any impact on the level of functional safety of the overall system	**1/7.16** **1/Table 1 [15]** **1/Figure 9**	N/A for guidance of TOES against SIL
20.	Decommissioning/disposal Plans & Records	To report the probable impact and results of decommissioning and disposal activities.	**1/7.17** **1/Table 1 [16]**	N/A for guidance of TOES against SIL
21.	Verification Documentation	To demonstrate for each phase of the life-cycle, by review, analysis or test documentation, that the outputs for the phase meet the specified requirements.	**1/7.18**	N/A for guidance of TOES against SIL

4.2.3 2.3 MAPPING OF E/E/PES (PART 2) TOES TO IEC 61508 CLAUSES

Version used: IEC 61508-2 65A/254/FDIS/c2 (1999)

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
1.	E/E/PES Safety Life-cycle	To structure the development of the **E/E/PES** into defined phases and activities that will allow the safety of the **E/E/PES** to be developed/maintained/verified etc.	**2/7.1** **2/7.1.3.3** **2/7.1.3.5**	**2/7.1.3.1** **2/Table 1** **2/7.2 – 2/7.9**	**2/7.1.3.2** **2/7.1.3.4** N/A for guidance of TOES against SIL
2.	Fully Functioning E/E/PES	To satisfy the requirements of the **E/E/PES Design Documentation**.	**2/7.5.2.1** **2/Table 1[9.4]**	**2/7.5.2.2**	**2/7.5.2.3** N/A for guidance of TOES against SIL
3.	Fully Validated E/E/PES	To implement all the requirements of the **E/E/PES Safety Requirements Specification** (2/7.7.1).	**2/Table 1[9.6]**	**2/7.7.1**	N/A for guidance of TOES against SIL
4.	E/E/PES Safety Plan	To define all the management and technical activities during the **E/E/PES Safety Life-cycle** that are necessary to ensure that the safety related systems and external risk reduction facilities achieve and maintain the required functional safety (1/6.2.1).	**1/6.2.1 a-p** **1/6.2.4**	**1/6.2.2** **1/6.2.5**	**1/6.2.3**

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
5.	E/E/PES Safety Requirements Specification	To identify the safety functions requirements and safety integrity requirements for each **E/E/PES** (2/7.2.1).	**2/Table 1[9.1]** **2/7.2.2.3** **2/7.2.3.3**	**2/7.2.2.1** **2/7.2.3.1 a-j**	**2/7.2.2.2** **2/7.2.3.2 a-e**
6.	E/E/PES Safety Validation Plan	To define the steps/procedures to be used to validate the **E/E/PES** against the **E/E/PES Safety Requirements Specification** (2/7.3.2.1)	**2/7.3.2.1** **2/Table B.5** Guidance on SIL level given in table	**2/7.3.2.2 a-g**	**2/7.7.2.7**
7.	E/E/PES Design Documentation	To define and justify the architectural design, detailed design and hardware implementation of the **E/E/PES** that meets the requirements of **the E/E/PES Safety Requirements Specification** (2/7.4.1). This includes sub-system/component design and test specifications where relevant.	**2/Table 1[9.3]** **2/7.4.2.8** **2/7.4.3** **2/7.4.3.1.3** **2/7.4.5.2** **2/7.4.5.3** **2/7.4.7.1** **2/7.4.7.2** **2/7.4.7.7** **2/7.4.4.1** **2/7.4.4.2** **2/7.4.4.3** **2/7.4.4.4** **2/7.4.4.5** **2/7.4.4.6**	**2/7.4.2.1** **2/7.4.2.9** **2/7.4.3.1.1** **2/7.4.3.1.4** **(Tables 2 & 3)** **2/7.4.7.3 a-o** **2/7.4.7.4** **2/7.4.7.6** **2/7.4.7.8** **2/7.4.7.9** **2/7.4.7.11 a-d** **2/7.4.7.12** **2/7.4.8.1** **2/7.4.8.2**	**2/7.4.2.2** **2/7.4.2.11** **2/7.4.3.1.2** **2/7.4.5.1** **Annex A – Tables A1,A2,A3, A4,A14, A15,A16 A17,A18** Guidance on SIL levels given in referenced tables

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
8.	E/E/PES Integration and Test Specification	To define the steps/procedures for integrating the software and hardware of the **E/E/PES** and to define the tests that will demonstrate that the integrated **E/E/PES** satisfies the **E/E/PES Design Documentation** (2/7.4.7.5).	**2/7.4.4.5** **2/Table B.3**	**2/7.9.2.10** Guidance on SIL levels given in table	**2/7.5.2.7**
9.	E/E/PES Integration and Test Report	To report the results (detailed and overall) of the integration testing.	**2/7.5.2.4** **2/7.5.2.5**	**2/7.5.2.6**	**2/7.9.2.10 [for (e)]**
10.	E/E/PES Integration and Test Log	To provide a chronological record of the integration and integration testing.	**2/Table 1[9.4]**		
11.	E/E/PES Operation and Maintenance Procedures	To define the procedures to be used to maintain the functional safety of the **E/E/PES** during operation and maintenance (2/7.6.1).	**2/7.6.2.1** **2/7.6.2.2** **2/7.6.2.5**	**2/7.6.2.4** **2/7.4.4.3** **2/Table B.4** Some guidance on SIL level given in Table B.4	**2/7.6.2.1 a-g** **2/7.6.2.3**
12.	E/E/PES Safety Validation Report	To report all the results (detailed and overall) of the **E/E/PES Safety Validation** (2/7.7.2.4).	**2/7.7.2.4 a-e** **2/7.7.2.3** **2/7.7.2.7**	**2/7.7.2.1** **2/7.7.2.5**	**2/7.7.2.2** **2/7.7.2.6**

