



## **Technical Schedules for Application Specific Assessments**

### **Targets of Evaluation**

(CASS Type 2 Assessment ASAT)

---

CONTENTS LIST

---

<b>1</b>	<b>INTRODUCTION</b>	<b>3</b>
<b>2</b>	<b>SUMMARY OF TARGETS OF EVALUATION, ATTRIBUTES, AND ASSESSMENT CRITERIA</b>	<b>4</b>
2.1	<i>TOES FOR ASAT ASSESSMENT IEC 61508 PART 2</i>	4
2.2	<i>TOES FOR ASAT ASSESSMENT IEC 61508 PART 3</i>	5
<b>3</b>	<b>MAPPING OF E/E/PES TOES TO IEC61508 CLAUSES</b>	<b>7</b>
<b>4</b>	<b>MAPPING OF SOFTWARE TOES TO IEC61508 CLAUSES</b>	<b>19</b>

---

CHANGE HISTORY

<b>Version Number</b>	<b>Date</b>	<b>Principal changes since last issue</b>
<b>V5</b>	<b>11<sup>th</sup> November 2002</b>	<b>For Industry Comment</b>
<b>V6</b>	<b>25<sup>th</sup> January 2010</b>	<b>Reviewed and updated by CASS to issue for comment</b>
<b>CASS31-Rev0</b>	<b>21 June 2010</b>	<b>Reformatted and issued for comment as CASS31, with no technical change.</b>

**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.

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

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

The use of the CASS Logo on or in relation to a product or system is permitted only as specified by the relevant Certification Body and is a claim by a manufacturer or user that the product or system has been manufactured or is being used (as appropriate) in accordance with the requirements of the referenced standard. The accuracy and status of the use of the Logo is therefore solely the responsibility of the manufacturer or the user.

The CASS Scheme Ltd

---

# 1 INTRODUCTION

---

For a general introduction to the CASS Scheme and the development of guidance for assessors, please see 'The CASS Guide', available from The CASS Scheme Ltd ([www.cass.uk.net](http://www.cass.uk.net)).

This document provides, for the assessor, specific guidance on the targets of evaluation (TOE) associated with those clauses within IEC61508 Edition 1 which are relevant to each Application-Specific Assessment Type (ASAT).

The Application-Specific Assessment Types covered here are:

1. Type 2a comprising an integrated System that include all functional elements (hardware and software) from the connection to the measuring device through to final actuation device. The end to end system in its working environment is the scope of this assessment type. The assessment will include installation, final validation and commissioning activities to prepare the system for use. The system assessed may perform a single safety function or a number of safety functions.
2. Type 2b comprising a sub-system that includes components and sub-systems that implement a part of a safety function. A typical type 2b system will comprise a logic system that includes hardware and application software installed in an enclosure or housing that is suited to the final working environment. The assessment will include the partial validation carried out at factory acceptance testing. The system assessed may perform a single safety function or a number of safety functions.

An assessment prompt list is included to ensure an assessor covers all relevant issues. The prompts should not be used as a tick list such that a non-conformance is noted if the assessee has used a different approach. In such cases a judgement will need to be made as to whether the different approach complies with the requirement within IEC 61508.

Prompt lists will be added to as experience in conformity assessment progresses. Assessors should propose additions or deletions that will lead to more consistent approaches.

## 2 SUMMARY OF TARGETS OF EVALUATION, ATTRIBUTES, AND ASSESSMENT CRITERIA

The following tables identify the Targets of Evaluation (TOE) within each of the normative parts of IEC61508, which are relevant for each Application-Specific Assessment Type. There are tables for IEC61508 2, and 3, and criteria within each of these tables are applicable to each ASAT.

### KEY TO TABLE ENTRIES

Y = TOE for this assessment type

### 2.1 TOES FOR ASAT ASSESSMENT IEC 61508 PART 2

		Application-Specific Assessment Type	
	IEC 61508 Part 2	Integrated Systems 2a	Sub Systems 2b
	<b>Process TOEs</b>		
1	Conformance to this standard	Y	Y
2	Documentation	Y	Y
3	Management of functional safety	Y	Y
4	E/E/PES safety lifecycle	Y	Y
	<b>Documentation TOEs</b>		
5	E/E/PES Safety Requirements Specification	Y	Y
6	E/E/PES Safety Validation Plan	Y	Y
7	E/E/PES Design Documentation General requirements	Y	Y
8	E/E/PES Design Architectural constraints on hardware safety integrity	Y	Y
9	E/E/PES Design Requirements for estimating the probability of failure	Y	Y
10	E/E/PES Design Requirements for the avoidance of failures	Y	Y
11	E/E/PES Design Requirements for the control of systematic faults	Y	Y
12	E/E/PES Design Requirements for system behaviour on detection of a fault	Y	Y
13	E/E/PES Design Requirements for E/E/PES implementation	Y	Y
14	E/E/PES Design Requirements for data communication	Y	Y

15	E/E/PES Integration and Test Specification	Y	Y
16	E/E/PES Integration and Test Report	Y	Y
17	E/E/PES Integration and Test Log	Y	Y
18	E/E/PES Operation and Maintenance Procedures	Y	Y
19	E/E/PES Safety Validation Report	Y	Y
20	E/E/PES Safety Validation Log	Y	Y
21	E/E/PES Modification Procedures	Y	Y
22	E/E/PES Verification Plans	Y	Y
23	E/E/PES Verification Reports	Y	Y
	<b>E/E/PES TOEs</b>		
24	Fully Functioning E/E/PES	Y	
25	Fully Validated E/E/PES	Y	
26	Functional safety assessment of the E/E/PES	Y	Y

## 2.2 TOES FOR ASAT ASSESSMENT IEC 61508 PART 3

		Application-Specific Assessment Type	
IEC 61508 Part 3		Integrated Systems 2a	Sub system 2b
<b>PROCESSES</b>			
1	Software Safety Life Cycle	Y	Y
2	Software Configuration Management	Y	Y
<b>DOCUMENTS</b>			
3	Software Safety Requirements Specification	Y	Y
4	Software Safety Verification and Validation Plan	Y	Y
5	Software Design General Requirements	Y	Y
6	Development Tools	Y	Y
7	Software Architecture Design Description	Y	Y
8	Software System Design Specification	Y	Y
9	Software Module Design Specification	Y	Y
10	Coding Manual	Y	Y
11	Software Module Source Code Listing	Y	Y

12	Software Test Specification General Requirements	Y	Y
13	Software Test Log General Requirements	Y	Y
14	Software Test Results General Requirements	Y	Y
15	Software Module Test Specification	Y	Y
16	Software Module Test Report	Y	Y
17	Software System Integration and Test Specification	Y	Y
18	Software System Integration and Test Log	Y	Y
19	Software System Integration and Test Report	Y	Y
20	Software Architecture Integration and Test Specification	Y	Y
21	Software Architecture Integration and Test Log	Y	Y
22	Software Architecture Integration and Test Report	Y	Y
23	PE and Software Integration Test Specification	Y	Y
24	PE and Software Integration Test Log	Y	Y
25	PE and Software Integration Test Report	Y	Y
26	Software Safety Validation Specification	Y	Y
27	Software Safety Validation Log	Y	Y
28	Software Safety Validation Report	Y	Y
29	Software Operation Procedures	Y	Y
30	Software Modification Procedures	Y	Y
31	Software Modification Log	Y	Y
32	Software Modification Report	Y	Y
33	Software Modification - Verification Report	Y	Y
	<b>SOFTWARE AND PE</b>		
34	Fully Functioning Software and PE	Y	Y
35	Fully Validated Software and PE	Y	Y

