

**Introduction, background and Help for Completion of Part 2, Tables 1, 2, 3 and 4 of
CASS32
‘CASS Functional Safety Management Declaration lodged with CASS-appointed body’**

Document History

Revision	Date	
0	7 Feb 2011	1 st Issue

DISCLAIMER

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

Table of Contents

REFERENCE AND RELATED DOCUMENTS.....	3
ABBREVIATIONS & TERMINOLOGY.....	3
INTRODUCTION.....	5
UNDERSTANDING THE TABLES.....	7
PART 2 TABLE STRUCTURE.....	7
<i>Ref. Column:</i>	8
<i>Document Column:</i>	8
<i>Evidence Column:</i>	8
EXPLANATION OF TABLE 1.....	10
ASSISTANCE IN THE COMPLETION OF TABLE 1.....	10
<i>Mapping of OVERALL (Part 1) TOES to IEC61508 Clauses</i>	11
EXPLANATION OF TABLE 2.....	16
ASSISTANCE IN THE COMPLETION OF TABLE 2.....	16
EXPLANATION OF TABLE 3.....	17
ASSISTANCE IN THE COMPLETION OF TABLE 3.....	17
EXPLANATION OF TABLE 4.....	18
ASSISTANCE IN THE COMPLETION OF TABLE 4.....	18
<i>Mapping of Functional Safety TOES to IEC61508 Clauses</i>	19

Reference and related documents

The following documents are available from www.cass.uk.net

CASS28	CASS Templates For Software Requirements In Relation To IEC 61508 Part 3 Safety Function Assessment (Based on IEC61508 Edition 1)
CASS32	The CASS Functional Safety Management Declaration Lodged with a CASS-appointed Body
CASS33	Help and guidance on CAS32 in general, and on completing Part 1 of CASS32 in particular
CASS34	Help and guidance on completing Part 2 of CASS32
CASS35	Help and guidance on completing Part 3 of CASS32
FSCA Technical Schedules	Section 3 of The CASS Guide. The detailed cross- references to CASS Targets of Evaluation (TOEs) and IEC61508 Edition 1 clauses applicable to Functional Safety Capability Assessment (FSCA)
The CASS Guide	A Published CASS Document defining the processes related to formal accredited assessment for compliance to IEC61508 Edition 1

Other Documents, not available from www.cass.uk.net

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

Abbreviations & Terminology

CASS	Conformity Assessment of Safety-related Systems; an abbreviation for The CASS Scheme Ltd.
Declaration	CASS32, including any specified attachments.
E/E/PE	Electrical, Electronic, or Programmable Electronic. A descriptive term with reference to the technology of a safety-related system, as used in IEC61508
E/E/PES	An Electrical, Electronic, or Programmable Electronic safety-related system
FSCA	Functional Safety Capability Assessment. A CASS term used for the assessment of a Functional Safety Management system.
FSM	Functional Safety Management

HELP DOCUMENT - PART 2
CASS Functional Safety Management Declaration
Lodged with CASS-appointed body.

Owner	the person, business, partnership or other legal entity who is completing the CASS32 form describing and documenting their Functional Safety Management system
Part 1	When used alone, this is a reference to the specific Part 1 of the Declaration (CASS32) document
Part 2	When used alone, this is a reference to the specific Part 2 of the Declaration (CASS32) document
Part 3	When used alone, this is a reference to the specific Part 3 of the Declaration (CASS32) document
PES	A Programmable Electronic safety-related System, usually with the emphasis on being ‘programmable’ or software-based.
SIL	Safety Integrity Level. An IEC61508 term (q.v.) related to the increasing requirements in terms of performance properties and assessment rigour of a safety system with the increasing levels of risk reduction involved, from 1 (low) to 4 (highest)
TCSL	The CASS Scheme Ltd.
TOE	Target Of Evaluation. A specific property of a Functional Safety Management system for which the requirements are specified in one or more clauses in IEC61508, and for which a demonstration of compliance is required.

Introduction

This CASS34 document provides guidance on completion of PART 2 of CASS32, the CASS Functional Safety Management Declaration to be Lodged with a CASS appointed Body.