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
13.	E/E/PES Safety Validation Log	To provide a chronological record of the **E/E/PES Safety Validation** (2/7.7.2.4).	**2/Table 1[9.6]** **2/7.7.2.7** **2/Table B.5** Some guidance on SIL level given in Table B5	**2/7.7.2.1** **2/7.7.2.4**	**2/7.7.2.2** **2/7.7.2.5**
14.	E/E/PES Modification Procedures	To define the procedures to be used during modification of the **E/E/PES**; the procedures should ensure that the safety of the **E/E/PES** is maintained. It was decided that modification is distinct from maintenance. Modification can occur from early stages in the life-cycle and can occur independently of the **E/E/PES**'s use in a system, whereas maintenance occurs only after use of the **E/E/PES** in a system.	**2/7.8.2.1 a-I** **2/7.8.2.3** Requires same level of expertise (competence) as design	**2/7.5.2.5** **2/7.8.2.4**	**1/7.16.2.6**
15.	E/E/PES Modification Report	To record all change requests for the **E/E/PES**, their impact and progress.	**2/Table 1**		
16.	E/E/PES Modification Log	To record all change requests for the **E/E/PES**, their impact and progress (2/7.8.2.1).	**2/7.8.2.1**	**2/7.8.2.3** Requires same level of expertise (competence) as design	**2/7.8.2.1 a-i**

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
17.	E/E/PES Safety Requirements Specification - Verification Plan	To define how the **E/E/PES Safety Requirements Specification** will be verified against the **Safety Requirements Allocation Description.**	**2/7.9.2.7**		
18.	E/E/PES Validation Planning - Verification Plan	To define how **the E/E/PES Safety Validation Plan** will be verified against the **E/E/PES Safety Requirements Specification**.	**2/7.9.2.1** **2/7.9.2.4**	**2/7.9.2.2** **2/7.9.2.6**	**2/7.9.2.3**
19.	E/E/PES Design and Development - Verification Plan	To define how the following verifications will be performed: a) E/E/PES Design Documentation against the E/E/PES Safety Requirements Specification (2/7.9.2.8) b) each representation of the E/E/PES Design Documentation against the previous level of representation (2/7.9.2.8) c) E/E/PES Integration and Test Specification against the E/E/PES Design Documentation (2/7.9.2.8).	**2/7.9.2.1** **2/7.9.2.4** **2/7.9.2.8**	**2/7.9.2.2** **2/7.9.2.5** **2/Table B.5** Some guidance on SIL level from Table B5	**2/7.9.2.3** **2/7.9.2.6**

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**	
20.	E/E/PES Integration - Verification Plan	To define how **the E/E/PES Integration and Test Report, E/E/PES Integration and Test Log** and E/E/PES will be verified against the **E/E/PES Integration and Test Specification** (2/7.9.2.9).	**2/7.9.2.9**	
21.	E/E/PES Operation and Maintenance Procedures - Verification Plan	To define how the **E/E/PES Operation and Maintenance Procedures** will be verified against the **E/E/PES Safety Requirements Specification** and **E/E/PES Design Documentation.**		N/A for guidance of TOES against SIL
22.	E/E/PES Safety Validation - Verification Plan	To define how the **E/E/PES, E/E/PES Safety Validation Report and E/E/PES Safety Validation Log** will be verified against the **E/E/PES Safety Validation Plan** and the **E/E/PES Safety Requirements Specification.**		N/A for guidance of TOES against SIL

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**
23.	E/E/PES Modification - Verification Plan	To define how **the E/E/PES Modification Report** and **E/E/PES Modification Log** will be verified against the **E/E/PES Safety Requirements Specification** and **E/E/PES Modification Procedures.**	N/A for guidance of TOES against SIL
	Standard Attributes for each Verification Report	These generic attributes apply to each Verification Report. The individual reports are identified in the following rows of the table.	**2/7.9.2.6** N/A for guidance of TOES against SIL
24.	E/E/PES Safety Requirements Specification - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL
25.	E/E/PES Validation Planning - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL
26.	E/E/PES Design and Development - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL
27.	E/E/PES Integration - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL
28.	E/E/PES Operation and Maintenance Procedures - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL

TOE Ref	E/E/PES (Part 2) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**
29.	E/E/PES Safety Validation - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL
30.	E/E/PES Modification - Verification Report	To report the results of the corresponding verification activities.	N/A for guidance of TOES against SIL