### 3 MAPPING OF E/E/PES TOES TO IEC61508 CLAUSES

In the following table references shown as 2/7.3.2.1 are referring to IEC61508 first edition Part 2 clause 7.3.2.1

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
1	Conformance to the standard	To determine the degree of rigour necessary to demonstrate that the requirements of the standard have been met.	<p>Establish the factors that would determine the degree of rigour to be applied e.g. complexity, novelty, technology, size, SIL, number of teams involved, physical distribution, nature of hazards.</p> <p>Is it claimed that any requirements are unnecessary; if so what is the basis e.g. Compliance with some tables may be unnecessary if sub-systems are demonstrated as compliant with IEC 61508 or proven in use.</p>	2/4 refers to 1/4 for detail		
2	Documentation	To specify the information to be documented to enable E/E/PES lifecycle and safety management activities to be performed effectively	<p>Review document structure to ensure it is:</p> <ul style="list-style-type: none"> <li>• sufficient for each phase of the E/E/PES</li> <li>• sufficient for functional safety assessment</li> <li>• sufficient for the duties to be performed</li> <li>• titles or names indicating the scope of the contents and index</li> <li>• revision index</li> <li>• documents structured to enable search for relevant information</li> <li>• documents revised, amended, approved and under the control of a document control scheme</li> </ul> <p>In judging the adequacy of a document system account will need to be taken of the degree of rigour required (see under 1 for factors).</p>	2/5 refers to 1/5 for detail		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
3.	Management of functional safety	To specify the management and technical activities and those responsible	<p>Use list for Functional Safety Management as basis for review together with how it has been applied to the specific application. The requirements for management of functional safety will apply to all contractors and sub-contractors including:</p> <ul style="list-style-type: none"> <li>vendors of equipment for sub-systems</li> <li>consultants e.g Reliability Analysts</li> <li>installation contractors</li> <li>pre-commissioning contractors</li> <li>commissioning (may be Contractor or User)</li> </ul> <p>Where an organisation has a FSCA it will be sufficient to ensure: the FSCA applies to the range of equipment used the safety management system for which the FSCA has been obtained has been implemented in a satisfactory way</p> <p>Examine Safety Plan for specific E/E/PES application implementation.</p> <p>What are plans for independent functional safety assessment, it should be in multiple stages for large or complex projects, ensure there are sufficient stages such that assessors are not subject to intolerable pressure to accept design basis at a late stage.</p>	2/6 refers to 1/6 for details		
4.	E/E/PES Safety Lifecycle	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.	<p>What is the scope of the lifecycle to be applied?</p> <p>How is this documented?</p> <p>Is the document structure suitable for the lifecycle scope?</p> <p>Are the functional safety management responsibilities for each lifecycle phase defined?</p> <p>If an alternative to the IEC 61508 lifecycle is used, how is this justified and documented e.g. is there an equivalent to Table 1?</p> <p>Each organisation involved in the integration may have a separate lifecycle, in which case how are they linked and are they complete?</p>	2/7.1 2/7.1.3.3 2/7.1.3.5	2/7.1.3.1 2/Table 1	2/7.1.3.2 2/7.1.3.4

	TOE	Purpose of TOE	Assessment Prompt List	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).	<p>Are the safety functions clearly defined and are expressed and structured to be clear, unambiguous, verifiable, testable, feasible the requirements for design and development are adequate</p> <p>The following are defined or stated: boundary of the safety related system  throughput and response time  operator and maintenance interfaces  safety-relevant modes of operation of the process  requirements for start up, restarting after a demand or a fault and after fault diagnosis  the extremes of all environmental conditions  necessary SIL for each function  demand mode and target PFD or dangerous failure rate as appropriate</p> <p>Look for specified values for trip points, response time and criteria for success. Will the specification be capable of validating against these requirements?</p>	2/7.2.2.3 2/7.2.3.3	2/7.2.2.1 2/7.2.3.2 a-e	2/7.2.3.1 a-j 2/7.2.2.2

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
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)	<p>Is validation in stages e.g partial validation at FAT?</p> <p>What tools and techniques are planned to check against tolerances for trip point and response time?</p> <p>Have facilities been planned to allow final testing in situ and on line?</p> <p>Are there policies for resolving validation failures?</p> <p>Is validation plan updated as design proceeds?</p> <p>Are the planned techniques and measures consistent with the SIL?</p> <p>Are all of the requirements in the safety requirements specification covered?</p> <p>Are pass/fail criteria clearly stated?</p>	2/7.3.2.1 2/Table B.5	2/7.3.2.2 a-g	2/7.7.2.7

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
7.	E/E/PES Design  General Requirements	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification (2/7.4.1). General requirements	<p>How are non safety functions treated, are they independent or implemented as safety functions, consider field equipment, cables, hook ups, junction boxes?</p> <p>Can any failures of non safety equipment cause failure to function of safety system, examine interfaces with all external systems.</p> <p>How are different functions with different SILs treated, do the functions have independence or are they implemented to the highest SIL (need not apply to field equipment that has only one function)?</p> <p>Review the developer procedures for review of safety requirements specification.</p> <p>Are the techniques and measures (see EIC 61508-2 annexes A and B) to be used documented and justified?</p> <p>Have hardware and software interactions been evaluated?</p> <p>Have specifications been described for sub-systems, how have these been derived and how is it shown that overall spec is achieved?</p> <p>How are sub-systems to be integrated and tested?</p> <p>If a system has more than one output, how have all failure modes been identified and has a check been carried out to establish if they lead to additional hazards?</p>	2/7.4.2.		

