## Introduction

This conformity assessment template is for safety-related elements and most subsystems 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*.

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. A full E/E/PE system (developed or integrated from pre-compliant subsystems/elements) that needs to comply with IEC 61508 can be assessed using CASS-508-SYS (see references below). In certain circumstances, CASS-508-SYS may also be more suitable for large scale, significant or complex E/E/PE subsystems where the specific target application is known. Ultimately this decision is something the assessor should make considering all factors on a case-by-case basis.
3. 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 B5).
4. 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-SYS – System (IEC 61508-2)
* CASS-508-SW – Software (IEC 61508-3)

## Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
|  |  |
| *λD* | *Dangerous failure rate* |
| *CASS* | *Conformity assessment of safety-related systems* |
| *DC* | *Diagnostic coverage* |
| *E/E/PE* | *Electrical, electronic and programmable electronic* |
| *FSA* | *Functional safety assessment* |
| *FSM* | *Functional safety management* |
| *HFT* | *Hardware fault tolerance* |
| *MRT* | *Mean repair time* |
| *QMS* | *Quality management system* |
| *SC* | *Systematic capability* |
| *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 and TOEs added / adjusted |
|  |  |  |
|  |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61508 reference** | **Supporting documents** | **Assessor’s comments**  **(IEC 61508-2:2010)** |
| --- | --- | --- | --- | --- | --- |
| 0 | IEC 61508 Conformance | To ensure there is general evidence for conformance with the relevant clauses of IEC 61508-1 and, where applicable, IEC 61508-3. | 1/4 (2/4),  1/5 (2/5),  1/6 (2/6),  3/4. |  |  |
| 1 | Safety lifecycle | To ensure that the E/E/PE element / subsystem safety lifecycle phases are structured, in a systematic manner, to support the achievement of functional safety.  NOTE: For simpler devices, this may be a QMS based approach. | 2/7.1.3. |  |  |
| 2 | Safety requirements | To ensure that detailed safety requirements and safety assumptions are defined to satisfy the safety integrity and enable the validation of the element or subsystem. | 2/7.2.2. |  |  |
| 3 | Product identification | To ensure the element / subsystem is clearly identified, for both hardware and software, to enable configuration management and to support integration into a system(s). | 2/7.4.9.3 (d). |  |  |
| 4 | Functional specification | To ensure that the functional requirements for the element / subsystem are sufficiently detailed before implementation.  NOTE: At this stage it is recommended to consider carefully the suitability and relevance of any selected general failure data sources. | 2/7.2.3,  2/7.4.3,  2/7.4.9.3 (a),  2/7.4.9.5. |  |  |
| 5 | Verification and validation planning | To ensure the verification of each lifecycle phase output and the validation of the element or subsystem is planned prior to performing those activities. | 2/7.3.2,  2/7.9.2.1 –  2/7.9.2.4. |  |  |
| 6 | Suitability of component failure data | To ensure that any failure data is of a sufficient confidence level before it is used for the estimation of any failure rates. | 2/7.4.9.5, Note (1), (2),  Table B.6,  2/7.4.10.4,  2/7.4.10.5. |  |  |
| 7 | Quantitative failure analysis | To ensure that the quantitative estimated failure analysis is reasonable for the intended SIL considering:   * Is the element safety function (IEC 61508-4, 3.5.3) stated for which the analysis relates? * Are all items in the assembly included and their reference to the drawing / circuit / BoM? * Is the rationale for the choice of component failure rate clear and reasonable for the intended application and environment? * For each component, is the failure mode distribution / allocation reasonable? * For each component, is the classification (safe, dangerous, etc) reasonable considering the stated element safety function? * For each component, is the diagnostic coverage (if applicable) reasonable? * Does the analysis conclude the type (A or B) of the element (or support it, if stated elsewhere in the design documentation)? * Does the analysis estimate at least the discrete failure mode data required to enable architectural constraints for the element/subsystem and the system level calculations to be established (i.e., as a minimum, λD, DC and SFF) * Are any assumptions or dependencies on external factors clearly stated and carried forward to the safety manual if relevant? | 2/7.4.5,  2/7.4.9.4 (a), 2/7.4.9.4 (c),  2/7.4.9.4 (h),  2/7.4.9.4 (j),  2/7.4.9.4 (l),  2/7.4.9.5,  2/7.4.5 for PFD context,  2/Annex A,  2/Annex C,  7/B.6.6.1. |  |  |
| 8 | Lifetime limits | To ensure the element / subsystem approach and design has considered and documented any relevant lifetime limitations. | 2/7.4.9.4 (f). |  |  |