4.2.4 MAPPING OF SOFTWARE (PART 3) TOES TO IEC 61508 CLAUSES

Version used: IEC 61508-3, Version 4.0, 5/12/97

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
1.	Software Safety Life-cycle	To structure the development of the software into defined phases and activities.	**3/7.1.1** **3/7.1.2.3** **3/7.1.2.5**	**3/7.1.2.1** **3/Table 1** **3/7.1.2.6**	**3/7.1.2.2** **3/7.1.2.4** **3/7.1.2.7** Some guidance on SIL levels given in 3/Annex A & B
2.	Software Configuration Management	To develop procedures to apply the administrative and technical controls to identify uniquely and to record accurately the software components necessary to maintain the safety integrity of the E/E/PES Safety Related System. This involves the establishment of change controls procedures and modification approvals adequate to permit the reconstruction of any configuration baseline. The Configuration Management process is required to record formally the release of software.	**1/6.2.1 o**	**3/6.2.3 a-f**	

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
3.	Fully Functioning Software and PE	To provide a complete software system on PE for validation testing.	**3/7.5.2.1** **3/Table 1[9.4]** **3/7.5.2.6**	**3/7.5.2.2** **3/7.5.2.4** **3/7.5.2.7**	**3/7.5.2.3** **3/7.5.2.5** **3/7.5.2.8** See specific TOES for guidance against SIL
4.	Fully Validated Software and PE	To ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.	**3/Table 1[9.6]** **3/7.7.2.4 a-f** **3/7.7.2.8**	**3/7.7.2.2** **3/7.7.2.6 a-c**	**3/7.7.2.3** **3/7.7.2.7** See specific TOES for guidance against SIL
5.	Software Safety Plan	To define the strategy for the software procurement, development, integration, verification, validation and modification to the extent required by the SIL of the E/E/PE safety related system.	**1/6.2.1 a-p** **1/6.2.4** **3/6.2.3**	**1/6.2.2** **1/6.2.5**	**1/6.2.3** **3/6.2.2**
6.	Software Safety Requirements Specification	To identify the safety functions requirements and safety integrity requirements for the software system (3/7.2.1).	**3/Table 1[9.1]** **3/7.2.2.3** **3/7.2.2.8** **3/7.2.2.11 a-b**	**3/7.2.2.2** **3/7.2.2.6** **3/7.2.2.9 a-d** **Table A.1** Guidance on SIL levels given in table A1	**3/7.2.2.4 a-f** **3/7.2.2.7** **3/7.2.2.10**

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
7.	Software Safety Validation Plan	To define the steps/procedures to be used to validate the software against the **Software Safety Requirements Specification** (3/7.3.2.1)	3/7.3.2.1 **3/Table A.7** Guidance on SIL levels given in table A7	**3/7.3.2.2 a-j** **3/7.3.2.4**	**3/7.3.2.3** **3/7.3.2.5**
8.	Software Architecture Design Description.	To define and justify the software architecture which meets the **Software Safety Requirements Specification.**	**3/Table 1[9.3]** **3/7.4.3.3**	**3/7.4.3.1 Annex Tables** **A.2, B.7** Guidance on SIL levels given in tables A2, B7	**3/7.4.3.2 a-f**
9.	Coding Manual	To define programming practices to be used and the procedures for source code documentation.	**3/Table 1[9.3]** **3/7.4.4.3 a-e** **3/7.4.4.6 a-d**	**3/7.4.4.1** **3/7.4.4.4** Annex A – Tables A.3	**3/7.4.4.2** **3/7.4.4.5** Guidance on SIL levels given in table A3
10.	Software System Design Specification	To define the major components and subsystems of the software system.	**3/Table 1[9.3]** **3/7.4.5.3** **Annex Tables A.4,B.1,B.7** **B.9**	**3/7.4.5.1** **3/7.4.5.5**	**3/7.4.5.2** Guidance on SIL levels given in tables A4, B1, B7, B9
11.	Software Module Design Specification	To define the detailed design of each module required by the Software Design Specification.	**3/Table 1[9.3]**	**3/7.4.5.4**	

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
12.	Software Module Source Code Listing	To define source code that meets the Software Module Design specification.	**3/Table 1[9.3]** **Annex Tables** **A.4,B.1,B.7** **B.9**	**3/7.4.6.1 a-d**	**3/7.4.6.2** Guidance on SIL levels given in tables A.4,B.1,B.7 B.9
13.	Software Module Test Specification	To define the steps and procedures to test the source code of a module against its Software Module Design Specification.	**3/Table 1[9.3]** **3/7.4.7.2** **Annex Tables** **A.5,B.2,B.3** **B.6**	**3/7.4.5.4** **3/7.4.7.3**	**3/7.4.7.1** **3/7.4.7.4** Guidance on SIL levels given in tables A.5,B.2,B.3 B.6
14.	Software System Integration and Test Specification	To define the steps/procedures for integrating the software modules into software systems and define the tests to demonstrate that the software modules interact correctly in accordance with the Software System design Specification. (3/7.4.8).	**3/7.4.7.1** **3/7.4.8.1** **3/7.4.8.4**	**3/7.4.7.2** **3/7.4.8.2 a-f** **Annex Tables** **A5** **B2,B3,B6**	**3/7.4.7.3** **3/7.4.8.3** Guidance on SIL levels given in tables A5 B2,B3,B6
15.	Software Architecture Integration and Test Specification	To define the steps and procedures for integrating the software systems and the tests to demonstrate that the software systems interact correctly in accordance with the Software Architecture Design Specification.	**3/Table 1[9.3]** **3/7.4.8.3** **Annex Tables** **A.5,B.2,B.3,** **B.6**	**3/7.4.8.1** **3/7.4.8.4**	**3/7.4.8.2 a-f** **3/7.4.8.5** Guidance on SIL levels given in tables A.5,B.2,B.3, B.6