	<b>TOE</b>	<b>Purpose of TOE</b>	<b>Assessment Prompt List</b>	<b>Referring IEC 61508 Clauses and Tables</b>		
8	E/E/PES design  Architectural constraints on hardware safety integrity	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Architectural constraints on hardware safety integrity (2/7.4.3.1)	<p>Check type A / type B basis for decision</p> <p>How is safe failure fraction determined (systematic failures can be excluded, minor safe failures are sometimes included to raise SFF, note limits on diagnostic coverage through DCS, note proof test is not diagnostic)?++</p> <p>How is fault tolerance determined for complex systems (are any low probability faults excluded)?</p> <p>What procedure has been followed?</p> <p>Note – For proven in use systems the data supplied will need to be considered in the context of the application e.g. the safe failure fraction of a sub-system will depend on whether it is used in the application as energise or de-energise to trip. Data from the type 1 template will need to be processed for each specific application to determine safe failure fraction, dangerous failure rate and fault tolerance.</p>	2/7.4.3.1		
9	E/E/PES design  Requirements for estimating the probability of random hardware failure	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for estimating the probability of random hardware failure (2/7.4.3.2)	<p>Is the failure data for subsystem components reliable ? (vendor claims on basis of maintenance returns need to be examined for proof of application as a minimum, database claims checked for similar environment)</p> <p>Have common cause failures been accounted for, what common cause failure model was used? (justify if not model in part 6)</p> <p>Are the assumptions of proof test interval and repair time justified?</p> <p>Have all functions in the safety requirements specification been included?</p> <p>Does the achieved performance meet SIL range or specified value in safety requirements specification?</p>	2/7.4.3.2		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
10	E/E/PES design  Requirements for the avoidance of failures	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for the avoidance of failures (2/7.4.4)	NOTE – Checking that sub-systems are compliant with measures and techniques in tables is outside scope of type 2, check should be limited to integration activities  How do design methods and tools used accord with tables in Annex B?  Are all sub-systems assessed as meeting the requirements of IEC 61508 (check scope of the assessment and check conditions on schedules are met) or are sub-systems proven in use (see template)?	2/7.4.4		
11	E/E/PES design  Requirements for the control of systematic faults	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for the control of systematic faults (2/7.4.5)	NOTE – Checking that sub-systems are compliant with measures and techniques in tables is outside scope of type 2, check should be limited to integration activities  Are all sub-systems assessed as meeting the requirements of IEC 61508 (check scope of the assessment since it may not include all elements and check conditions on schedule are met)?  Otherwise, how are the requirements for control of systematic faults met?  Refer to Annex A for recommended techniques and measures.  Have the sub-systems been designed for operability, maintainability, and testability?  Consider overrides for testing and start up - unique keys, switches set to prevent re-configuration - consider interfaces for human factors	2/7.4.5		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
12	E/E/PES design  Requirements for system behaviour on detection of a fault	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for system behaviour on detection of a fault (2/7.4.6)	<p>Check that non-redundant sub-systems in high demand mode cause safe state on detection of a fault by diagnostic tests</p> <p>Check that non-redundant sub-systems in low demand mode achieve a safe state on detection of a fault by diagnostic tests or can be repaired within the MTTR assumed in the PFD calculation.</p> <p>Check that for redundant sub-systems in either demand mode, a safe state is achieved or the system can be repaired within the MTTR assumed.</p> <p>Is safe state achieved automatically or is operator action required, how is operator made aware, has a procedure been defined?</p> <p>Check if diagnostic actions are in accordance with safety requirements specification.</p>	2/7.4.6		
13	E/E/PES design	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for E/E/PES implementation (2/7.4.7)	<p>Examine comprehensive information on all sub-systems.</p> <p>Examine justification for proven in use (see template for proven in use, note that proven in use is intended for field equipment).</p> <p>How are safety sub-systems identified, field equipment, connections, cables, junction boxes and terminations?</p>	2/7.4.7		
14	E/E/PES design  Requirements for data communication	To ensure the design and implementation of the E/E/PES meets the requirements of the E/E/PES Safety Requirements Specification Requirements for data communication (2/7.4.8)	<p>Is the safety function dependent on data communication between sub-systems being integrated – if HART or fieldbus are used how is this justified?</p> <p>Have failure modes and failure rates been included in calculations – where does data come from?</p> <p>Refer to IEC 61784-3</p>	2/7.4.8		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
15.	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 and Safety Requirements Specification (2/7.4.7.5).	<p>Will integration be carried out in stages, what testing will be carried out at each stage?</p> <p>Is there an adequate test plan?</p> <p>How will it be shown that unintended functions are not carried out?</p> <p>What procedures are there for impact analysis prior to modification if validation activities require changes?</p> <p>What techniques are used from 2/table B3?</p> <p>Does the competency examination include all contractors undertaking safety-related activities?</p> <p>Note – Integration activities will include the work of installation contractors and will include pre-commissioning and commissioning activities. 2/7.5.2 only covers the PES integration activities. To verify that all installation and commissioning activities are covered, Part 1 clauses (1/7.9) need to be considered.</p> <p>How are discrepancies and faults recorded, resolved and re-tested? Consider a) discrepancies between the design documentation and the safety requirements specification and b) discrepancies between the E/E/PES and the design documentation.</p>		2/7.5.2.	2/Table B.3
16.	E/E/PES Integration and Test Report	To report the results (detailed and overall) of the integration testing.	<p>What documents are produced describing tests and results: The test results? Discrepancy between expected and actual results?</p>	2/7.5.2.4	2/7.5.2.6	
17.	E/E/PES Integration and Test Log	To provide a chronological record of the integration and integration testing.	<p>What documents are produced describing tests and results: Version of E/E/PES and test specification? Criteria for acceptance? Any analysis made and decisions taken?</p>	2/7.5.2.6		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
18.	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).	<p>Any limits on lifetime to maintain the validity of failure rates e.g. capacitor or battery life.</p> <p>Check maintenance procedures for:            Actions to prevent wear out between proof tests            Proof testing, tools used, fault diagnosis, repair, revalidation, permits            Procedures for reporting and analysis of failures,</p> <p>Check operations procedures for:            Actions on start up, shut down, fault diagnosis            Control and authority level for override keys            Logging and analysis of demands            Permit procedures</p> <p>Audit procedures</p> <p>Have procedures been checked by those who will have responsibility for operation and maintenance?</p>	2/7.6.2.1 2/7.6.2.2 2/7.6.2.5	2/7.6.2.4 2/7.4.7.3 2/Table B.4	2/7.6.2.1 a-g 2/7.6.2.3
19.	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).	<p>Has test equipment been calibrated and verified?</p> <p>Was the validation plan followed?</p> <p>Have operations and maintenance procedures been validated?</p> <p>Have appropriate validation procedures been used?</p>	2/7.7.2.4 a-e 2/7.7.2.5 2/7.7.2.3	2/7.7.2.1	2/7.7.2.6 2/7.7.2.7 2/Table B5
20.	E/E/PES Safety Validation Log	To provide a chronological record of the E/E/PES Safety Validation (2/7.7.2.4).	Check log for discrepancy and follow through analysis, judgements and resolution.		2/7.7.2.4 2/7.7.2.5	

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
21.	E/E/PES Modification Procedures, report and logs	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 NOTE - Modification can occur from early stages in the lifecycle 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.	How is impact of modifications assessed, is impact on risk considered, are failure modes and failure rates considered, is original risk analysis reviewed?  What is approval procedure and authority levels?  Are procedures in place to initiate changes as a result of defects in equipment and procedures?  What competency is specified for those carrying out modification?  Is a safety lifecycle specified for modifications?  Examine modification reports and log for the specified application and track impact analysis and approvals through to completion of revalidation.	2/7.8.2.1 a-i 2/7.8.2.2 2/7.8.2.3 2/7.8.2.4	2/7.5.2.5 (Changes during integration)	
22	E/E/PES Verification Plan	To test and evaluate the outputs of all phases to ensure correctness and consistency  (NOTE – this is an amalgamation of several specific verification plan TOES in an early version and requires more work to cover all aspects of the individual verification plans)	Has a verification plan been developed – a plan developed as per ISO 9000 may not be sufficient for safety and will need to be examined for sufficiency?  Consider verification activities for installation and commissioning verification. Verification plans should include: Criteria, techniques and tools for each phase Activities to be performed at each phase How are non conformances tracked to resolution What procedures prevent operation prior to non conformance resolution			
23	E/E/PES VERIFICATION REPORT	To record the outcome of verification activities	How are verification activities documented: Signature boxes may be sufficient for simple equipment Verification reports and logs may be necessary for complex equipment Examine verification reports for the specific application			
24.	Fully Validated E/E/PES	To implement all the requirements of the E/E/PES Safety Requirements Specification (2/7.7.1).	All documents are complete and all recommendations from audits, verification, and validation are resolved. All equipment installed as per design What check lists are used	2/Table 1[9.6]	2/7.7.1	

