# Introduction

This conformity assessment template is for the assessment of Limited Variability Language (LVL) software to IEC 61511:2017, *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 61511:2017), 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 software LVL aspects from IEC 61511-1.
2. For the Functional Safety Management (FSM) and safety lifecycle aspects, see CASS-511-FSM – Functional Safety Management (FSM).
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-FSM – Functional Safety Management (FSM)
* CASS-511-FSA – Functional Safety Assessment (FSA)
* CASS-511-OP – Operation and Maintenance

# Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
| AP | Application Program |
| CASS | Conformity assessment of safety-related systems |
| COTS | Commercially off the shelf |
| FS | Functional safety |
| FSA | Functional safety assessment |
| FSM | Functional safety management |
| LVL | Limited Variability Language |
| PE | Programmable electronic |
| SIF | Safety instrumented function |
| SIL | Safety integrity level |
| SIS | Safety instrumented system |
| SRS | Safety requirements specification |
| TOE | Target of evaluation |
| V&V | Verification & validation |

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of change |
| V1 | 19/06/2024 | First issue |
|  |  |  |
|  |  |  |
|  |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE** | **IEC 61511 references** | **Supporting documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| 1 | Functional safety management (overall) | To ensure the overall FSM approach is in conformance with the IEC 61511 series of standards as relevant for the software.  For all SILs, ensure there is general evidence for conformance with the FSM aspects of IEC 61511-1 in relation to the software. | 5.2.1,  5.2.2.1,  5.2.2.2. |  | Delete before use: *This TOE is intended to provide a general status on conformance for the FSM aspects related to software.* |
| 2 | AP competence | To ensure that competence management has been applied for the software lifecycle and software development.  For all SILs, ensure there is general evidence of competence management covering the software lifecycle and software development. This includes competence specific to the AP platform / software and those performing AP reviews. | 5.2.2.3. |  | Delete before use: *This TOE is intended to consider only the software aspects of competence.* |
| 3 | AP safety planning | To ensure the overall safety planning approach has considered the relevant software aspects.  For all SILs, ensure there is general evidence of safety planning for the software lifecycle and development. | 5.2.4. |  | Delete before use: *This TOE is intended to consider only the planning related to the software.* |
| 4 | AP configuration management | To ensure the software and associated tools are under configuration management and revision control.  For all SILs, ensure there is evidence of software and tool configuration management and software revision control. This evidence includes aspects for the backup and restoration of software and parameters.  NOTE: This includes software or configurations for sensors and final elements. | 5.2.7.1,  5.2.7.2,  12.2.8. |  |  |
| 5 | AP modification procedures | To ensure that the AP is subject to written modification procedures for controlling and authorizing changes.  For all SILs, ensure there are written modification procedures, a method for identifying / requesting changes, evidence for impact analysis and relevant authorisation before changes. | 12.2.8,  17.2.1,  17.2.3,  17.2.8. |  |  |
| 6 | AP backup and restoration procedures | To ensure that the AP is subject to written backup and restoration procedures.  For all SILs, ensure there are written backup / restoration procedures for the specific AP and system. | 12.2.8. |  |  |
| 7 | AP safety lifecycle | To ensure the AP development fits with the overall safety lifecycle and that a specific AP safety lifecycle is defined and used.  For all SILs, ensure the AP safety lifecycle has each phase defined in terms of its elementary activities, objectives, required input information, output results and verification requirements. A simple V-model like that defined in IEC 62061:2021 is useful. | 6.2.1,  6.3.1. |  |  |
| 8 | AP verification planning | To ensure that the verification of the AP is planned.  For all SILs, ensure that the verification of the AP (using reviews, analysis, simulation and tests) was planned with written procedures / specifications. | 7.2.1,  12.5.1. |  |  |