For an overview and for guidance to the CASS Functional Safety Management Declaration process, please refer to CASS33, Help and guidance for Completion of Part 1 of the 'CASS Functional Safety Management Declaration Lodged with CASS-appointed body'

In general, no single Owner has involvement in the standard from start to finish of the full life-cycle. An end-user has a requirement and so the early (definition) stages and the later (operational) stages of the safety instrumented lifecycle are undertaken by an end-user. A contractor might additionally be involved with the process design and commissioning stages. A system integrator may be involved in supplying the safety instrumented system. Consequently different people and organizations are involved in different stages of the lifecycle. In order for a reader of your Functional Safety Management Declaration to make sense of your system they don't just need to know what your system is – they also need to know what your scope of work is under the IEC61508 group of standards. The reader is also seeking the assurance that you have structured your Functional Safety Management system specifically to ensure compliance with the requirements of the standard, and that you can demonstrate your day-to-day compliance with those procedures by reference to your operational and project records.

In Part 2 you will record the information about the systems you use, and identify the reports and records which contain your assessment of how those systems will meet the requirements, when appropriately applied. In Part 3 you will demonstrate that they are appropriately applied, by reference to the records of the evidence of day-to-day compliance with your documented systems for Functional Safety Management

Part 2 requires the Owner to complete a set of Tables which identify the schedule of activities covered by this self-assessment Declaration, and identify the associated assessment reports justifying why the activities will be claimed to be in compliance with the IEC61508 requirements, when appropriately implemented. Those Tables are:

- TABLE 1: Activities covered by the IEC61508 group of standards
- TABLE 2: Electrical / Electronic / Programmable Electronic Systems ("E/E/PES") activities
- TABLE 3: Software-related activities for safety instrumented systems
- TABLE 4: Functional Safety Management

Example extracts from the CASS32 Declaration Tables are repeated in this document, for information only. The entries must be made in the Declaration, not in this HELP document.

Most of the guidance in this document is derived from the published CASS documents which contain Mapping Tables for CASS TOEs which relate the

TOE activities to specific clause requirements within the standard.

The TOEs and associated Mapping Tables for IEC61508 Edition 1 (1999/ 2000) are published within the CASS Guide,

<http://www.cass.uk.net/PDF's/The%20CASS%20Guide.pdf> and available at www.cass.uk.net

A comprehensive and detailed Guide for the Software aspects with respect to IEC61508 Edition 1 is published as CASS28 - [CASS Templates For Software Requirements In Relation To IEC 61508 Part 3 Safety Function Assessment](#)

The TOEs and associated Mapping Tables for IEC61508 Edition 2 (2010) are under development. Preliminary versions of the Edition 2 TOEs have been used where available (and noted as such) within this document, and will be published and maintained at www.cass.uk.net

The reader should reference the latest version of the TOEs when completing the Declaration formally. Refer to the CASS website for the latest versions www.cass.uk.net

Understanding the Tables

A “TOE” is a target of evaluation. This is a description of the objective that is to be achieved if compliance to the IEC61508 group of standards is to be demonstrated. This means that for every part of the IEC61508 standard a claim of compliance will have been demonstrated if the target of evaluation is met.

Part 2 of the declaration is a list of all the targets of evaluation (“TOE”) covering everything within the scope of the standard. Because your scope of work is unlikely to involve everything in that list, it is important that you identify as ‘Not Applicable’, using Strikethrough, all the TOEs for stages in which you are NOT involved. The remaining applicable list of TOEs shows both your scope of work and the TOE that must be met in order for you to claim that you comply with the standard.

When undertaking a component of work under the standard you will use a particular process or procedure. Each line of Part 2 gives you a place to identify that procedure, state what the evidence is for the procedure being compliant with the requirements of the standard, and the location where the controlled master versions can be found.

Part 2 Table structure

Part 2 Tables have the general form:

Ref.	Overall TOEs	Document	Evidence	Location	Comments
2.1.1	Overall Safety Life-cycle				
2.1.2	Concept				
2.1.3	Fully Installed E/E/PES				
2.1.4	Fully Commissioned E/E/PES				

The columns are:

Ref. Column:

The reference number in the first column relates to the tables of TOEs in the published guidance documents so that you can then relate the particular target of evaluation (“TOE”) to available help notes. The numbering refers to Declaration “Part”. “Table”. “TOE” ., i.e. in the above extract from Part 2 Table 1, the ‘Ref’ column entry “ 2.1.1” is the 1st CASS TOE documented in Table 1 of Part 2 in the Declaration;

Thus the meaning of a reference number of 2.1.1 is:

2	Part 2
1	Table 1
1	TOE1

Document Column:

The Owner should provide, under the heading ‘Document’ the unique identifier and revision level to whatever Owner document best describes the Overall TOE activities of the Owner for that row of the table.