	<b>TOE</b>	<b>Purpose of TOE</b>	<b>Assessment Prompt List</b>	<b>Referring IEC 61508 Clauses and Tables</b>		
25.	Fully Functioning E/E/PES	To satisfy the requirements of the E/E/PES Design Documentation.	<p>All pre-commissioning and commissioning completed.</p> <p>All isolations open, all stops removed, lines cleaned and drained.</p> <p>What check list is used</p> <p>Are check lists linked to start up authority</p>	2/7.5.2.1 2/Table 1[9.4]	2/7.5.2.2	2/7.5.2.3
26.	Functional safety assessment of the E/E/PES	To investigate and arrive at a judgement on the functional safety achieved by the E/E/PES	<p>Have all phases been covered?</p> <p>Have all tools been considered e.g. computer maintenance systems?</p> <p>Have actions from previous assessments been resolved?</p> <p>Confirm competence and independence of the team.</p>	2/8 refers to 1/8		

## 4 MAPPING OF SOFTWARE TOES TO IEC61508 CLAUSES

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
1.	Software Safety Lifecycle Structure	To structure the development of the software into defined phases and activities.	<p>SIL1+</p> <p>Confirm through audit that:</p> <ul style="list-style-type: none"> <li>- the safety lifecycle is defined in writing</li> <li>- that it recognises software requirements, architectural design, detailed design, module design, coding, module test, SW integration test, PE integration test and validation - or if not that the reasons for departure from this lifecycle are justified</li> <li>- that the interfaces to the hardware and system lifecycles are identified</li> <li>- that the interfaces between design, test, functional safety assurance and quality assurance throughout the lifecycle are identified</li> <li>- that the performance criteria for the information to be available at the input and output from each phase of the lifecycle are identified</li> <li>- that all lifecycle results are documented</li> <li>- that on change there is a requirement to identify the lifecycle phases which are impacted and to revisit all these lifecycle phases</li> </ul>	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 3/7.2 – 3/7.9	3/7.1.2.2 3/7.1.2.4 3/7.1.2.7
1.	←	←	<p>← SIL 2+</p> <p>← Undertake a separate review of the lifecycle to confirm that the assessor agrees with the extent to which the lifecycle is claimed to conform with IEC 61508 in terms of the attributes identified in the body and in Tables of Part 3.</p> <p>←</p> <p>← AND/OR</p> <p>←</p> <p>← Confirm that any departure from the lifecycle is justified through demonstrating that the necessary information attributes listed in the body and Tables of IEC 61508 are achieved through alternative mechanisms</p> <p>←</p>	←	←	←

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
1.			SIL 3+ Confirm that any alternative mechanisms have been justified to show why they are at least as rigorous as the original IEC 61508 requirements.			
1.			SIL 4(+) Undertake a separate review of justifications for deviations to confirm that the assessor can identify rationale for the approach.			
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.	SIL 1+ Confirm through audit that the configuration management system provides written policies, purpose & scope for CM activities which differentiates (if necessary) between company and system/project mechanisms and which define the following: <ul style="list-style-type: none"> <li>- the stage at which formal configuration control is to be implemented</li> <li>- the items which will have a unique identification consistent with the level of detail and control authority at each level of configuration management</li> <li>- the points at which baselines will be established</li> <li>- the means of identifying the unique configuration at baselines</li> <li>- the means of confirming functional and physical accuracy of the configuration</li> <li>- provides traceability between levels of control to maintain the integrity throughout</li> <li>- the means of controlling changes to the configuration</li> <li>- criteria for entry or re-entry to the configuration control system</li> <li>- the means of impact assessment</li> <li>- the means by which it is formally confirmed that the software safety requirements continue to be satisfied after change</li> <li>- controls obsolete documents and code</li> <li>- the means to identify configuration status, release status, the justification for and approval of all modifications</li> <li>- the minimum details that a modification shall record</li> <li>- define retention periods and disposal criteria</li> </ul>	1/6.2	3/6.2.3 a-f	