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**
16.	PE and Software Integration Test Specification	To define the steps for integrating the software onto the target programmable electronics and to plan and define the testing which will demonstrate their compatibility in meeting the Software Safety Requirements Specification and the E/E/PES Hardware Architecture Design. (**3/7.5.1.1 and 3/7.5.1.2**)	**3/Table 1[9.4] 3/7.5.2.1 3/7.5.2.3 3/7.5.2.4 a-c 3/7.5.2.5 3/7.5.2.6 3/7.5.2.7 3/7.5.2.8**
17.	Software Operation and Modification Procedures	To provide information and procedures concerning software necessary to ensure the functional safety of the safety-related system is maintained during operation and modification. (**3/7.6.1**)	**3/Table 1[9.5] 3/7.8 2/7.6.2.1 a-g** Guidance on SIL levels given in table A8 **2/7.6 Annex Table 2/7.6.2.2 A.8**
18.	Software Modification Procedures	To define procedures for making corrections, enhancements or adaptations to the validated software, ensuring that the required Software safety Integrity Level is sustained. (**3/7.8.1**)	**3/7.8.2.1 2/7.5.2.5 1/7.16.2.6 3/7.8.2.2 a-c 3/7.8.2.3 a-b 3/7.8.2.4 3/7.8.2.5 3/7.8.2.6 a-d 3/7.8.2.8 a-3/7.8.2.9**
19.	Software Module Test Log	To provide a chronological record of the software module testing. (*N.B. Not required explicitly by IEC61508*)	
20.	Software Module Test Report	To report the results of software module testing	**3/7.4.7.3** N/A for guidance of TOES against SIL
21.	Software System Integration and Test Log	To provide a chronological record of the software system integration and testing.	**3/7.5.2.7** N/A for guidance of TOES against SIL

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
22.	Software Integration and Test Report	To report the results of integrating and testing the software system against the Software System Integration and Test Specification.	**3/Table 1[9.4]**	**3/7.4.8.4**	N/A for guidance of TOES against SIL
23.	Software Architecture Integration and Test Log	To provide a chronological record of the software architecture integration and testing.			
24.	Software Architecture Integration and Test Report	To report the results of integrating and testing the integrated software systems against the Software Architecture Integration and Test Specification.	**3/7.4.8.4**		N/A for guidance of TOES against SIL
25.	PE and Software Integration Test Log	To provide a chronological record of the programmable electronics and software integration and testing.	**3/7.5.2.7**		N/A for guidance of TOES against SIL
26.	PE AND SOFTWARE INTEGRATION TEST REPORT	To report the results of testing against the PE and Software Integration Test Specification.	**3/7.5.2.8**		N/A for guidance of TOES against SIL
27.	SOFTWARE SAFETY VALIDATION LOG	To provide a chronological record of the **Software Safety Validation** (3/7.7.1.1).	**3/7.7.2.3**		N/A for guidance of TOES against SIL
28.	SOFTWARE SAFETY VALIDATION REPORT	To report all the results (detailed and overall) of the **Software Safety Validation** (3/7.7.1.1).	**3/7.7.2.6 a-c** **Annex Table A.7,B.3,B.5** Guidance on SIL levels given in tables A7,B3, B5	**3/7.7.2.4 a-f** **3/7.7.2.7 a-b**	**3/7.7.2.5** **3/7.7.2.8 a-c**

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
29.	Software Modification Log	To record the details of all software modifications, their impacts and progress (3/7.8.1)	**3/7.8.2.4**	**2/7.8.2.8 a-e**	**2/7.8.2.9** N/A for guidance of TOES against SIL
30.	Software Modification Report	To record all change requests for the **PES software**, their impact and progress.	**3/Table 1[9.5]**	**3/7.8.2.8 a-e**	N/A for guidance of TOES against SIL
31.	Software Safety Requirements Specification - Verification Plan	To define how the **Software Safety Requirements Specification** will be verified against the **E/E/PES Safety Requirement Specification** for functionality, safety integrity, performance and any other requirements of safety planning.	**3/7.9.2.8 a-c**		Some guidance on SIL levels given in table A9, B2 and B8
32.	Software Safety Validation Planning - Verification Plan	To define the activities to verify the outputs of the software safety validation planning phase (**Software Safety Validation Plan**) against the Software Safety.	**3/7.9.2.8 a-c**		**2/7.2** Some guidance on SIL levels given in table A9, B2 and B8

