# Introduction

This conformity assessment template is for the assessment of Functional Safety Management (FSM) 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 FSM and safety lifecycle aspects from IEC 61511-1 (now combined as of v2).
2. This conformity assessment template shall be used to develop plans and procedures prior to the execution of any SIS project.
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 SIS operation and maintenance aspects from IEC 61511-1 clause 16, refer to template CASS-511-OP – Operations and Maintenance.

# References

* CASS-511-FSA – Functional Safety Assessment (FSA)
* CASS-511-LVL – Subsystem LVL Software
* CASS-511-OP – Operations and Maintenance

# Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
| BPCS | Basic process control system |
| CASS | Conformity assessment of safety-related systems |
| CM | Configuration management |
| FSA | Functional safety assessment |
| FSM | Functional safety management |
| H&RA | Hazard & risk analysis |
| LVL | Limited Variability Language |
| QMS | Quality management system |
| SIF | Safety instrumented function |
| SIL | Safety integrity level |
| SIS | Safety instrumented system |
| SLC | Safety lifecycle |
| SRS | Safety requirements specification |
| TOE | Target of evaluation |

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of change |
| V1 | Feb-2018 | First issue |
| V2 | 09/05/2024 | Updated and merged with SLC TOEs onto the new template |
| V2.1 | 30/06/2025 | Missing TOE 5 added back in (from old lifecycle template) |
|  |  |  |