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
2.			<p>SIL 2+</p> <p>Confirm through sample review of safety analysis and requirements; problem reporting and change records, software specification and design documents; software source code modules, physical media; verification and test plans and results; pre-existing software components and packages, tools and development environments that the configuration system is sufficient to:</p> <ul style="list-style-type: none"> <li>-identify the structure and relationship between Configuration Items</li> <li>- identify Configuration Items to the smallest compilation unit</li> <li>- identify compatibility between configuration items</li> <li>- controls I/Fs changes, deviations, waivers</li> <li>- allows traceability to the source code level</li> <li>- utilises identification techniques understandable to those needing to manage the configuration</li> <li>- control from point of formal release</li> </ul>			
2.			<p>Confirm through sample review of documentation that the change control procedure is sufficient to:</p> <ul style="list-style-type: none"> <li>- identify approval authorities for undertaking change depending on the level of impact</li> <li>- document the reason for change</li> <li>- describe and priorities the change</li> <li>- uniquely identify all affected components associated with the change</li> <li>- uniquely identifies all the stages of the safety lifecycle and existing products which will need to be revisited</li> <li>- provide sufficient evidence to justify that the change is necessary and continues to meet the safety requirements for all operating modes</li> <li>- defined the means by which the change will be verified and validated and demonstrates why this level of re-verification / revalidation is sufficient</li> <li>- ensure that all operations have been carried out to demonstrate that the required software safety integrity is achieved</li> <li>- control and resolve discrepancies, deviations &amp; waivers</li> </ul>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
2.			<p>Confirm through audit that the transfer and storage mechanisms are suitable to:</p> <ul style="list-style-type: none"> <li>- maintain a master copy of software and its documentation</li> <li>- accurately transfer software information between design, source and object receptacles</li> <li>- of sufficient environmental integrity</li> <li>- protect from unauthorised changes/corruption (including security protocols)</li> <li>- provide a mechanism of disaster recovery</li> <li>- maintain consistency between as designed and as operating</li> </ul>			
2.			<p>For SIL 3+</p> <p>Conduct sample review of all items listed under SIL 1 and also object code &amp; executable versions, data, libraries, operating manuals, test scripts &amp; harnesses, traceability records, inspections &amp; static code analysis, external interfaces (platform, plant, other systems, environment) to determine whether:</p> <ul style="list-style-type: none"> <li>- alternative solutions are evaluated and the ALARP rationale is argued</li> <li>- any proposal to undertake less than 100% re-verification / revalidation of changes items and their interfaces is justified</li> <li>- use of computer based tools to track and manage configuration items, including library management and access, release mechanisms, records of modifications and audit trail of modifications carried out, dependencies between documentation, source and object code</li> <li>- auditable records of configuration status auditing are available which confirm the safety functionality is achieved by the configuration</li> <li>- reviewers and review criteria are identified</li> </ul>			
2.			<p>For SIL 4(+)</p> <p>Conduct a sample functional and physical audit of the system configuration to confirm above sufficient to ensure</p> <ul style="list-style-type: none"> <li>- appropriate, compatible, verified and authorised components are in use</li> <li>- the justification for such is traceable through all levels of design, V&amp;V and functional safety assurance documents and media</li> </ul>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
3.	Software Safety Requirements Specification	To identify the safety functions requirements and safety integrity requirements for the software system (3/7.2.1).	<p>SIL1+</p> <p>Conduct sample inspection of the software requirements documents to confirm that</p> <ul style="list-style-type: none"> <li>- requirement allocation / definition has been carried out to software configuration item level</li> <li>- requirements placed on the software have been reviewed for feasibility addressing functions, interfaces, architecture, SIL, capacity, response times</li> <li>- any interface anomalies or SIL issues are tracked and have either been resolved or else the reason for non-resolution is justified and recorded</li> </ul>	<p>3/Table 1[9.1]</p> <p>3/7.2.2.3</p> <p>3/7.2.2.8</p> <p>3/7.2.2.11</p> <p>a-b</p>	<p>3/7.2.2.2</p> <p>3/7.2.2.6</p> <p>3/7.2.2.9</p> <p>a-d</p> <p>Table A.1</p>	<p>3/7.2.2.4</p> <p>a-f</p> <p>3/7.2.2.7</p> <p>3/7.2.2.10</p>
3.			<p>Conduct sample inspection of the software requirements documents to confirm that the following are defined:</p> <ul style="list-style-type: none"> <li>- modes of operation</li> <li>- identification of safe state</li> <li>- use of health monitoring and alarms</li> <li>- on- &amp; off- line test of safety functions</li> <li>- features facilitating modification</li> <li>- capacity and response times</li> <li>- the SIL of each operational function</li> <li>- the existence of any non-safety functions</li> <li>- any interface constraints (hardware, operator etc)</li> </ul>			
3.			<p>SIL 2+</p> <p>In carrying out the above inspection, make an assessment of the adequacy of requirements specification in terms of clarity, precision, , unequivocal, verifiability, testability, maintainability, feasibility, understandability</p> <p>Undertake a sample review of the specification to confirm traceability to the interfacing specifications (operator, hardware, system, environment, peer systems etc).</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
3.			<p>SIL 3+</p> <p>Undertake an inspection of the specification to confirm that a systematic technique has been used throughout which supports representation of the mathematical properties of the system behaviour and performance.</p> <p>Extend the traceability study to a full forward coverage of the traceability from system level requirements to software requirements.</p>			
3.			<p>SIL 4(+)</p> <p>Undertake a design review of the specification to confirm that the specification is a sufficient and adequate definition of the mathematical properties of the system behaviour and performance.</p> <p>Extend the traceability study to both forward and reverse coverage of the relevant specifications.</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
4.	Software Safety Verification and Validation Planning	To define the steps/procedures to be used to validate the software against the Software Safety Requirements Specification (3/7.3.2.1)	<p>SIL 1+</p> <p>Confirm through audit that a software Verification, Validation and Test Plan exists which defines the extent to which the following V&amp;V activities will be applied:</p> <ul style="list-style-type: none"> <li>- review/analysis of the software safety requirements specification and of any subsequent change specifications</li> <li>- review/analysis of each design specification, including architectural design, detailed design, module design and coding manuals</li> <li>- review of the module, SW integration, HW integration and software system functions test specifications and test case design criteria</li> <li>- review/test of the operating procedures</li> <li>- code walkthrough and static analysis</li> <li>- review of data structures, application data, modifiable parameters, plant and communication interfaces</li> <li>- conduct of the module, SW integration, HW integration and system functions tests</li> <li>- review of all plans and procedures (including the V&amp;V plan and modification procedures)</li> <li>- conduct of 1st and 2nd party audits</li> </ul> <p>Confirm that the plan defines the criteria, techniques and tools to be used for each activity.</p>	3/7.3.2.1 3/Table A.7	3/7.3.2.2 a-j 3/7.3.2.4	3/7.3.2.3 3/7.3.2.5
4.			<p>Confirm that the plan addresses:</p> <ul style="list-style-type: none"> <li>- the evaluation of the safety function and integrity requirements;</li> <li>- testability, readability and verifiability and modifiability of software components</li> <li>- the pass/fail criteria</li> <li>- the selection of verification strategies, activities and techniques;</li> <li>- the selection and utilisation of verification tools (test harness, special test software, input/output simulators etc.);</li> <li>- the evaluation of verification results;</li> <li>- the means of handling corrective actions</li> <li>- the production of a list of verified items, information used and non-conformances.</li> </ul>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
4.			<p>SIL2+</p> <p>Review the proposed V, V and test methods to determine whether they are consistent with the attributes defined for each category of information by IEC 61508 Part 3 body and Tables.</p> <p>Make a judgement on whether the V, V and test activities have shown compatibility between</p> <ul style="list-style-type: none"> <li>- the output of a phase and its parent specification(s)</li> <li>- the output of a phase and its integration tests</li> <li>- the integration tests and the parent specification(s) tests</li> </ul> <p>Establish whether complexity metrics and test coverage metrics have been produced and whether the existence of incomplete coverage has been adequately justified.</p> <p>Confirm that V&amp;V plans are in place for pre-existing software.</p>			
4.			<p>SIL 3+</p> <p>In addition to above review the verification methods to confirm they address:</p> <ul style="list-style-type: none"> <li>- compliance with requirements</li> <li>- accuracy &amp; consistency</li> <li>- compatibility with host</li> <li>- conformance to standards</li> <li>- accuracy &amp; behaviour of algorithms</li> <li>- partitioning integrity</li> <li>- correct use of hardware addresses &amp; memory mapping</li> <li>- completeness of H/W &amp; S/W configuration</li> <li>- existence of dead code &amp; deactivated code</li> <li>- adequacy of test case coverage</li> </ul>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
4.			<p>Confirm that the test plans address requirements coverage (normal &amp; robustness)</p> <ul style="list-style-type: none"> <li>- operating system anomalies</li> <li>- timing constraints</li> <li>- software exceptions</li> <li>- hardware anomalies</li> <li>- BITE</li> <li>- I/f errors</li> <li>- data parameters</li> <li>- data corruption</li> <li>- insufficient resolution</li> <li>- incorrect sequencing</li> <li>- algorithm failure</li> <li>- compiler errors</li> </ul>			
4.			<p>SIL 4(+)</p> <p>Make a judgement of the extent to which the V&amp;V process will be able to show that the specifications are a complete, consistent and sufficient description of the mathematical and performance behaviour of the software.</p> <p>Make a judgement on the extent to which statistical analysis of test coverage will be used to support confidence testing of software</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
5. Properties Common to following items 8, 10, 11 and 12	Software design General requirements		<p>SIL1(+)</p> <p>Conduct a sample inspection of each level of the software documentation to make a judgement on the extent to which it achieves:</p> <ul style="list-style-type: none"> <li>- Control of complexity (e.g. through abstraction, modularity, information hiding, encapsulation)</li> <li>- Captures the necessary behaviour and performance information (eg functionality, information flow, sequencing and response time, concurrency, data structures, design assumptions)</li> <li>- is understandable and unambiguous</li> <li>- is capable of verification and validation</li> <li>- is testable and modifiable</li> <li>- any changes at interfaces are agreed with all parties to that interface</li> </ul> <p>That the operating system version, including “service pack” or equivalent issue, upon which any compiler or application software is to be run is defined and recorded.</p> <p>Confirm that responsibilities for preparation of each level of software are defined.</p>	7.2.2.6 7.4.2 7.4.5 7.4.6		
5. Properties common to items 7, 8, 9 & 11			<p>SIL 4+</p> <p>Ensure that justification of sufficient independence is based on allocation into different hardware platforms with protection against lower SIL software corrupting the interfaces.</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
6.	Design methods and Development Tools	To provide a suitable set of development tools for the required safety integrity level.	<p>SIL1+</p> <p>Identify and inspect the proposed design methods, tools and languages to form a judgement on whether:</p> <ul style="list-style-type: none"> <li>- an integrated set of tools, including languages, compilers, configuration management tools, and automatic testing tools has been selected which is also suitable for modification during subsequent lifecycle stages</li> </ul> <p>Identify and inspect the design and programming language(s) to form a judgement on whether:</p> <ul style="list-style-type: none"> <li>- The operating system version, including “service pack” or equivalent issue, upon which any compiler or application software is to be run is defined and recorded.</li> <li>- the translator/compiler has been shown to be sufficiently error free</li> <li>- are completely and unambiguously defined or restricted to unambiguously defined features</li> <li>- match the characteristics of the application;</li> <li>- contain features that facilitate the detection of programming mistakes</li> <li>- provide features that are compatible with the design method.</li> </ul> <p>If there are any weaknesses, assess whether a justification has been provided to demonstrate the suitability of the programming language that details its fitness for purpose and any additional measures to address shortcomings.</p> <p>Check Coding standards specify good practice and prescribe unsafe language features. Check they also specify procedures for source code documentation.</p>	3/7.4.4.1 3/7.4.4.2 3/7.4.4.3 3/7.4.4.4 3/7.4.4.5 3/7.4.4.6		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
7.	Software Architecture Design Description.	To define and justify the software architecture which meets the Software Safety Requirements Specification.	<p>SIL 1+</p> <p>Conduct the activities described in Software Design General Requirements above and:</p> <p>SIL1+</p> <p>Conduct a sample inspection of the software architecture specification to make a judgement on the extent to which it:</p> <ul style="list-style-type: none"> <li>- defines and provides justification for an integrated set of techniques and measures in accordance with the Tables and addressing both fault tolerant and fault avoidance techniques</li> <li>- provides partitioning into components</li> <li>- identifies each component as either new or existing</li> <li>- justifies the extent to which pre-existing components and their interfaces to the current system have been previously verified</li> <li>- demonstrates the adequacy of software/hardware interactions</li> <li>- provides proof test, diagnostics and self test</li> <li>- minimises safety related parts</li> <li>- specifies design features for maintaining the integrity of data, including plant input-output data, communications data, operator interface data, maintenance data and internal database data</li> <li>- specifies appropriate software architecture integration test cases</li> </ul> <p>SIL1+</p> <p>Confirm that structured design methods and notations are used.</p>	3/Table 1[9.3] 3/7.4.3.3	3/7.4.3.1 Annex Tables A.2, B.7	3/7.4.3.2 a-f
7.			<p>SIL2+</p> <p>Confirm that deterministic algorithms are used.</p>			
7.			<p>SIL3+</p> <p>Confirm that the design is resilient to faults.</p>			
7.			<p>SIL4(+)</p> <p>Confirm that the specification represents the mathematical behaviour and performance properties and that defensive programming techniques are used to protect against faults.</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
8.	Software System Design Specification	To define the major components and subsystems of the software system.	<p>Conduct the activities described in Software Design General Requirements above and:</p> <p>SIL1+</p> <p>Conduct a sample inspection to determine the extent to which the design achieves:</p> <ul style="list-style-type: none"> <li>- partitioning of software configuration items into modules</li> <li>- specification of appropriate integration and module tests</li> <li>- use of structured design and programming methods, a module approach</li> </ul>	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
8.			<p>SIL2+</p> <p>Conduct a sample inspection to determine the extent to which the design:</p> <ul style="list-style-type: none"> <li>- uses methods with semantics which represent the behaviour of the system</li> <li>- uses design and coding standards</li> </ul>			
8.			<p>SIL3+</p> <p>Conduct a sample inspection to determine the extent to which the design:</p> <ul style="list-style-type: none"> <li>- uses automated and integrated toolkits to reduce error</li> <li>- uses defensive programming techniques to protect against error</li> </ul>			
8.			<p>SIL 4+</p> <p>Conduct a sample inspection to determine the extent to which the design:</p> <ul style="list-style-type: none"> <li>- uses methods with formally defined semantics which represent the behaviour of the system.</li> </ul>			
9.	Software Module Design Specification	To define the detailed design of each module required by the Software Design Specification.	Conduct the activities described in Software Design General Requirements above.	3/Table 1[9.3]	3/7.4.5.4	

