# Introduction

This conformity assessment template is for the assessment of Operation and Maintenance of a Safety Instrumented System (SIS) to IEC 61511:2016+AMD1:2017, *Functional safety – Safety instrumented systems for the process industry sector.*

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* on using the CASS Methodology 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 61511:2016+AMD1:2017), 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 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 conformity assessment template is for the generic SIS operation and maintenance aspects from IEC 61511-1 clause 16.
2. For the assessment of the generic FSM and lifecycle aspects from IEC 61511-1, refer to template CASS-511-FSM – FSM Assessment.
3. For the Functional Safety Assessments (FSA) stages 1 – 5, this includes all clauses from 8 to 18, refer to template CASS-511-FSA – Functional Safety Assessment (FSA).
4. For the assessment of the generic LVL aspects from IEC 61511-1 clauses 7, 10, 11, 12, 13 and 15, refer to template CASS-511-LVL – Subsystem LVL Software.

# References

* CASS-511-FSM – FSM Assessment
* CASS-511-FSA – Functional Safety Assessment
* CASS-511-LVL – Subsystem LVL Software

# Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
| CASS | Conformity assessment of safety-related systems |
| FSA | Functional safety assessment |
| FSM  MAINT | Functional safety management  Maintenance |
| LVL | Limited Variability Language |
| O&M  OPS | Operation and maintenance  Operations |
| SIF | Safety instrumented function |
| SIS | Safety instrumented system |
| TOE | Target of evaluation |