| **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. |  |  |
| 1 | Functional safety management (overall) | This is provided as an overall objective, to ensure there is an overall framework with a deliberate and strategic approach to FSM that is appropriate for the business scope and relevant SIS life-cycle phases. The details of the FSM procedures are then examined in the TOEs that follow below. | 1/5.1. | As listed below in this column against each TOE | Overall comments may be provided here (e.g., regarding lifecycle scope, how the FSM has been integrated with the QMS, etc); the TOEs that follow below are used to assess how the actual requirements are met. |
| 2 | Functional safety policy | To ensure there is an appropriate policy and strategy for achieving functional safety, together with the means of evaluating its achievement, authorised by senior management and communicated within the organisation. | 1/5.2.1. |  |  |
| 3 | Organisation and responsibilities | To ensure that the persons, departments or organisations who perform, review, audit or assess SIS safety lifecycle activities are identified (documented) and informed of the responsibilities assigned to them. | 1/5.2.2.1. |  |  |
| 4 | Management of competence | To ensure there are procedures to demonstrate, document and manage the competence of persons, departments or organisations who are assigned to perform, review, audit or assess SIS safety lifecycle activities.  Procedures to manage and periodically assess competence should consider all the points in clause 5.2.2.2 (knowledge, training, experience, process, technology, safety, field devices, event consequences, SIL, novelty, complexity, legal, regulatory, management and leadership, as appropriate to the role). Competence should be re-assessed in the event of changes to an assigned role. | 1/5.2.2.2,  1/5.2.2.3. |  |  |
| 5 | Information and documentation (general) | To confirm that documentation produced as part of SIS safety lifecycle activities/phases is fit for purpose, available to those involved in the SIS safety lifecycle and contains all relevant descriptions of the SIS design, installation, operation, maintenance and testing. Each document should be accurate, understandable, accessible, maintainable (i.e. editable) and traceable to the SRS and H&RA. | 19.2.1  19.2.2  19.2.3  19.2.5 |  |  |
| 6 | Document identification and revision control | To ensure each document will be appropriately designated for its type, is uniquely identifiable, contains a revision index, is searchable and stored so as to allow location of the latest revision and is revised, reviewed, approved and under appropriate revision control. | 1/19.2.4,  1/19.2.6,  1/19.2.7,  1/19.2.8. |  |  |
| 7 | Documentation scope and contents | To ensure the documentation will cover:   1. Results of the H&RA and the related assumptions 2. Equipment that forms the SIS with related safety requirements 3. Organisation responsible for maintaining functional safety 4. Procedures necessary to achieve and maintain functional safety of the SIS 5. Revisions from any modifications 6. Relevant safety manual(s) 7. Design, implementation, test and validation | 1/19.2.9. |  |  |
| 8 | Risk evaluation and management | To ensure that hazards are identified, their risks evaluated, and the necessary risk reduction determined following recognised standards and techniques in accordance with Clause 8. | 1/5.2.3,  1/8.2. |  |  |
| 9 | SIS safety lifecycle definition | To ensure the approach to the phases and activities of the SIS safety lifecycle are structured and defined in a manner that corresponds to Figure 7 and Table 2 of 61511-1 for the scope of the project and that it defines the inputs, outputs and verification to a sufficient level of detail to allow completion of each phase/activity. | 1/6.2.1,  1/6.2.2. |  |  |
| 10 | Overall Safety planning | To ensure that appropriate safety plans exist, to a level of detail appropriate to the role that the individual or organisation is performing in the SIS safety lifecycle (including review, audit and assessment).  The overall safety plan may be a separate document, a section in the quality plan or several documents which may include company procedures. | 1/5.2.4. |  |  |
| 11 | SIS safety plan | To confirm the SIS safety plan/planning defines the activities, criteria, techniques, measures, procedures and responsible organisations/people to ensure:   1. SIS safety requirements are achieved for all modes of the process 2. proper installation and commissioning of the SIS 3. safety integrity of the SIF after installation 4. safety integrity during operation 5. process hazards are addressed during SIS maintenance | 1/6.2.3. |  |  |
| 12 | Verification planning (general) | To ensure verification is planned in a sufficient level of detail to describe:   1. the verification activities 2. the procedures, measures and techniques to be used 3. when verification will take place 4. the persons, departments and organizations responsible, including levels of independence 5. how to manage and implement actions, recommendations and non-conformances identified by verification 6. identification of items to be verified 7. identification of the information against which the verification is carried out 8. the adequacy of the outputs against the requirements for that phase 9. correctness of the data 10. tools and supporting analysis 11. the completeness of the SIS implementation and the traceability of the requirements 12. the readability and audit-ability of the documentation 13. the testability of the design 14. the tests that demonstrate non-safety functionality does not interfere with safety-functions | 1/7.2.1,  1/7.2.3. |  |  |
| 13 | SIS application program lifecycle | To ensure the SIS application program lifecycle is structured and defined in a manner that corresponds to Figure 8 and Table 3 of 61511-1 for the scope of the project and that it defines the inputs, outputs and verification to a sufficient level of detail to allow completion of each phase/activity. | 1/6.3.1,  1/6.3.3. |  | *See CASS-511-LVL for detail* |