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
33.	Software Design and Development - Verification Plan	To define the activities to verify the outputs of the software design and development phase (Software Architecture Design Description, Coding Manual, Software System Design Specification, Software Module Design Specification, Source Code Listings, Software Integration and Test Specification, Software Architecture Integration and Test Specification, and Verified Integrated Software Systems) against the inputs of the phase (Software Safety Requirement Specification and E/E/PES Hardware Architecture Design).	**3/7.9.2.9 a-d** **3/7.9.2.11 a-d** **3/7.9.2.13 a-e**	**3/7.2** **3/7.9.2.12**	**3/7.9.2.10 a-d** Some guidance on SIL levels given in table A9, B2 and B8
34.	PE and Software Integration - Verification Plan	To define the activities to verify the outputs of the PE and Software Integration phase (Fully Functioning PE and Software) against the inputs of the phase.	**3/7.9.2.4**	**3/7.5.2.5**	**3/7.5.2.8** Some guidance on SIL levels given in table A9, B2 and B8
35.	Software Operation and Modification Procedures - Verification Plan	To define the activities to verify the Software Operation and Modification Procedures against the Software Safety Requirement Specification.			Some guidance on SIL levels given in table A9, B2 and B8

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
36.	Software Safety Validation - Verification Plan	To define the activities to verify the outputs of the software Safety Validation (Software Safety Validation Report and Validated Software) against the Software Safety Validation Plan and Software Operation and Modification Procedures.	**3/7.9.2.4**		Some guidance on SIL levels given in table A9, B2 and B8
37.	Software Modification - Verification Plan	To define how the Software Modification Report and Software Modification Log will be verified against the Software Safety Requirements Specification and Software Modification Procedures.			Some guidance on SIL levels given in table A9, B2 and B8
	Standard Attributes for each Verification Report	These generic attributes apply to each Verification Report. The individual reports are identified in the following rows of the table.	**3/7.9.2.4**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
38.	Software Safety Requirements Specification – Verification Report	To report the results of the activities of the Software Safety Requirements – Verification Plan .	**3/7.9.2.4** **3/7.9.2.8 a-c**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
39.	Software Safety Validation Planning – Verification Report	To report the results of the corresponding plan to verify the outputs of the Software Validation phase (Software Safety Validation Plan) against the Software Safety Requirements Specification.	**3/7.9.2.4**	**3/7.9.2.5**	3/7.9.2.6 N/A for guidance of TOES against SIL

TOE Ref	SOFTWARE (Part 3) **Target of Evaluation (TOE)**	**Purpose of TOE**	**Referring IEC 61508 Clauses and Tables**		
40.	Software Design and Development – Verification Report	To report the results of the activities of the corresponding verification plan.	**3/7.9.2.4** **3/7.9.2.9 a-d** **3/7.9.2.12**	**3/7.9.2.5** **3/7.9.2.10 a-d**	**3/7.9.2.6** **3/7.9.2.11 a-e** N/A for guidance of TOES against SIL
41.	PE and Software Integration - Verification Report	To report the results of the corresponding verification activities.	**3/7.9.2.4**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
42.	Software Operation and Modification Procedures - Verification Report	To report the results of the corresponding verification activities.	**3/7.9.2.4**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
43.	Software Safety Validation - Verification Report	To report the results of the corresponding verification activities.	**3/7.9.2.4**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
44.	Software Modification - Verification Report	To report the results of the verification of the Software Modification. *The verification will depend on the phases of the Life-cycle affected by the modification*.	**3/7.9.2.4**	**3/7.9.2.5**	**3/7.9.2.6** N/A for guidance of TOES against SIL
45.	Development Tools	To provide a suitable set of development tools for the required safety integrity level.	**3/7.4.4.2**		Some guidance of SIL in Table A3

CASS - FSCATS
ANNEX A : MAPPING MATRIX FOR FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

CASS Functional Safety Capability TOE	Evidence	Location	Comments
Functional Safety Management System			
Functional Safety Policy			
Organisation and Responsibilities			
Identification of relevant life-cycle phases			
Documentation structure and content policy			
Techniques and Measures conformance plan			
Corrective action procedure			
Competence assessment process			
Procedure for handling of hazardous incidents			
Procedure for O&M performance analysis			
Functional safety audit process			
Modification process for safety related systems			
Procedures for maintaining information on hazards with respect to Safety-Related Systems			
Configuration management procedures			
Procedures for provision of training and information for the emergency services			
Functional Safety Management System - Formal Reviews			
Supplier Assessment Process			
Functional Safety Assessment			
Overall TOES (sample)			See Annex B
E/E/PES TOES (sample)			See Annex B

CASS Functional Safety Capability TOE	Evidence	Location	Comments
Software TOES (sample)			See Annex B