If the activity is within scope, but there is no current relevant document, then the Owner must consider the activities undertaken and proceed to construct and formally document the appropriate processes, as this will be an essential part of the evidence for a Functional Safety Management System. Where this is the case, the Owner may not yet be ready to submit a completed Declaration, as there may not at this time be any formal evidence of compliance to a newly-documented process.

Evidence Column:

This defines the evidence provided by the Owner that the processes and methods described in the “Owner Document” in the Document column for this TOE will meet the requirements of the IEC61508 standard for that TOE, when appropriately applied.

Under ‘Evidence’ enter a reference to whatever Owner document best describes the justification or evaluation by the Owner that the document defined in the Document column appropriately and adequately addresses the requirement of the standard in the referenced IEC61508 Clauses and Tables (see the referenced ‘Mapping’ table for this TOE).

If there is no current documented justification for compliance then the Owner must consider the document defined in the Document column, consider the specific clause requirements in the standard, and document a formal clause-by clause assessment or justification which supports a claim that the

referenced document addresses the requirements of the standard appropriately for the Owner's scope of activity, as this will be an essential part of the evidence for a Functional Safety Management System.

Part of the evidence for compliance should also include identification of the processes, reports, and tracking mechanisms by which the Owner intends to demonstrate day-to-day compliance for the activity.

Location Column:

It is necessary to record where the Owner locates the master copy of the documents referenced in the Document column, and the Evidence column. Documents do not have to be paper, and may indeed only exist in electronic format such as 'WORD', Visio, Autocad, etc., but the location of the master must be clearly established for future potential audits by interested parties such as the HSE or authorised customers. A good place to keep FSM evidence is as a subset of the normal ISO9000 Quality Documentation.

Comments Column:

The Owner may record here any explanatory comments needed to define how access to the document might be obtained or any restrictions that might apply. For instance a comment might record that the lifecycle only describes activities at a particular site which has Functional Safety involvement but all QA/FSM documentation are maintained on the main Network system at the Company headquarters in London.

Explanation of Table 1.

Part 2 Table 1 lists TOE's 1 to 21, and these are concerned with part 1 of IEC61508, The Overall Safety Lifecycle requirements. Most Owners will not be involved with the complete IEC61508 lifecycle documented in IEC61508-1 Figure 2. In order to assist the reader of your declaration to deal with the process of assessment in a systematic manner, this Help document, and these CASS TOEs, both use the IEC61508 lifecycle as a reference.

Table 1 is therefore used to identify, for a particular Owner, the lifecycle activities that are relevant.

The numbering of the CASS TOES in the following Mapping Table is from #1 to #21, corresponding to the Part 2 Table 1 Ref Column numbering 2.1.1 to 2.1.21

Assistance in the completion of Table 1

Primary reference – This document, CASS 34 section: [Mapping of OVERALL \(Part 1\) TOES to IEC61508 Clauses](#)

Secondary reference: The CASS Guide, for compliance to IEC61508 Edition 1

CASS32 Part2 Table 1 is taken from preliminary CASS documents, MAPPING OF OVERALL (PART 1) TOES TO IEC61508 Edition 2 CLAUSES, Users of this Help document are advised to use this Help document (CASS34) as guidance when seeking to establish compliance against IEC61508 Edition 2, and to use The CASS Guide as guidance when seeking to establish compliance against IEC61508 Edition 1. Users are advised to check for the latest guidance related to IEC61508 Edition 2 on the CASS website www.cass.uk.net

The Mapping Table below describes the TOE, provides an explanation of the purpose of the TOE to assist in understanding and therefore completion of Table 1., and provides the cross-references to the clauses within the standard related to that TOE.

The Owner document entered into the Part 2 Table 1 Document Column should address the processes by which all of the activities for that TOE are managed, with reference to the cross-referenced IEC61508 clauses; the document entered into the Evidence Column should justify how and why those processes are intended to meet all of the requirements of those cross-referenced clauses, and how the evidence for day-to-day compliance with those clauses will be captured in practice.