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of change |
| V1 | 09/05/2024 | First issue |
|  |  |  |
|  |  |  |
|  |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61511 references** | **Supporting documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| 0 | IEC 61511 conformance | To ensure the overall approach is in conformance with the IEC 61511 standard.  For operators of a SIS, the requirements of IEC 61511 Functional Safety Management (CASS-511-FSM) and Functional Safety Assessment (CASS-511-FSA Stage 4) are also applicable. | 1/5.2 |  |  |
| **Operation and Maintenance Planning** | | | | | | |
| 1 | **Planning** - Routine and Abnormal operational activities | To plan for routine and abnormal operation of the Safety Instrumented system, this will also include the procedures, measures and techniques to use during operation and maintenance. (1/16.2.1)    The activities carried out as a result of 1/16.2.1 shall be implemented and progress monitored. | 1/16.2.1 |  |  |
| 2 | **Planning -** Proof Testing | To plan for proof testing of the Safety Instrumented System(1/16.2.1)    The activities carried out as a result of 1/16.2.1 shall be implemented and progress monitored. | 1/16.2.1 |  |  |
| 3 | **Planning –** Operational Response to faults | To plan for operational requirements and actions in the event of a fault or failure being identified.  The activities carried out as a result of 1/16.2.1 shall be implemented and progress monitored. | 1/16.2.1 |  | *New to IEC 61511 Edition 2* |
| 4 | **Planning -** Verification activities | To plan the verification activities necessary in order to ensure adherence to the operational and maintenance procedures.  The activities carried out as a result of 1/16.2.1 shall be implemented and progress monitored. | 1/16.2.1 |  |  |
| 5 | **Planning –** Schedule of Proof Testing | To schedule the proof testing of SIFs necessary in order to ensure adherence to the Safety Requirement Specification.  The activities carried out as a result of 1/16.2.1 shall be implemented and progress monitored. | 1/16.2.1 & 16.3.1.3 |  |  |
| 6 | **Planning -** Operation and maintenance scheduling | To schedule for the operational and maintenance requirements of the SIS. | 1/16.2.1 |  |  |
| 7 | **Planning -** Responsible Person(s) / Department(s) | To identify who is responsible for maintaining the SIS. | 1/16.2.1 |  |  |
| 8 | **Planning –** SIS Spare Parts | To identify and make available the required parts to minimise the by-pass or unavailability duration of the SIS. | 1/16.2.12 |  | *New to IEC 61511 Edition 2* |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61511 references** | **Supporting documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| **Operation and Maintenance Procedures** | | | | | | |
| 9 | **Procedures –** Maintain the SIS in an *‘as designed’* condition. | To demonstrate that all routine procedures necessary to maintain the SIS in the ‘as designed’ condition are clearly defined.  This can include:   * Proof Test Procedures, * Calibration of Equipment which forms part of the SIS, * Replacement of perishable components, * Routine Inspections. | 1/16.2.2 & 16.3.1.4 |  |  |
| 10 | **Procedures –** Quality and consistency of proof tests. | To demonstrate that all proof tests are being carried out in a consistent manner. | 1/16.2.2 |  |  |
| 11 | **Procedures –** Validation after replacement of any device. | To demonstrate that validation is being carried out in a consistent manner following the replacement of a device which forms part of the SIS. | 1/16.2.2 |  |  |
| 12 | **Procedures –** Minimise the unwanted hazardous event from occurring during maintenance/SIS is unavailable. | To ensure ongoing safe operation when the SIS is not available due to maintenance or unavailability. | 1/16.2.2 |  |  |
| 13 | **Procedures –** To test the diagnostic part of the SIS. | To ensure the diagnostic part of the SIS is tested against well-defined procedures using proven methods. | 1/16.2.2 |  |  |
| 14 | **Procedures –** Fault diagnosis and Repair of the Safety Instrumented System. | To ensure that fault diagnosis and repair tasks are being carried out against a defined procedure. | 1/16.2.2 |  |  |
| 15 | **Procedures –** Identification and correct use of calibrated test equipment. | To ensure the correct test equipment is being used on a system against a defined procedure. | 1/16.2.2 |  |  |
| 16 | **Procedures** - Proof Test Procedures | To ensure clear evidence of sufficient step by step Proof Test Procedure, for all SIFs, to reveal all dangerous undetected failures across the entire SIS.  The procedures will also describe   * The correct operation of the Sensor & FEs * Correct Logic action * Correct alarms and indications | 1/16.2.11, 16.3.1.1 & 16.3.1.2 |  |  |
| 17 | **Procedure** - Application Software update | To ensure that where a change has occurred to the application software the system has gone through a revalidation and proof test. | 1/16.3.1.6 |  |  |
| 18 | **Procedure** – Deferral of Proof Test | To ensure procedures exist on the deferral of proof test so as not to cause significant delays.  See TOE 12 for further information on safe operation in the event of a significant delay in proof testing. | 1/16.3.1.7 |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61511 references** | **Supporting documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| **By-Pass Procedures** | | | | | | |
| 19 | **Procedures –** Compensating measures with operational limits due to disabled or degraded SIS | To define what is required for continued safe operation whilst the safety system is unavailable or in by-pass mode. | 1/16.2.3 |  | *New to IEC 61511 Edition 2* |