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
10.	Coding Manual	To define programming practices to be used and the procedures for source code documentation.	SIL1+ Conduct an audit of the (documented) coding manual to determine whether coding standards are: - reviewed as fit for purpose - used for the development of all relevant software	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
10.			Form a judgement on whether the coding standards: - specify good programming practice - proscribe unsafe language features - specify procedures for source code documentation including, owner, author, description; inputs and outputs; configuration management history.			
10.			SIL2+ Form a judgement on whether the coding standards: - proscribe use of dynamic objects and unconditional branching - provide compile time checking - identify features of the support environment or language which should not be used, ie Safe language sub-sets and libraries			
10.			SIL3+ Form a judgement on whether the coding standards: - proscribe use of dynamic variables - limit use of interrupts, pointers and recursion - provide run time control and data checks			
10.			SIL4(+) Form a judgement on whether the coding standards: - address safe use of system resources - address safe execution order and duration - address precision & accuracy of calculations - address use of diverse functions to avoid tool error - address safe exception handling			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
11.	Software Module Source Code Listing	To define source code that meets the Software Module Design specification.	<p>Conduct the activities described in Software Design General Requirements above and:</p> <p>SIL 1+ Undertake a sample inspection to determine whether the coding conforms to the defined coding standards.</p>	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
11.			<p>SIL2+ Undertake a sample inspection to determine whether the coding has been shown to possess good control flow and data use characteristics and any anomalies have been explained.</p>			
11.			<p>SIL3+  SIL4(+) Undertake a sample inspection to determine whether the coding has been shown to comply through semantic assessment against the design specifications and any anomalies have been explained</p>			
12 Properties common to items 15, 17, 20, 23 & 26	general test specification requirements		<p>SIL1+ Conduct a sample inspection of each level of test specifications to determine whether:</p> <ul style="list-style-type: none"> <li>- software tests are specified concurrently with the design and development activities</li> <li>- the specified software tests address procedures for corrective action on failure</li> <li>- are adequate to show that the software correctly perform the specified functional and integrity requirements</li> <li>- are adequate to show that the software does not perform unintended functions (see expected test coverage below)</li> </ul>	7.4.7 7.4.8 7.5 7.7		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
13  Properties common to items 18, 21, 24 & 27	general test log requirements		<p>SIL1+</p> <p>Conduct a sample inspection of the test records to confirm that the following information is available:</p> <ul style="list-style-type: none"> <li>- a chronological record of test activities is available</li> <li>- the version of the specification against which the testing is conducted</li> <li>- the version of the software safety validation plan</li> <li>- the safety function being validated;</li> <li>- the tools, equipment and calibration data used;</li> <li>- the configuration identification of the item under validation</li> <li>- the procedures applied</li> <li>- the test environment;</li> <li>- the input stimuli and other events applied to the test configuration</li> <li>- record of discrepancies between expected and actual results</li> <li>- analysis of discrepancies with the decisions on how to proceed after occurrence of a discrepancy and rationale</li> </ul>	7.4.7 7.4.8 7.5 7.7		
14  Properties common to items 16, 19, 22, 25 & 28	general test result requirements		<p>SIL1+</p> <p>Conduct a sample inspection of each level of test results to determine:</p> <ul style="list-style-type: none"> <li>- whether the component was actually tested in accordance with the V&amp;V plan and against the specs developed during design (note – the V&amp;V plan will identify the rigour of the test methods to be applied for each SIL as detailed above)</li> <li>- whether the results show the component provides the intended functions</li> <li>- the adequacy of the documented results</li> <li>- whether the results have been analysed to determine the adequacy of the software</li> <li>- that on test failure procedures for corrective action are followed</li> </ul>	7.4.7 7.4.8 7.5 7.7		
14			<p>SIL1+</p> <p>Conduct a sample review of each level of test documentation to determine:</p> <ul style="list-style-type: none"> <li>- the extent to which the tests show the component does not perform unintended functions - at SIL 1 this shall be judged on coverage of the functional 'black box' interface to the software component</li> </ul>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
14			<p>SIL2+</p> <p>Conduct a sample review of each level of test documentation to determine:</p> <ul style="list-style-type: none"> <li>- the extent to which the tests show the component does not perform unintended functions - at SIL 2 this shall also be judged on coverage testing of the paths through the software (which should be traced to and compared with coverage at the functional level)</li> <li>- whether appropriate rigour has been applied as detailed in the V&amp;V plan.</li> </ul>			
14			<p>SIL3+</p> <p>Conduct a sample review of each level of test documentation to determine:</p> <ul style="list-style-type: none"> <li>- the extent to which the tests show it does not perform unintended functions – at SIL 3 this shall also be judged on coverage of response times, memory constraints and avalanche and stress testing, and shall include unusual modes of operation</li> <li>- whether appropriate rigour has been applied as detailed in the V&amp;V plan.</li> </ul>			
14			<p>SIL4(+)</p> <p>Conduct a sample review of each level of test documentation to determine:</p> <ul style="list-style-type: none"> <li>- the extent to which the tests show it does not perform unintended functions – at SIL 4 this shall also be judged on the extent to which analytical analysis demonstrates that no non-tested behaviour is present in the software</li> <li>- whether appropriate rigour has been applied as detailed in the V&amp;V plan.</li> </ul> <p>Conduct a sample inspection of each level of test documentation to determine the extent to which statistical analysis confirms the confidence levels associated with the test predictions.</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
15.	Software Module Test Specification	To define the steps and procedures to test the source code of a module against its Software Module Design Specification.	Conduct the activities described in Software General Test Specification requirements.	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
16.	Software Module Test Report	To report the results of software module testing	Conduct the activities described in Software General Test Result Requirements and:  SIL2+ Control and data use coverage should be conducted at the source code level and traceable to the software requirements specification	3/7.4.7.3		
17.	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).	Conduct the activities described in Software General Test Specification requirements and  SIL1+ Conduct an inspection to form a judgement on whether - a phased integration approach is planned - documentation is available on test cases and test data; test types; test environment, tools, configuration and programs; test criteria - change impact analysis processes are required	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
18.	Software System Integration and Test Log	To provide a chronological record of the software system integration and testing.	Conduct the activities described in Software General Test Log Requirements	3/7.5.2.7		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
19.	Software Integration and Test Report	To report the results of integrating and testing the software system against the Software System Integration and Test Specification.	<p>Conduct the activities described in Software General Test Result Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether:</p> <ul style="list-style-type: none"> <li>- documentation is available on test cases and test results</li> <li>- a clear statement is available on whether the objectives and criteria of the test criteria have been met</li> <li>- if there is a failure, the reasons for that failure are documented</li> <li>- if the software is subject to modification or change a documented record of the change impact assessment exists which identifies the modules impacted, the re-design and the re-validation activities</li> </ul>	3/Table 1[9.4]	3/7.4.8.4	
20.	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.	<p>Conduct the activities described in Software General Test Specification Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- the test provide a means to evaluate the fault tolerance mechanisms and their suitability to meet the architectural requirements specification</li> <li>- documentation is available on test cases and test data; test types; test environment, tools, configuration and programs; test criteria</li> <li>- change impact analysis processes are required</li> </ul>	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
21.	Software Architecture Integration and Test Log	To provide a chronological record of the software architecture integration and testing.	Conduct the activities described in Software General Test Log Requirements.			
22.	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.	<p>Conduct the activities described in Software General Test Results Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- provide the results of an evaluation of the fault tolerance mechanisms and their suitability to meet the architectural requirements specification</li> </ul>	3/7.4.8.4		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
23.	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)	<p>Conduct the activities described in Software General Test Specification Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- the test provide the means to evaluate compatibility of H/W and S/W at three distinct levels: S/W on target H/W; integration with sensors and actuators; full integration with EUC</li> <li>- the specification recognises that at different locations only limited ability to exercise the full behaviour during integration, and in particular identifies where site access is required to complete testing</li> <li>- documentation is available on test cases and test data; test types; test environment, tools, configuration and programs; test criteria</li> <li>- change impact analysis processes are required</li> </ul>	3/Table 1[9.4] 3/7.5.2.4 a-c 3/7.5.2.7	3/7.5.2.1 3/7.5.2.5 3/7.5.2.8	3/7.5.2.3 3/7.5.2.6
24.	PE and Software Integration Test Log	To provide a chronological record of the programmable electronics and software integration and testing.	Conduct the activities described in Software General Test Log Requirements	3/7.5.2.7		
25.	PE and Software Integration Test Report	To report the results of testing against the PE and Software Integration Test Specification.	<p>Conduct the activities described in Software General Test Report Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- the results provide an evaluation of the compatibility of H/W and S/W at three distinct levels:</li> <li>- S/W on target H/W</li> <li>- integration with sensors and actuators</li> <li>- full integration with EUC</li> </ul>	3/7.5.2.8		