Mapping of OVERALL (Part 1) TOES to IEC61508 Clauses

Version used: IEC 61508-1:2010

When referring to IEC61508 Clauses and Tables the notation used 1/7.1 which means “IEC61508 part 1, clause 7.1”

Ref.	TOE Ref.	OVERALL (IEC61508 Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
2.1.1	1.	Overall Safety Life-cycle	To structure and clarify 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	
2.1.2	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 Phase 1	
2.1.3	3.	Fully Installed E/E/PES	To implement all the requirements of the Overall Installation Plan	1/7.13.2.1 1/Table 1 Phase12	
2.1.4	4.	Fully Commissioned E/E/PES	To implement all the requirements of the Overall Commissioning Plan	1/7.13.2.3 1/Table 1 Phase12	

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

Ref.	TOE Ref.	OVERALL (IEC61508 Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
2.1.5	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 Phase12	
2.1.6	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 Phase2	
2.1.7	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. to 1/6.2.18	
2.1.8	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 Phase3	

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

Ref.	TOE Ref.	OVERALL (IEC61508 Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
2.1.9	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 other risk reduction facilities in order to achieve the required functional safety for the project.	1/7.5 1/Table 1 Phase4	
2.1.10	10.	Overall 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 other risk reduction facility the allocation of a Safety Integrity Level (SIL) and target failure measure to each safety function.	1/7.6 1/Tables 2 & 3 1/ Table 1 Phase5 1/Figure 6	
2/1/11	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 Phase7	

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

CASS34

Ref.	TOE Ref.	OVERALL (IEC61508 Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
2.1.12	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, testing & maintenance	1/7.7 1/Figure 8 1/Table 1 Phase6 1/Figure 7	
2.1.13	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 Phase8	
2.1.14	14.	E/E/PE System Safety Requirements Specification	To define the E/E/PE System Safety Requirements Specification	1/7.10 1/Table 1 Phase9	This shall be issued to the safety system developer
2.1.15	15.	E/E/PE safety-related systems: realisation phase deliverables	To create the E/E/PE safety-related systems conforming to the E/E/PE System Safety Requirements Specification	1/7.11 Parts 2 & 3 1/Table 1 Phase10	System design Requirements Specification Software Safety Requirements Specification See E/E/PES & Software TOEs

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

Ref.	TOE Ref.	OVERALL (IEC61508 Part 1) Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508 Clauses and Tables	Comments
2.1.16	16.	OTHER Risk Reduction MEASURES: SPECIFICATION and realisation phase deliverables	To confirm delivery of all other risk reduction facilities which have been specified as part of the overall safety system	1/7.12 1/Table 1 Phase11	No 61508 requirements. Show evidence of delivery against Overall Safety Requirements Specification
2.1.17	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 Phase13	Appropriate levels of rigour for relevant SIL
2.1.18	18.	Overall Operation, Maintenance & Repair Records	To report the results of any operation, maintenance & repair activities	1/7.15 1/Table 1 Phase14	Appropriate levels of rigour for relevant SIL
2.1.19	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 Phase15 1/Figure 9	Appropriate levels of rigour for relevant SIL
2.1.20	20.	Decommissioning/disposal Plans & Records	To report the probable impact and results of decommissioning and disposal activities.	1/7.17 1/Table 1 Phase16	
2.1.21	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	

Explanation of Table 2

CASS32 Part2 Table 2 is taken from ‘The CASS Guide’ Section 4.2.3 MAPPING OF E/E/PES (PART 2) TOES TO IEC 61508 CLAUSES, and relates to IEC61508 Edition 1. Users of this Help document are advised to use The CASS Guide as guidance when seeking to establish compliance against IEC61508 Edition 1, and to use it as preliminary informative guidance when seeking to establish compliance against IEC61508 Edition 2. In general, CASS TOEs are unlikely to change significantly between Edition 1 and Edition 2, but clause references may differ. Users are advised to check for the latest guidance related to IEC61508 Edition 2 on the CASS website www.casss.uk.net

The numbering of the CASS TOES in the CASS Guide section 4.2.3 is from #1 to #30, corresponding to the Part 2 Table 2 Ref Column numbering 2.2.1 to 2.2.30

Part 2 Table 2 lists Targets of Evaluation (“TOEs”) and these are concerned with IEC61508-2 in its entirety, and may be expected to apply to those Owners actually designing, manufacturing, integrating, maintaining, operating, or modifying Electrical/Electronic/Programmable electronic components (IEC61508 Elements) or systems for safety loop applications. These Owners may not be involved with the complete IEC61508 lifecycle documented in IEC61508-1 Figure 2, but should have a lifecycle similar to that of IEC61508-2 Figure 2 for these activities.