| 20 | **Procedures –** Applying and removing of a by-pass | To define the correct manner in which a by-pass should be applied and then subsequently removed. | 1/16.2.3 |  | *New to IEC 61511 Edition 2* |
| 21 | **Procedures –** Maximum length of time a by-pass can be in place for. | To define the maximum allowable time limit a by-pass can be in operation for. | 1/16.2.3 |  | *New to IEC 61511 Edition 2* |
| 22 | **Procedures –** Performing a Hazard analysis to determine compensating measures provide adequate risk reduction. | To ensure the other means of risk reduction against the defined unwanted hazardous scenario are adequate whilst the safety system is unavailable. | 1/16.2.4 |  | *New to IEC 61511 Edition 2* |
| **By-Pass Log** | | | | | | |
| 23 | Log – Status of all by-passes. | To ensure the correct status of all by-passes is maintained. | 1/16.2.7 |  | *New to IEC 61511 Edition 2* |
| 24 | Log – Authorisation of all by-passes. | To ensure the application of a by-pass has been satisfactorily authorised and indicated as such | 1/16.2.7 |  | *New to IEC 61511 Edition 2* |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61511 references** | **Supporting documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| **Operation and Maintenance Training** | | | | | | |
| 25 | **Training –** Operational crews. | To demonstrate that all staff involved in the operation of a Safety Instrumented System has been provided with sufficient training.  The evidence shall demonstrate that the persons(s) or department(s) involved:   * Understand how the SIS functions; * The Hazard being protected against; * Operation of any by-passes and when to use them; * Operation of all manual shutdowns, overrides, start-ups, and when to use them; *and* * Action to take in the event of a Diagnostic alarm. | 1/16.2.6 |  |  |
| 26 | **Training –** Maintenance crews. | To demonstrate that all staff involved in the maintenance of a Safety Instrumented System has been provided with sufficient training to full fill their role. | 1/16.2.8 |  |  |
| **Monitoring of SIS** | | | | | | |
| 27 | **Analyse** – Discrepancies between expected and actual demand rate of the SIF. | To analyse the demand rates for the SIFs and ensure ongoing relevance of the basis of design. | 1/16.2.9 |  | *New to IEC 61511 Edition 2* |
| 28 | **Analyse** – Expected and actual actions following a demand on the system. | To ensure the correct action is being taken upon a demand being placed on the system. | 1/16.2.9 |  | *New to IEC 61511 Edition 2* |
| 29 | **Analyse** – Failure modes of equipment forming part of the system. | To identify the failure modes that equipment in the system is being subjected too. | 1/16.2.9 |  |  |
| 30 | **Analyse** – Expected and actual cause and frequency of spurious trips on the system. | To analyse the spurious trip rate for the SIFs and ensure ongoing relevance of the basis of design. | 1/16.2.9 |  |  |
| 31 | **Analyse** – Failure of equipment forming part of the compensating measures. | To ensure all other means of risk reduction are being maintained and are still relevant against the unwanted hazardous scenario. | 1/16.2.9 |  | *New to IEC 61511 Edition 2* |
| 32 | **Analyse** – Test frequency for the system. | To ensure that the test frequency for the system remains justified.  Data such as Plant Experience, Historical Data & H/W degradation can be used.  See TOE 37 for more information | 1/16.3.1.5 |  | *New to IEC 61511 Edition 2* |
| 33 | **Analyse** – Discrepancies between expected and actual demand rate of the SIF. | To analyse the demand rates for the SIFs and ensure ongoing relevance of the basis of design. | 1/16.2.9 |  | *New to IEC 61511 Edition 2* |
| **Audit and Revision** | | | | | | |
| 34 | **Review** - Operational and maintenance procedures. | To provide clear evidence that procedures are revised following   * An audit; * Test of a SIS;   Experience from Normal or Abnormal events. | 1/16.2.10 |  |  |
| 35 | **Review** - Hazard and Risk analysis | To provide evidence associated with the design to ensure assumptions made during earlier analysis are still valid. | 1/16.2.13 |  | *New to IEC 61511 Edition 2* |
| **Inspection** | | | | | | |
| 36 | **Inspection –** Periodic Inspection of the SIS | To ensure no unauthorised modifications have been carried out and to also ensure there are no observable deteriorations to the system. | 1/16.3.2 |  |  |
| **Records** | | | | | | |
| 37 | **Record –** Data on demand rates for SIS. | To provide evidence that information on demand is being retained for the SIS so that reliability parameters for the SIS can be re-evaluated. | 1/16.2.2 |  | *New to IEC 61511 Edition 2* |
| 38 | **Record –** Audits and Tests of the SIS. | To show evidence that all audits and tests performed on the safety system are being collected. | 1/16.2.2 |  |  |
| 39 | **Record –** Test/Inspection carried out | To show evidence of what Test / Inspection has been carried out | 1/16.3.3 |  |  |
| 40 | **Record –** Dates and Times of Test/Inspection | To show evidence of when the Test / Inspection was carried out. | 1/16.3.3 |  |  |
| 41 | **Record –** Name of person(s) who performed the Test/Inspection | To show evidence of who performed the Test / Inspection that was carried out. | 1/16.3.3 |  |  |
| 42 | **Record –** Serial Number of the system tested. | To show evidence of which system(s) was Tested / Inspected. | 1/16.3.3 |  |  |
| 43 | **Record –** Results from test / inspection | To show evidence of the results from performing a Test / Inspection including the as found and as left conditions. | 1/16.3.3 |  |  |