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
26.	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)	<p>Conduct the activities described in Software General Test Specification Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- the test provide the means to evaluate achievement of the software functions and integrity specification</li> <li>- the test provides the means to evaluate interactions with the system, operator and hardware functions and constraints</li> <li>- the specification recognises that at different locations only limited ability to exercise the full behaviour during integration, and in particular identifies where site access is required to complete testing</li> <li>- documentation is available on test cases and test data; test types; test environment, tools, configuration and programs; test criteria</li> <li>- change impact analysis processes are required</li> </ul>	3/7.3.2.1 3/Table A.7	3/7.3.2.2 a-j 3/7.3.2.4	3/7.3.2.3 3/7.3.2.5
27.	Software Safety Validation Log	To provide a chronological record of the Software Safety Validation (3/7.7.1.1).	Conduct the activities described in Software General Test Log Requirements	3/7.7.2.3		
28.	Software Safety Validation Report	To report all the results (detailed and overall) of the Software Safety Validation (3/7.7.1.1).	<p>Conduct the activities described in Software General Test Results Requirements and</p> <p>SIL1+</p> <p>Conduct an inspection to form a judgement on whether</p> <ul style="list-style-type: none"> <li>- the results provide an assessment of the means to evaluate achievement of the software functions and integrity specification</li> <li>- the test provides the means to evaluate interactions with the system, operator and hardware functions and constraints</li> </ul>	3/7.7.2.6 a-c Annex Table A.7,B.3,B. 5	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
29.	Software Operation Procedures	To provide information and procedures concerning software necessary to ensure the functional safety of the safety-related system is maintained during operation. (3/7.6.1)	As System Operation requirements.	3/Table 1[9.5] 2/7.6 2/7.6.2.2	3/7.8 Annex Table A.8	2/7.6.2.1 a-g