Table 2 is therefore used to identify the lifecycle activities that are relevant to those addressed in IEC61508 Part 2.

Assistance in the completion of Table 2

Primary Reference: The CASS Guide, Section 4.2.3

Please refer to The CASS Guide section 4.2.3, which contains a mapping of the CASS TOE’s to IEC61508 Edition 1 clauses, as given in the CASS32 Declaration Part 2 Table 2. Additionally an explanation of the purpose of the TOE is provided to assist in understanding and therefore completion of Table 2. The Mapping Table describes the TOE, provides an explanation of the purpose of the TOE to assist in understanding and therefore completion of Table 1, and provides the cross-references to the clauses within the standard related to that TOE.

The Owner document entered into the Part 2 Table 2 Document Column should address the processes by which all of the activities for that TOE are managed, with reference to the cross-referenced IEC61508 clauses; the document entered into the Evidence Column should justify how and why those processes are intended to meet all of the requirements of those cross-referenced clauses, and how the evidence for day-to-day compliance with those clauses will be captured in practice.

For compliance to IEC61508 Edition 2, use this as informative guidance on the principles involved. Some clause references will be incorrect.

Explanation of Table 3.

CASS32 Part2 Table 3 is taken from CASS28, CASS Templates For Software Requirements In Relation To IEC 61508 Part 3 Safety Function Assessment Section 7, IEC 61508 Part 3, Software Requirements, Targets of Evaluation, and relates to IEC61508 Edition 1.

Users of this Help document are advised to use CASS28 as guidance when seeking to establish compliance against IEC61508 Edition 1, and to use it as preliminary informative guidance when seeking to establish compliance against IEC61508 Edition 2. In general, CASS TOEs are unlikely to change significantly between Edition 1 and Edition 2, but clause references may differ. Users are advised to check for the latest guidance related to IEC61508 Edition 2 on the CASS website www.cass.uk.net

The numbering of the CASS TOES in CASS28 Section 7 is from #1 to #38, corresponding to the Part 2 Table 3 Ref Column numbering 2.3.1 to 2.3.38

Table 3 lists TOE's 1 to 38 and these are concerned with IEC61508-3 in its entirety and may be expected to apply to those Owners designing, integrating, maintaining, and modifying software for safety loop applications. These Owners may not be involved with the complete IEC61508 lifecycle documented in IEC61508-1 Figure 2, but should have a lifecycle similar to that of IEC61508-3 Figure 2 and Figure 3 for these activities.

Table 3 is therefore used to identify, for a particular PES Owner, the lifecycle activities that are relevant, and the documents which support the claim for conformance to the requirements of the standard.

Assistance in the completion of Table 3

Primary Reference: CASS28, Section 7

Please refer to CASS28 which contains the mapping of the CASS TOE's to IEC61508 clauses. Additionally an explanation of the purpose of the TOE is provided to assist in understanding and therefore completion of Table 3.

The Owner document entered into the Part 2 Table 3 Document Column should address the processes by which all of the activities for that TOE are managed, with reference to the cross-referenced IEC61508 clauses; the document entered into the Evidence Column should justify how and why those processes are intended to meet all of the requirements of those cross-referenced clauses, and how the evidence for day-to-day compliance with those clauses will be captured in practice.

For compliance to IEC61508 Edition 2, use this as informative guidance on the principles involved. Some clause references will be incorrect.

Explanation of Table 4.

Part 2 Table 4 lists TOE's 1 to 18 and these are concerned with IEC61508-1 Clause 6.0 in its entirety, and may be expected to apply to all those Owners involved with Functional Safety in whatever manner. These Owners may not be involved with the complete IEC61508 lifecycle documented in IEC61508-1 Figure 2, but should have something similar.

Table 4 is therefore used to identify the lifecycle activities that are relevant and must be covered by the Owners FSM in order for a self declaration to be acceptable.

