## Introduction

This conformity assessment template is for E/E/PE safety-related systems under IEC 61508-2:2010, *Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 2: Requirements for electrical / electronic / programmable electronic safety-related systems* (See notes below for when this template is used rather than others).

The following notes should be read prior to the assessment:

## General Notes

1. For general guidance on using CASS conformity assessment documents, refer to *The CASS Guide* available from [www.61508.org/cass](http://www.61508.org/cass) (Document: ‘*CASS-Guide-A’).*
2. Use of this template assumes acceptance of the CASS scheme liability disclaimer in ‘*CASS-Guide-A*’.
3. This conformity assessment template does not replace the standard (IEC 61508-2:2010), it is intended to be used in conjunction with a copy of the standard as a method to manage the assessment of functional safety to support the assessor. The “Purpose of TOE” is a general guide to provide context and scope, and it is the assessor’s responsibility to ensure compliance with all the relevant clauses within the standard.
4. The supporting documents section shall be used to reference evidence and documentation that supports the assessor’s findings and comments.
5. The assessor’s comment section shall be used for positive reporting including reference to the document sections / clauses relevant to evidence compliance.

## Template Specific Notes

1. This assessment template should be used in conjunction with other CASS templates for IEC 61508 (see reference documents below).
2. This template should be used when the full scope and application of the E/E/PES is known (normally defined in the safety requirements specification) and covers all lifecycle phases from specification through to validation and supporting procedures. In certain circumstances, this can apply to large scale, significant or complex E/E/PE *subsystems*, in which case this template may also be suitable for their assessment prior to their integration into the overall E/E/PES.
3. This assessment template assumes that the E/E/PES is formed from elements (and generally subsystems) that are already assessed to the IEC 61508 series of standards, especially the more complex subsystems. See the assessment template CASS-508-SUB which can be used for the assessment of elements. Products that are pre-compliant (e.g., appropriately certified) to IEC 61508 may be acceptable if found to be suitable for the target application.
4. This conformity assessment template should be used when one of the sector standards (e.g., IEC 61511, IEC 62061) do not apply.
5. For every TOE, generally the rigour shall increase with increasing SIL; guidance on SIL can also be found in the tables in IEC 61508-2 Annex B (Tables B1 to B6).
6. Compliance with the techniques & measures detailed in Annex A and B of IEC 61508-2 is required to support an assessment using this template. The assessment documentation must include a section detailing this compliance (as it is not covered within this template).

## References

* CASS-508-FSM – Functional Safety Management (IEC 61508-1)
* CASS-508-SLC – Safety Lifecycle (IEC 61508-1)
* CASS-508-SUB – Subsystem Element (IEC 61508-2)
* CASS-508-SW – Software (IEC 61508-3)

Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
|  |  |
| CASS | Conformity assessment of safety-related systems |
| E/E/PES | Electrical/Electronic/Programmable-Electronic safety-related System |
| FSA | Functional safety assessment |
| FSM | Functional safety management |
| HFT | Hardware Fault Tolerance |
| SFF | Safe Failure Fraction |
| SIL | Safety integrity level |
| TOE | Target of evaluation |

## Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of Change |
| V1 | 2016 | Updated for IEC 61508-2:2010 |
| V2 | 03/11/2023 | Updated to new naming convention; restructured for dual template approach. |
|  |  |  |
|  |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61508 references** | **Supporting documents** | **Assessor’s comments**  **(IEC 61508-2:2010)** |
| --- | --- | --- | --- | --- | --- |
| **0** | IEC 61508 Conformance | To ensure there is general evidence for conformance with IEC 61508-1 and, where relevant, IEC 61508-3. | 1/4,  2/4,  3/4. |  |  |
| **1** | E/E/PES Safety Lifecycle | To structure the realisation of the E/E/PES into defined phases and activities that will allow the safety of the E/E/PES to be specified, developed, verified, etc. | 2/7.1.3,  2/7.1 – 2/7.9,  2/7.4.2.14,  Table 1. |  |  |
| **2** | E/E/PES Safety Plan | To check the provisions of FSM have been implemented on this E/E/PES. | 2/6. |  |  |
| **3** | E/E/PES Design Requirements Specification | To ensure that the safety function(s) requirements and safety integrity requirements are identified for the E/E/PES and its subsystems and elements (2/7.2.1). | 2/Table 1[10.1],  2/7.2.2.1,  2/7.2.2.2,  2/7.2.3.1,  2/7.2.3.2 a-j,  2/7.2.3.3 a-g,  2/7.2.3.4,  2/7.2.3.5,  2/7.2.3.6,  2/Table B.1. |  |  |
| **4** | E/E/PES Verification Plan | To ensure there is an overall verification plan for all phases of the E/E/PES lifecycle, defining how the outputs of each phase are to be evaluated for correctness and consistency with all the relevant phase inputs. | 2/7.9.2.1 – 2/7.9.2.10,  2/Table 1[10.4],  2/Table B.1,  2/Table B.2,  2/Table B.3,  2/Table B.4,  2/Table B.5. |  |  |
| **5** | E/E/PES Design Requirements Specification - Verification Report | To ensure that the verification of the E/E/PES Design Requirements Specification is documented (as planned) including the verification results. | 2/7.9.2.6,  2/7.9.2.7. |  |  |
| **6** | E/E/PES Safety Validation Plan | To ensure that the steps / procedures to be used to validate the E/E/PES against the E/E/PES Safety Requirement Specification and the E/E/PES Design Requirements Specification had been defined (2/7.3.2.1) | 2/7.3.2.1,  2/7.3.2.2 a-g,  2/7.7.2.7,  2/Table B.5. |  |  |
| **7** | E/E/PES Validation Planning – Verification Report | To ensure that the verification of the E/E/PES Validation Planning is documented (as planned) including the verification results. | 2/7.9.2.6. |  |  |
| **8** | Design and Development – General | To define and justify the architectural design, detailed design and hardware implementation of the E/E/PES that meets the requirements of the E/E/PES Design Requirements Specification (2/7.4.1). This includes sub-system/element design and test specifications where relevant. | 2/Table 1[10.3],  2/7.4.2.1 – 2/7.4.2.14,  2/Annex E,  2/Annex F. |  |  |
| **9** | Design and Development – Synthesis of Elements | To ensure that the design and development has, when used, correctly partitioned the E/E/PES into elements of different systematic capability. | 2/Table 1[10.3],  2/7.4.3.1 – 2/7.4.3.4. |  |  |
| **10** | Design and Development – Architectural Constraints | To ensure that the design and development has correctly applied Route 1H and / or Route 2H (including SFF and HFT), as applicable. | 2/Table 1[10.3],  2/7.4.4.1 – 2/7.4.4.3,  2/Table 2 & 3,  2/Annex A,  Table A1 –Table A14,  2/Annex C. |  |  |
| **11** | Design and Development – Subsystems and elements | To ensure that each subsystem and element in the E/E/PES has been independently assessed for its suitability in the target application, in terms of its:   * Functional specification, * Conformity with all relevant parts / requirements of IEC 61508, * Adherence to all restrictions and / or conditions of use stated in the safety manual.   NOTE: The CASS subsystem / element template may be used to perform this assessment (if access to the relevant design authority evidence is possible). Appropriately assessed or certified products with a safety manual may also be acceptable. | 2/7.2 – 2/7.4,  2/7.7 – 2/7.9,  2/8. |  |  |
| **12** | Design and Development – Random Hardware Failures | To ensure that the design and development has correctly estimated the hardware failure rates for the E/E/PE system (relevant to each safety function), based on a system analysis of failure data from each element/subsystem. To ensure that these estimates for the E/E/PE system are equal to or less than the defined target failure rate in the safety requirements specification. | 2/Table 1[10.3],  2/7.4.5.1 – 2/7.4.5.5,  2/Annex A Table A1 – Table A14. |  |  |
| **13** | Design and Development – Avoidance of Systematic Faults | To ensure an appropriate group of techniques and measures were used to avoid systematic faults during design and development. | 2/Table 1[10.3],  2/7.4.6.1 – 2/7.4.6.7,  2/Annex B Table B2 |  |  |