| 14 | Application programming methods | To ensure the appropriate methods, techniques and tools have been planned for development of the SIS application program to meet clause 12.6.2. | 1/6.3.2. |  | *See CASS-511-LVL for detail* |
| 15 | Verification planning (testing) | To ensure that when testing is specified, verification planning covers:   1. the strategy for integration of application program and hardware and field devices, including the integration of sub-systems that shall comply with other standards 2. test set-up and type of test to be performed including the hardware, application programming, and programming of devices 3. test cases and test data 4. the test environment, tools, hardware, software and required configuration 5. test criteria on which the results of the test will be evaluated 6. procedures for corrective action on failure during test or non-conformances 7. physical location(s) (e.g., factory or site) 8. dependence on external functionality 9. personnel 10. management of change | 1/7.2.2. |  |  |
| 16 | Implementing the verification plan | To ensure the verification activities will be performed in accordance with the verification plan for each phase/activity specified in the SIS safety lifecycle planning.  To ensure the verification results will be made available and the objectives and criteria have been met (See also TOEs 5-7). | 1/7.2.4,  1/7.2.6. |  |  |
| 17 | Suppliers of products or services | To ensure FSM and quality management systems (QMS) are in place for:   * Organisations that have overall responsibility for a lifecycle phase * Suppliers of products or services on which functional safety depends   The FSM shall conform to:   * IEC 61508-1:2010, Clause 6 or, * the equivalent FSM requirements of a relevant IEC 61508 derived standard (such as IEC 61511-1:2016 Clause 5)   Suppliers of products and services on which functional safety does not depend need only demonstrate they have an appropriate QMS in place. | 1/5.2.5.2. |  |  |
| 18 | SIS performance analysis | To ensure there are procedures in place to evaluate the SIS against its safety requirements, identify and prevent dangerous systematic failures, and to monitor and assess reliability parameters and demand mode assumptions of the SIS that were made during the risk assessment and design stages. | 1/5.2.5.3. |  |  |
| 19 | Legacy systems (and those not installed to IEC 61511) | To demonstrate that for installed SIS not designed and constructed in accordance with IEC 61511, the user must determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner. | 1/5.2.5.4. |  |  |
| 20 | Functional safety assessment (FSA) | To ensure the organisation has procedures to specify or deal with FSA at defined stages throughout the SIS safety lifecycle so that a judgment can be made on the functional safety and the safety integrity achieved by every SIF. The procedure(s) should ensure that the assessment team has the necessary competence (in the relevant aspects being assessed), authority, independence, access (to information and persons) and that the FSA has been planned in accordance with clause 5.2.6.1.3, including status and outcomes of previous FSAs.  Specific FSA requirements apply (see clause 5.2.6.1.5) prior to hazards being present and periodically throughout operations and maintenance (5.2.6.1.10). FSA applies to the evaluation of FSA tools and to the SIS Modification phase (clause 17) (see Note 4 above this table). The results of FSA are required to be documented and made available. | 1/5.2.6.1.1 to 1/5.2.6.1.10. |  | See CASS-511-FSA for detail. |
| 21 | Functional safety audit | To ensure procedures exist for periodic and independent audits of the FSM system to monitor its effectiveness and facilitate its improvement. The procedures should define the frequency of the audits, degree of independence, recording and follow-up. | 1/ 5.2.6.2.1 to 1/5.2.6.2.3. |  |  |
| 22 | Corrective action (Implementation and Monitoring) | To ensure there are procedures for prompt follow-up and satisfactory resolution of recommendations arising from hazard analysis, risk assessment, assurance activities, verification and validation, FSAs, audits, post-incident and post-accident activities. | 1/5.2.5.1. |  |  |
| 23 | Management of Change procedures | To ensure management of change procedures are in place to initiate, document, review, implement and approve changes to the SIS, including changes that affect SIS requirements (such as changes to the BPCS or hazard scenario initiating events).  Modifications to installed SIS or resulting from testing shall be controlled by appropriate procedures for identifying, requesting, analysing the impact of, authorising, controlling and re-verifying modifications.  Modification activity shall not begin until a Functional Safety Assessment is carried out on the impact analysis and the authorisation of the modification.  Modification shall be performed by properly qualified and trained personnel. Those affected by the change will also receive notification and training in relation to the change.  In the event of a SIS modification (SIS lifecycle phase 7), the work should be subject to a detailed FSA against all the requirements of clause 17. | 1/5.2.6.1.9,  1/5.2.6.2.4,  1/5.2.6.2.5,  1/7.2.5,  1/17.2.1 to 1/17.2.8. |  |  |
| 24 | Changes to previous lifecycle phases | To confirm that any required changes that affect a previous lifecycle phase are re-examined, altered as required and re-verified. This applies to changes identified anywhere from hazard and risk assessment to O&M, e.g., as a result of document review, design, test, implementation, etc. If the change is to a SIS already in the O&M phase, then the lifecycle phase ‘SIS modification’ applies and will require a detailed assessment against each requirement in clause 17. | 1/6.2.4. |  |  |
| 25 | Configuration management | To ensure procedures exist for configuration management (CM) of the SIS during any SIS safety lifecycle phase, including when formal CM is introduced, how each component and the application program is uniquely identified, and how unauthorised devices are prevented from entering service.  CM should include the SIS software, hardware and tools used to develop and execute the application program which should all be under revision control. | 1/5.2.7.1,  1/5.2.7.2. |  |  |