CASS - FSCATS
ANNEX B : MAPPING MATRIX FOR SAMPLE TARGETS OF EVALUATION

B.1 MAPPING MATRIX- OVERALL TOES

OVERALL TOEs	Evidence	Location	Comments
Overall Safety Life-cycle			
Concept			
Fully Installed E/E/PES			
Fully Commissioned E/E/PES			
Overall Installation &Commissioning Records			
Overall Scope Definition Documents			
Overall Safety Plan			
Hazard & Risk Analysis Report			
Overall Safety Requirements Specification			
Safety Requirements Allocation Report			
Overall Safety Validation Plan			
Overall Operation and Maintenance Plan			
Overall Installation & Commissioning Plan			
E/E/PE safety-related systems: realisation phase deliverable			

OVERALL TOEs	Evidence	Location	Comments
Other technology safety-related systems: confirmation of realisation phase deliverables			
External Risk Reduction facilities: confirmation of realisation phase deliverables			
Overall Safety Validation Records			
Overall Operation, Maintenance & Repair Records			
Overall Modification & Retrofit Records			
Decommissioning/disposal Plans & Records			
Verification Documentation			

B.2 MAPPING MATRIX- E/E/PES TOES

E/E/PES TOES	Evidence	Location	Comments
Process Objects			
E/E/PES Safety Life-cycle			
E/E/PES Objects			
Fully Functioning E/E/PES			
Fully Validated E/E/PES			
Documentation Objects			
E/E/PES Safety Plan			
E/E/PES Safety Requirements Specification			
E/E/PES Safety Validation Plan			
E/E/PES Design Documentation			
E/E/PES Integration and Test Specification			
E/E/PES Integration and Test Report			
E/E/PES Integration and Test Log			
E/E/PES Operation and Maintenance Procedures			
E/E/PES Safety Validation Report			
E/E/PES Safety Validation Log			
E/E/PES Modification Procedures			
E/E/PES Modification Report			

E/E/PES TOES	Evidence	Location	Comments
E/E/PES Modification Log			
Verification Plans			
E/E/PES Safety Requirements Specification - Verification Plan			
E/E/PES Validation Planning - Verification Plan			
E/E/PES Design and Development - Verification Plan			
E/E/PES Integration - Verification Plan			
E/E/PES Operation and Maintenance Procedures - Verification Plan			
E/E/PES Safety Validation - Verification Plan			
E/E/PES Modification - Verification Plan			
Verification Reports			
E/E/PES Safety Requirements Specification - Verification Report			
E/E/PES Validation Planning - Verification Report			
E/E/PES Design and Development - Verification Report			
E/E/PES Integration - Verification Report			
E/E/PES Operation and Maintenance Procedures - Verification Report			
E/E/PES Safety Validation - Verification Report			
E/E/PES Modification - Verification Report			

B.3 MAPPING MATRIX- SOFTWARE TOES

SOFTWARE TOES	Evidence	Location	Comments
Processes			
Software Safety Life Cycle			
Software Configuration Management			
Software And PE			
Fully Functioning Software and PE			
Fully Validated Software and PE			
Documents			
Software Safety Plan			
Software Safety Requirements Specification			
Software Safety Validation Plan			
Software Architecture Design Description			
Coding Manual			
Software System Design Specification			
Software Module Design Specification			
Software Module Source Code Listing			
Software Module Test Specification			
Software System Integration and Test Specification			
Software Architecture Integration and Test Specification			

SOFTWARE TOES	Evidence	Location	Comments
PE and Software Integration Test Specification			
Software Operation and Maintenance Procedures			
Software Modification Procedures			
Test Logs/Reports			
Module Test Log			
Software Module Test Report			
Software System Integration and Test Log			
Software System Integration and Test Report			
Software Architecture Integration and Test Log			
Software Architecture Integration and Test Report			
PE and Software Integration Test Log			
PE and Software Integration Test Report			
Software Safety Validation Log			
Software Safety Validation Report			
Software Modification Log			
Software Modification Report			
Verification Plans			
Software Safety Requirements - Verification Plan			
Software Safety Validation Planning - Verification Plan			
Software Design and Development- Verification Plan			

SOFTWARE TOES	Evidence	Location	Comments
PE and Software Integration - Verification Plan			
Software Operation and Maintenance Procedures - Verification Plan			
Software Safety Validation - Verification Plan			
Software Modification - Verification Plan			
Verification Reports			
Software Safety Requirements - Verification Report			
Software Safety Validation planning - Verification Report			
Software Design and Development - Verification Report			
PE and Software Integration - Verification Report			
Software Operation and Maintenance Procedures - Verification Report			
Software Safety Validation - Verification Report			
Software Modification - Verification Report			
Resources			
Development Tools			

ANNEX C : COMPETENCY ASSESSMENT PROCESS CHECKLIST

C.1 PURPOSE

The purpose of this checklist is to improve the repeatability and consistency of CASS assessments of a competency assessment process. It is in two parts the first deals with the existence of a competency assessment process the second deals with the use of specific competency factors.

This guidance note defines the types of evidence that a CASS assessor might expect to see when examining the competency assessment process within an organisation. The relevant sections of IEC 61508 are Part 1 clause 6.2.1h and Annex B. These define the overall requirement for competence and the factors to be addressed by a competency assessment process. Where available, types of evidence for each factor are taken from the detailed descriptions given in the IEE/BCS competency study, with the reference from the study.