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
30.	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)	<p>As System Modification requirements plus the following additional requirements:</p> <p>SIL1+</p> <p>Identify and inspect the proposed modification procedures to confirm that prior to any modification being made:</p> <ul style="list-style-type: none"> <li>- the software development procedures are available and are consistent with the above requirements</li> <li>- the modification request is required to be properly documented with the proposed change, rationale for change and appropriate authorisation</li> <li>- that an analysis procedure is in place which will assess the impact on hazards and failure modes, ensure identification of of all documentation which needs to be reworked and the lifecycle stages which will be revisited</li> <li>- the implementation of the modification is planned in accordance with the above procedures and that staff competency is addressed</li> <li>- that the documentation procedures are defined and address all relevant items including analysis, changed documentation and history records</li> <li>- that the configuration management procedures are consistent with the above software lifecycle requirements</li> <li>- that the reverification &amp; revalidation plans address all changed components</li> </ul>	3/7.8.2.1 3/7.8.2.2 a-c 3/7.8.2.5 3/7.8.2.9	2/7.5.2.5 3/7.8.2.3 a-b 3/7.8.2.6 a-d	1/7.16.2.6 3/7.8.2.4 3/7.8.2.8 a-e
30			<p>SIL2+</p> <p>In addition to the above confirm that</p> <ul style="list-style-type: none"> <li>- that the impact analysis and V&amp;V plans address all affected components including side effects or – if this is not possible – that suitable rationale is provided to justify that the revalidation is consistent with the quality of the original validation activity</li> </ul> <p>Inspect the quality of the modification design and revalidation procedures to confirm adequacy as detailed above</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
30			<p>SIL 3+</p> <p>In addition to the above confirm that</p> <ul style="list-style-type: none"> <li>- that the impact analysis and V&amp;V plans address the complete system or</li> <li>- if this is not possible – that suitable rationale is provided to justify that the revalidation is consistent with the quality of the original validation activity. Undertake a technical review of the adequacy of the justification if given.</li> </ul> <p>Inspect the quality of the modification design and revalidation procedures in greater detail to confirm adequacy as detailed above</p>			
31.	Software Modification Log	To record the details of all software modifications, their impacts and progress (3/7.8.1)	<p>As System Modification requirements plus the following additional requirements:</p> <p>SIL1+</p> <p>Identify and inspect the modification records to confirm:</p> <ul style="list-style-type: none"> <li>- all aspects have been carried out in accordance with the procedures</li> <li>- the original modification request and authorisation is suitable</li> <li>- a suitable impact analysis has been carried out</li> <li>- that the lifecycle processes used are consistent with the SIL requirements</li> <li>- that the reverification and revalidation procedures are consistent with the SIL requirements and that all results are recorded</li> <li>- that the configuration management processes are consistent with the SIL requirements</li> </ul> <p>Confirm that the modification records address:</p> <ul style="list-style-type: none"> <li>- the original modification request</li> <li>- the impact analysis</li> <li>- the modification planning</li> <li>- the changed lifecycle documentation</li> <li>- the V&amp;V criteria and results</li> <li>- any deviations from normal operating conditions either as a temporary or permanent feature of the modification</li> <li>- any concessions with rationale for their acceptance.</li> </ul>	3/7.8.2.4	2/7.8.2.8 a-e	2/7.8.2.9

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
31			SIL 2+ In addition to the above carry out sample inspections of documents within the scope of the modification to determine the adequacy of the work carried out and that all side effects have been adequately addressed.			
31			SIL3+ In addition to the above carry out sample inspections of documents throughout the system to determine the adequacy of the work carried out and that all side effects have been adequately addressed.			
32.	Software Modification Report	To record all change requests for the PES software, their impact and progress.	As System Modification requirements plus the following additional requirements:  As modification logs but in addition ensure there is a clear statement that the results of the modification have demonstrated that either a) the hazard and risk assessment is unaffected by the modification, and the software continues to satisfy the safety requirement or b) a suitable revised hazard and risk assessment has developed a suitable new safety requirement and the software is consistent with the revised safety requirement	3/Table 1[9.5]	3/7.8.2.8 a-e	
33.	Verification Reports	These generic attributes apply to each Verification Report. The individual reports are identified in the following rows of the table.	SIL1+ Conduct a sample review of the verification reports prepared in accordance with the verification plans detailed above to make a judgement on the extent to which for the following attributes have been demonstrated: - that the verification activities have been conducted in accordance with the verification plans - that the results of the verification are documented and show that the lifecycle phase outputs meet phase objectives, achieve functional & integrity requirements and are compatible with previous phase	3/7.9.2.4	3/7.9.2.5	3/7.9.2.6

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
34.	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.	<p>As fully validated E/E/PES above plus following additional requirements:</p> <p>Conduct an inspection to determine whether any data configuration required to adapt the software to the fully functioning PE has been identified, implemented, verified and validated (see below)</p> <p>Conduct and inspection to determine whether interfaces between S/W and PE have been verified and tested as follows:</p> <p>SIL1+ positive and negative functional testing with traceability between interface definition and tests</p>	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
34.			SIL2 + coverage of equivalence classes at interface between hardware and software traceable, recorded and of sufficient defined coverage			
34.			SIL3+ performance testing and/or simulation of HW/SW interface parameters recorded and justified achieved			
34.			<p>SIL4(+) design review of HW/SW interface parameters confirms suitability; test metrics supported by probabilistic analysis to determine confidence</p> <p>Conduct and inspection to determine whether configuration control has been applied sufficient to ensure that the (fully traceable) compiled object code is resident in the correctly identified PE (see above)</p>			

	TOE	Purpose of TOE	Assessment Prompt List	Referring IEC 61508 Clauses and Tables		
35.	Fully Functioning Software and PE	To provide a complete software system on PE for validation testing.	<p>As fully functioning E/E/PES above plus the following additional requirements:</p> <ul style="list-style-type: none"> <li>- any data configuration required to adapt the software to the fully functioning PE has been identified, implemented, verified and validated (see below)</li> <li>- configuration control has been applied sufficient to ensure that the (fully traceable) compiled object code is resident in the correctly identified PE (see above)</li> </ul>	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
36	FUNCTIONAL SAFETY ASSESSMENT		<p>As System Modification requirements plus the following additional requirements:</p> <p>SIL3+ Conduct a sample inspection to confirm that a software functional failure analysis programme has been carried out and documented such that the software component functional behaviour can be linked to the system hazards.</p> <p>Conduct a sample inspection to determine that a suitable common cause failure analysis has been carried out and documented for the software components and their interaction with the hardware components.</p>	3/8 Table A.10		