| 9 | Additional requirements for data communications | To ensure that communications systems and approaches used for safety-related aspects of the element / subsystem are dependable and suitable for the SIL. | 2/7.4.11. |  |  |
| 10 | Requirements for system behaviour on detection of a fault | To ensure, dependent upon the HFT and other factors, that a relevant action is triggered upon detection of a dangerous fault. | 2/7.4.8. |  |  |
| 11 | Independence between functions | To ensure that, where required, there is sufficient independence between safety functions and between safety functions and non-safety functions. | 2/7.4.2.3 –  2/7.4.2.5. |  |  |
| 12 | Hardware fault tolerance | To ensure the element / subsystem approach and design has considered and documented the HFT. | 2/7.4.9.4 (m). |  |  |
| 13 | Highest SIL (architecture) | To ensure the element / subsystem approach and design has considered and documented the route to compliance and the highest achievable SIL as restricted by the architecture. | 2/7.4.9.4 (j),  2/7.4.9.4 (k),  for Type A/B,  2/7.4.4. |  |  |
| 14 | Diagnostic test interval | To ensure the diagnostic test interval is suitable to support credit taken for any diagnostics. | 2/7.4.9.4 (i),  2/Annex C. |  |  |
| 15 | Environmental limits (incl. de-rating) | To ensure the element / subsystem approach and design has considered and documented all relevant environmental limitations including relevant de-rating. | 2/7.4.9.4 (e),  2/7.4.2.13. |  |  |
| 16 | Proof test requirements | To ensure the element / subsystem approach and design has considered and documented the proof test requirements. | 2/7.4.9.4 (g),  Annex D. |  |  |
| 17 | Maintenance requirements | To ensure the element / subsystem approach and design has considered and documented the maintenance requirements. | 2/7.4.9.4 (g),  Annex D. |  |  |
| 18 | Other repair constraints | To ensure any additional repair information is available to support derivation of the MRT. | 2/7.4.9.4 (k). |  |  |
| 19 | Systematic capability – general approach | To ensure, when relevant, that a selection of techniques & measures for the avoidance and control of systematic faults have been used that support the claimed systematic capability (SC).  NOTE: This is a general TOE to record the overall approach and associated evidence. The SC will depend on a satisfactory approach to all wider aspects that could affect systematic integrity, e.g., FSM, a structured realisation lifecycle, and detailed aspects in the related TOEs below. | 2/7.4.2.2 (c),  2/7.4.6,  2/7.4.7. |  |  |
| 20 | Systematic capability – fault avoidance measures | To ensure the techniques & measures for the avoidance of systematic faults have followed a planned methodical approach resulting in supporting evidence for influence on design and implementation of outputs. | 2/7.4.9.4 (l),  2/7.4.6.1,  3/7.4,  2/Annex B, 2/Tables B.1 – B.5. |  |  |
| 21 | Systematic capability - fault control measures | To ensure the techniques & measures for the control of systematic faults have followed a planned methodical approach resulting in supporting evidence for influence on design and implementation of outputs. | 2/7.4.9.4 (m),  2/7.4.7.1 – 7.4.7.3,  2/7.4.11,  2/Annex A.3,  2/Tables A.15 – A.18,  3/7.4.3 (no change). |  |  |
| 22 | Evidence of similar conditions in previous use (Proven-in-Use) | To ensure that when the element is regarded as proven-in-use there is evidence of a clearly restricted and specified functionality supported by evidence for a sufficiently low likelihood of dangerous systemic faults (based on analysis of operational experience of a specific configuration with suitable analysis and testing).  NOTE: If this TOE is relevant, evidence for meeting each referenced subclause under 7.4.10 should be assessed separately in detail. | 2/7.4.10.1 –  2/7.4.10.6. |  |  |
| 23 | Verification and validation records | To ensure the element / subsystem has been verified as planned (see TOE 5), including the overall validation, and that reasonable and detailed results exist.  To also ensure the element / subsystem has been validated as planned (see TOE 5) and that reasonable and detailed results exist. | 2/7.4.9.3 (e),  2/7.7,  2/7.9.2.5 –  2/7.9.2.10,  3/7.7. |  |  |
| 24 | Systematic failure constraints | To ensure any instructions or constraints relating to the application of the element / subsystem relevant to prevent systematic failures are detailed in the safety manual. | 2/7.4.9.3 (b). |  |  |
| 25 | Safety manual | To ensure that all compliant items (elements or subsystems that claim compliance with IEC 61508) are well documented and supported by a safety manual. | 2/5,  2/7.4.9.6,  2/7.4.9.7,  2/Annex D. |  |  |
| 26 | Functional safety assessment | To ensure a FSA is planned, carried out and documented for all applicable aspects of the element / subsystem realisation. | 2/8,  1/8. |  |  |