The numbering of the CASS TOES in the following Mapping Table is from #1 to #18, corresponding to the Part 2 Table 4 Ref Column numbering 2.4.1 to 2.4.21

Assistance in the completion of Table 4

Primary reference – This document, CASS 34, Section: Mapping of Functional Safety TOES to IEC61508 Clauses

Secondary reference: The CASS Guide, for compliance to IEC61508 Edition 1

CASS32 Part2 Table 4 is taken from preliminary CASS documents, MAPPING OF FUNCTIONAL SAFETY TOES TO IEC61508 Edition 2 CLAUSES, Users of this Help document are advised to use this Help document (CASS34) as guidance when seeking to establish compliance against IEC61508 Edition 2, and to use The CASS Guide as guidance when seeking to establish compliance against IEC61508 Edition 1. Users are advised to check for the latest guidance related to IEC61508 Edition 2 on the CASS website www.cass.uk.net

The Mapping Table below describes the TOE, provides an explanation of the purpose of the TOE to assist in understanding and therefore completion of Table 4., and provides the cross-references to the clauses within the standard related to that TOE.

The Owner document entered into the Part 2 Table 4 Document Column should address the processes by which all of the activities for that TOE are managed, with reference to the cross-referenced IEC61508 clauses; the document entered into the Evidence Column should justify how and why those processes are intended to meet all of the requirements of those cross-referenced clauses, and how the evidence for day-to-day compliance with those clauses will be captured in practice.

Mapping of Functional Safety TOES to IEC61508 Clauses

Version used: IEC 61508-1:2010

When referring to IEC61508 Clauses and Tables the notation used **1/6.1** which means “IEC61508 part 1, clause 6.1”

Targets of evaluation (TOES) for management of Functional Safety in compliance with IEC61508-1:2010

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
1	Functional Safety Management System	<p>To specify all responsibilities in the management of Functional Safety that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety (1/6.1.1)</p> <p>The activities specified as a result of 1/6.2.16 shall be implemented and progress monitored</p>	1/6.2.1 to 6.2.18	This TOE calls for the following clauses which should be considered and need 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;	<p>1/6.2.2</p> <p>Figs 2,3,4, Table 1, and 1/6.2.1 as framework.</p>	This TOE requires that there should be a top-level policy statement (typically at Board level) that reflects the safety goals and objectives of the organisation

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
3	Organisation and Responsibilities	<p>Identification of the persons, departments and organisations who perform or review safety lifecycle activities and allocation of responsibilities for those activities.</p> <p>To ensure that all those specified as responsible for management of functional safety activities are informed of the responsibilities assigned to them.</p>	<p>1/6.2.3</p> <p>Figs 2,3,4, and 1/Table 1</p> <p>See Note under 6.2.1</p>	<p>FSM evaluation and assessment activities should verify that the allocation of roles and responsibilities are documented, and cover all of the scope of the subject organisation's activities. This may be presented in:</p> <ul style="list-style-type: none"> - Organisation Chart - Project Safety Plan - Responsibility matrix <p>This includes where relevant, licensing authorities or safety regulatory bodies.</p> <p>For guidance on level of rigour for this TOE against SIL – refer to TOE8 for competence of staff in technical positions.</p>
4	Identification of relevant lifecycle phases	The overall, E/E/PES or software safety lifecycle phases to be applied;	<p>1/6.2.1</p> <p>Figs 2,3,4, and 1/Table 1</p>	<p>The organisation shall demonstrate an understanding of where its activities fit in the overall life-cycle.</p> <p>This could be included as part of the safety plan, procedure or work instruction.</p>
5	Documentation structure and content policy	The way in which information is to be structured, communicated and the extent of the information to be documented.	<p>1/6.2.4</p> <p>1/5</p>	
6	Techniques and Measures conformance plan	The selected measures and techniques used to meet the requirements of a specified clause or sub-clause;	<p>1/6.2.12.a</p> <p>(see IEC61508 Parts 2, 3 and 6)</p>	<p>This TOE is looking for evidence of a general approach that pre-defines which T&M's shall be used.</p> <p>See Parts 2 & 3 Annexes or TOEs from other CASS templates (as appropriate to the relevant lifecycle phases) for guidance of rigour against SIL.</p>