Failures to comply with the requirements of the guidance checklist can only be highlighted as observations by the CASS assessor. However, the issue of competence is defined in general terms in the normative section of IEC 61508 Part 1, Clause 6.2.1h. The CASS assessor could raise non-conformances against this if the competency process is incomplete or deficient.

The competency indicators listed in the checklist will be investigated by the CASS assessor by inspecting a sample of training or experience records. The CASS assessor will not perform individual competency assessments as part of the FSCA assessment, the interest is in the process, not the individual.

References to the IEE/BCS study are to the document: ‘Safety, Competency and Commitment’ Published February 2000.

C.2 COMPETENCY ASSESSMENT PROCESS

This checklist investigates if a rational process is in place to assess the competency needs for an activity, and match the correct level of staff competency to the activity. Any remedial action, such as training or development, may be required.

The use of sub-contractors or suppliers for specific tasks may require the organisation with responsibility for the task to examine or enquire about the competency to task allocation process in use by the sub-contractor.

	Evidence
IDENTIFICATION OF COMPETENCY LEVELS/ SKILLS NEEDED FOR ACTIVITY	
Availability of information on staff competency levels/ skills	
Matching competency needs with available staff	
Training / development / recruitment instigated if competency needs not matched by available resources	
Repeat process until competency needs are fulfilled	
Examination of the competency to task allocation process used by sub-contractors or suppliers if applicable.	

Further indicators of an effective competence process within an organisation are provided by the report 'Successful Health & Safety Management', HS(G) 25, HSE 1993:
Arrangements made by companies who manage functional safety well will include:

- Recruitment and placement procedures which ensure that employees (including those at all levels of management) have the necessary mental abilities for their jobs, or can acquire these through training and experience.
- Systems to identify functional safety training needs arising from recruitment, changes in staff, plant, substances, technology, processes or working practices; the need to maintain or enhance competence by refresher training; and the presence of contractors' employees, self-employed people or temporary workers;
- Systems to provide the information, instruction, training and supporting communications effort needed to meet these needs;
- Arrangements to ensure competent cover for staff absences, particularly for staff with critical functional safety responsibilities.

C.3 COMPETENCY INDICATORS

These checklists contains general indicators which apply across all activities and task specific indicators which will need interpreting by the CASS assessor depending upon the task or role being checked.

C.3.1 ENGINEERING KNOWLEDGE APPROPRIATE TO THE APPLICATION AREA

(IEE/BCS references for general and task specific indicators: HRA8, SRS4, SV7, SAD4, and SHR8)

	Evidence
General indicators	
HAS HAD PRACTICAL WORK EXPERIENCE WITHIN THE RELEVANT INDUSTRY SECTOR AND WITH THE RELEVANT SAFETY RELATED SYSTEM APPLICATIONS	
Has done practical work on safety related applications within the relevant industry sector and can describe the key safety requirements for the safety related system	
Is familiar with the history of the development of safety philosophy and standards for the domain and the way in which previous incidents have influenced that development	
Task specific indicators	
Has written safety requirement specifications and can illustrate the key safety requirements for a safety-related system within the domain	
Can illustrate through working notes and safety validation plans, how domain specific safety requirements have been assessed during safety validation activities	
Knows the key issues relating to the environment in which the safety related systems are required to operate, their key modes of operation and typical architectural design solutions	
Constantly reflects relevant domain specific requirements in safety related system hardware design solutions	

C.3.2 ENGINEERING KNOWLEDGE APPROPRIATE TO THE TECHNOLOGY

(IEE/BCS study references for general and task specific indicators: SAD3 SAD6, SHR2)

	Evidence
General indicators	
Understands current engineering technologies and safe architecture design techniques relevant to safety related systems	
Has practical experience of the use of relevant technologies	
Task specific indicators	
Knows the standards and guidelines applicable to the notations and conventions used for specifying architectural designs	
Has prepared design specifications using relevant notations and conventions	
Has specified safety related system architectures, using the relevant notations and convention, in a way that clearly indicates where safety functions are to be implemented and how different sub-systems interact	

C.3.3 SAFETY ENGINEERING KNOWLEDGE APPROPRIATE TO THE TECHNOLOGY

(IEE/BCS study references for general and task specific indicators: CFM13, SRM15, ISA13, SRS5, and HF12)

	Evidence
General indicators	
HAS WORKED ON A SAFETY RELATED PROJECT RELATING TO THE CONTEXT WITHIN WHICH THE ORGANISATION OPERATES AND HAS GAINED KNOWLEDGE OF HOW SAFETY IS ADDRESSED WITHIN THE ORGANISATION	
Can describe relevant technologies and how they may be used for safety related work in the domain of interest	
Can explain basic functional safety practices employed in safety related applications within the industry	
Can explain how safety assurance has been achieved with reference to examples from actual project involvement	
Task specific indicators	
Can explain how safety assurance has been achieved, in relation to safety related maintenance and modification activities, with reference to examples from actual project involvement	

C.3.4 KNOWLEDGE OF THE LEGAL AND SAFETY REGULATORY FRAMEWORK

(IEE/BCS study references for general and task specific indicators: CFM7, PSM9, SRM12, ISA14, HRA7, SV8, SHR7, SSR8, HF10, and HF12.)