| **14** | Design and Development – Control of Systematic Faults | To ensure an appropriate group of techniques and measures were used to control systematic faults during design and development. | 2/Table 1[10.3],  2/7.4.7.1 – 2/7.4.7.3,  2/Annex A Table A15 – Table A18. |  |  |
| **15** | Design and Development – Behavior on Detection of Fault | To ensure that the design and development has appropriate consideration to subsystem reaction(s) upon detection of a dangerous fault. | 2/Table 1[10.3],  2/7.4.8.1 – 2/7.4.8.3. |  |  |
| **16** | Design and Development – Implementation | To ensure that the E/E/PES has been implemented according to the E/E/PES Design Requirements Specification and that all the relevant design and user information is documented and available. | 2/Table 1[10.3],  2/7.4.9.1 – 2/7.4.9.7,  2/Annex A Table A1 – Table A14,  2/Annex C,  2/Annex D. |  |  |
| **17** | Design and Development – Proven-in-Use | To ensure that, when used, the concept of proven-in-use is only applied to elements with clearly restricted and specified functionality and only when there is adequate documentary evidence for a suitably low occurrence of dangerous systematic faults. | 2/Table 1[10.3],  2/7.4.10.1 – 2/7.4.10.7. |  |  |
| **18** | Design and Development – Data Communications | To ensure that, when used, the approach for data communications used in the implementation of safety functions considers failure rates and appropriate techniques and measures suitable for the safety integrity. | 2/Table 1[10.3],  2/7.4.11.1 – 2/7.4.11.2. |  |  |
| **19** | E/E/PES Design and Development – Verification Report | To ensure the E/E/PES Design and Development verification is documented (as planned) including the verification results. | 2/7.9.2.5,  2/7.9.2.6,  2/7.9.2.8,  2/7.9.2.10. |  |  |
| **20** | E/E/PES Integration Test Specification | To ensure the steps / procedures (incl. techniques and measures) for integrating the software and hardware of the E/E/PES are defined and ensure that the tests for demonstrating that the integrated E/E/PES satisfies the E/E/PES Design Documentation are detailed. | 2/7.4.2.11,  2/7.4.6.5,  2/7.5.2.7,  2/7.9.2.10,  2/Table B.3. |  |  |
| **21** | E/E/PES Integration | To ensure that E/E/PES Integration satisfies the requirements of the E/E/PES Design Documentation. | 2/7.5.2.1 – 2/7.5.2.3,  2/Table 1[10.4]. |  |  |
| **22** | E/E/PES Integration Test Report | To ensure that the appropriate documentation details the results of the integration testing. | 2/7.5.2.4,  2/7.5.2.5, 2/7.5.2.6,  2/7.9.2.10,  2/Table 1[10.4]. |  |  |
| **23** | E/E/PES Integration – Verification Report | To ensure the E/E/PES Integration verification is documented (as planned) including the verification results. | 2/7.9.2.6,  2/7.9.2.9,  2/7.9.2.10. |  |  |
| **24** | E/E/PES Operation and Maintenance Procedures | To ensure that the procedures to be used to maintain and operate the E/E/PES are prepared during the design stage and are complete (2/7.6.1).  NOTE: The element safety manual(s) should be available with the E/E/PES procedures for O&M. | 2/7.6.2.1 – 2/7.6.2.5,  2/7.4.6.3,  2/Table B.4,  2/Annex D (for elements). |  |  |
| **25** | E/E/PES Operation and Maintenance Procedures – Verification Report | To ensure that the verification of the E/E/PES Operation and Maintenance Procedures is documented (as planned) including the verification results. | 2/7.9.2.6. |  |  |
| **26** | E/E/PES Safety Validation | To ensure that appropriate E/E/PES validation is carried out as planned and documented including all validation results. (2/7.7.2.4). | 2/7.7.2.1 - 2/7.7.2.7,  2/Table 1[10.6],  2/Table B.5. |  |  |
| **27** | E/E/PES Safety Validation - Verification Report | To ensure that the E/E/PES validation report is verified and documented (as planned) including the verification results. | 2/7.9.2.6,  2/7.9.2.10. |  |  |
| **28** | E/E/PES Modification Procedures | To ensure the procedures to be used during modification of the E/E/PES were defined; 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/PE in a system. | 1/7.16.2.6,  2/7.4.10.7,  2/7.5.2.5,  2/7.8.2.1 – 2/7.8.2.4.  Requires same level of expertise (competence) as design. |  |  |
| **29** | E/E/PES Modification Report | To ensure that all change requests for the E/E/PES, their impact, progress and status are recorded / documented. | 2/7.8.2.1 – 2/7.8.2.4,  2/Table 1. |  |  |
| **30** | E/E/PES Modification – Verification Report | To verify the E/E/PES modification is carried out as intended including the documentation of results. | 2/7.9.2.6,  2/7.9.2.10. |  |  |
| **31** | E/E/PES Functional Safety Assessment (FSA) | To ensure that appropriate FSAs are planned as delivered for the E/E/PES.  NOTE: This TOE may not be applicable when this template is used to support an FSA. | 1/8,  2/8. |  |  |
| **32** | FSA – Verification Report | To ensure that FSA verification is documented (as planned) including the verification results.  NOTE: This TOE may not be applicable when this template is used to support an FSA. | 2/7.9. |  |  |