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

CASS34

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
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;	1/6.2.5 Evidence from the relevant sections: 1/6.2.10, 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.	
8	Competence assessment process	To define procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle 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;	1/6.2.13, 6.2.14.a-k, 6.2.15 Figs 2,3,4 and 1/Table 1 as framework.	<p>Organisation training plan and training records are important supporting evidence.</p> <p>Sources of good guidance are:</p> <ul style="list-style-type: none"> - HSE competency guidelines - IET/BCS - FSM* TS ref Annex C <p>Some grading of competence to match SIL can be inferred from the competency level.</p> <p>* Note: FSM Assessment used to be called FSQA – Functional Safety Capability Assessment within CASS documents</p>

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation 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;	1/6.2.5.f, 6.2.6	Evidence of regular review of safety logs, incidents, trends for the organisation but also that the organisation considers what lessons may be learnt and disseminated from the published experience of other organisations.
10	Procedure for O&M performance analysis	To define procedures for analysing operations and maintenance performance. In particular procedures for: <ul style="list-style-type: none"> - 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; 	1/6.2.12.c Figs 2,3,4 and 1/Table 1 as framework.	<p>This TOE is only relevant to organisations performing O&M activities.</p> <p>Fig 7 (IEC61508-1:2010) provides an example of an operations and maintenance activities model.</p> <p>Fig 8 (IEC61508-1:2010) provides an example of an O&M management model.</p> <p>No guidance on level of rigour, for this TOE, against SIL – could be linked with the competency of reviewers and authorisers of modifications.</p>

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

CASS34

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
11	Functional safety audit process	<p>To define requirements for periodic functional safety audits in accordance with this sub-clause including:</p> <ul style="list-style-type: none"> - 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; 	1/6.2.7	<p>The organisation should be able to justify the level of independence of those conducting audits.</p> <p>An audit timetable, audit reports and actions should be available for review.</p> <p>Guidance given in 1/Table 4, 1/Table 5 on levels of independence, of the FSA auditor, against SIL.</p>
12	Modification process for Safety related systems	<p>To define the procedures for initiating modifications to the safety-related;</p> <p>To define the required approval procedure and authority for modifications;</p>	<p>1/6.2.8.a 1/6.2.8.b</p> <p>Figs 2,3,4 and 1/Table 1 as framework.</p> <p>1/7.16.2.2</p>	<p>The organisation should be able to demonstrate that modification procedures have been properly planned.</p> <p>The organisation should be able to demonstrate that the modification request has been properly documented and authorised and any impact analysis performed.</p> <p>The competence level of the checker/approver, of any modification, must be demonstrated by the organisation though there is no definitive guidance.</p>

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

CASS34

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
13	Procedures for maintaining information on hazards with respect to Safety-Related Systems.	To define the procedures for maintaining accurate information on hazards and safety-related systems;	1/6.2.9	
14	Configuration management procedures	<p>To define the procedures for configuration management of the E/E/PE safety-related systems during the overall, E/E/PES and software safety lifecycle phases; in particular the following should be specified:</p> <ul style="list-style-type: none"> - 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; 	<p>1/6.2.10</p> <p>Figs 2,3,4 and 1/Table 1 as framework.</p>	

HELP DOCUMENT - PART 2

CASS Functional Safety Management Declaration Lodged with CASS-appointed body.

	Target of Evaluation (TOE)	Purpose of TOE	Referring IEC 61508-1:2010 clauses and Tables	Evaluation comments
15	Procedures for provision of training and information for the emergency services.	To provide training and information for the emergency services.	1/6.2.11	Note that the requirement of this sub-clause may not be mandatory in all cases. Training records should be auditable (if appropriate).
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.	1/6.2.16	This is a formal review and decision making process with regard to the effectiveness of the FSM procedures Minutes of Review meetings and Review documents should be auditable.
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.	1/6.2.17	The requirement may be satisfied by an appropriate quality management system, certification to a recognised national or international standard, e.g. ISO9001, would be an advantage. Checks could include, where relevant, review of QMS certificates, supplier CASS assessments, OEM safety manuals (as required by normative Annex D of IEC61508-2, suppliers certificates of conformity (as per ISO/IEC 17050 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.	1/6.2.12.b 1/8.1 1/8.2 1/Table 4 1/Table 5 3/8 3/Table A10	This TOE is aimed at the two parties responsible for Functional Safety Assessments (FSA): for those responsible for providing the evidence that functional safety has been achieved and which is to be assessed by those performing the FSA (ii) for those responsible for performing the independent FSA