	Evidence
General indicators	
IS AWARE OF THE REQUIREMENTS OF THE RELEVANT FUNCTIONAL SAFETY STANDARDS APPROPRIATE TO THE INDUSTRY SECTOR	
Can describe and explain the key principles underlying the relevant regulatory regime and associated legal issues.	
Can identify the safety regulations and standards relevant to the domain within which the organisation operates and can describe their key requirements	
UNDERSTANDS THE PRINCIPLES OF FUNCTIONAL SAFETY ASSURANCE.	
Has read, and has a knowledge of, the safety assurance standards appropriate to the industry sector.	
Can explain how safety assurance has been achieved with reference to examples from actual project involvement.	
Can cite relevant safety assurance standards, can explain the fundamental concepts within them, and can identify the differences between them	
Task specific indicators	
Can illustrate through safety plans and maintenance and modification manuals, how safety regulatory requirements and legal issues are addressed in the performance of safety related system maintenance and modification activities	
Understands the key requirements of hardware safety regulations and standards relevant to the domain within which the organisation operates	
Understands the key requirements of the main software safety regulations and standards relevant to the domain within which the organisation operates	
Is aware of the key principles underlying the relevant regulatory regime, associated legal issues and how these relate to human factors safety issues	

C.3.5 MATCHING THE LEVEL OF RIGOUR AGAINST THE FOLLOWING FACTORS:-

The consequences in the event of failure of the E/E/PES safety related system; the greater the consequence, the more rigorous the specification and assessment of competence.

The safety integrity levels of the E/E/PES safety related system; the higher the safety integrity levels, the more rigorous the specification and assessment of competence.

The novelty of design, design procedures or application; the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be.

Previous experience and its relevance to the specific duties to be performed and the technology being employed. The greater the required competence levels, the closer the fit should be between competencies developed from previous experiences and those required for the specific duties to be undertaken.

	Evidence
Does the organisation take into account the factors listed above to determine if more rigour in the competency assessment process and higher levels of competency are needed	
Are competency levels, such as the IEE/BCS grades used	
What approaches are used to define a 'closer fit' of staff competencies to activity	

C.3.6 RELEVANCE OF QUALIFICATIONS TO SPECIFIC DUTIES TO BE PERFORMED

(IEE/BCS study references: CFM15, ISA15, HRA11, and HF13)

	Evidence
General indicators	
TYPICALLY A DEGREE OR EQUIVALENT IN A RELATED DISCIPLINE	
Has had practical safety engineering experience within the relevant industry sector	

ANNEX D : EVALUATION OF 'FUNCTIONAL SAFETY CULTURE' AS PART OF FUNCTIONAL SAFETY CAPABILITY ASSESSMENT

D.1 INTRODUCTION AND BACKGROUND

This Annex presents guidance for the consideration of the 'functional safety culture' of an organisation as part of a CASS functional safety capability assessment (FSCA). One of the key targets of evaluation in the assessment of functional safety capability of an organisation is the functional safety management system. The achievement of functional safety, in common with other management objectives such as overall safety of personnel and quality, requires that not only is a management system in place, but that it is applied effectively, and with positive attitude, by the relevant personal at all levels within the organisation. It is therefore important that the culture of an organisation is taken into account as part of the functional safety capability assessment. The work as presented is based on the more general background of 'safety culture' (ref. 1).

This Annex references the CASS FSCA Technical Schedules.

D.2 DEFINITION

Functional safety culture is defined within CASS as follows:

"The functional safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisations management of functional safety. Organisations with a positive functional safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of functional safety and by confidence in the efficacy of the measures and techniques used to achieve functional safety".

(This is a modified version of the definition of safety culture as given by the UK Health and Safety Commission (HSC's) Advisory Committee on the Safety of Nuclear Installations [ref. 2]).

D.3 SAFETY CULTURE CONSIDERATIONS AS PART OF FUNCTIONAL SAFETY CAPABILITY ASSESSMENT TECHNICAL SCHEDULES (FSCA TS)

Functional safety culture is not to be regarded as a target of evaluation in its own right, but rather as a consideration in the evaluation of the functional safety management system. The elements of a functional safety management system required for compliance with IEC 61508 are fully detailed in the Technical Schedules for Functional Safety Capability Assessments (FSCA TS), Chapter 4, Targets of Evaluation, 4.2.1 Mapping of FSCA TOES to IEC 61508 clauses. It is not necessary to add anything further to these TOES. However, there should be an explicit acknowledgement that the functional safety climate should be taken account of during the evaluations.

D.4 REFERENCES

1. Reducing error and influencing behaviour (HSG48, 2nd edition), Health & Safety Executive, 1999

2. ACSNI Study group on Human Factors, 3rd report: Organising for Safety, HSE Books 1993, ISBN 0 7176 0865 4