| 9 | AP safety requirements | To ensure the safety requirements are sufficient to design the SIS application program and consider the traceability required from the AP.  For all SILs, ensure the application program requirements are derived from the SIS SRS and include:   * individual SIF requirements (including voting), * any additional known requirements (e.g., due to architecture, safety manual limitations / constraints, due to hardware, due to embedded software, due to security). * any requirements rooted in safety planning. | 10.3.3,  10.3.4,  10.3.5,  10.3.6,  11.5. |  |  |
| 10 | AP and diagnostics | To ensure that the AP, possibly supported by its platform / subsystem, provides sufficient diagnostics for the SIS and SIL via monitoring of internal functions (e.g., watchdogs, data validation) or external devices (e.g., sensors and final elements).  For all SILs, ensure that, if relevant, the built-in monitoring and diagnostics of the AP platform / subsystem are supplemented by designed monitoring and diagnostics to support the achievement of the SIL.  NOTE: The AP safety requirements and AP design combined should define the overall monitoring and diagnostics strategy. | 10.3.5,  12.3.4. |  |  |
| 11 | AP subsystem selection | To ensure the general approach for application program development is appropriate and planned.  For all SILs, ensure that the COTS subsystem / platform for the application program is suitable for the application and conforms with IEC 61508 and / or IEC 61511, as relevant.  NOTE: The COTS subsystem / platform should come with a defined “coding standard” (limitations). If not, a coding standard (rules) will need to be defined. | 12.1,  12.2.1 – 12.2.7. |  |  |
| 12 | AP tool assessment | To ensure any tool(s) used for the software lifecycle or software development is suitable for its assigned task and does not have a negative impact on the SIS. Alternatively, to ensure the tool(s) output was confirmed by verification procedures.  For all SILs, ensure there is a relevant positive tool(s) assessment or specific tool(s) output verification. | 5.2.6.1.6 |  |  |
| 13 | AP combining SIFs | To ensure when a single AP covers various SILs (including non-SIL) the approach is suitable for all SILs (cannot negatively impacted any SIF).  For all SILs, ensure that the AP meets the highest overall SIL, has sufficient independence between SIFs, and any SIF cannot negatively impact another SIF. | 11.2.2,  11.2.3. |  |  |
| 14 | AP security and access control | To ensure that the overall SIS security risk assessment has been used to influence the AP.  For all SILs, ensure that the AP design and coding has considered the relevant security risk and access control requirements. | 8.2.4,  11.7.3.2,  11.7.3.4,  12.4.2. |  |  |
| 15 | AP safety validation planning | To ensure that the AP is part of the overall validation planning including specific AP aspects.  For all SILs, ensure that the AP validation plan covers all the functions, the technical strategy, the procedures to be used, the validation environment and the pass / fail criteria. | 15.2.1,  15.2.2, 15.2.5,  15.2.6. |  |  |
| 16 | AP design | To ensure application program design addresses all SIS logic including all process operating modes for each SIF including decomposition into modules if applicable.  For all SILs, ensure that a documented application program design, derived from and traceable to the SRS and application program safety requirements, covers all logic, each SIF and each operating mode.  To also ensure that the application program design demonstrates:   * completeness with respect to the SRS, * correctness with respect to the SRS, * freedom from ambiguity, and * freedom from design faults. | 12.3. |  |  |
| 17 | AP communications | To ensure that the communications approach for the AP subsystem / platform is suitable for the application and SIL(s).  For all SILs, ensure the communication / interface requirements are defined, the communication uses relevant safety techniques, and relevant failure modes have been considered.  NOTE: If the communications PFH / PFD is excluded from the SIF PFH / PFD calculation, check that this is sufficiently insignificant to do so.  NOTE: This TOE may need to consider security aspects for the communication link. | 10.3.5,  11.2.14,  11.7.4,  12.4.2. |  |  |
| 18 | AP implementation | To ensure that the application program development supports the required safety integrity and is derived from the AP safety requirement specification.  For all SILs, ensure that the application program development methodology complies with the development tools and restrictions of the SIS PE subsystem, is produced in a structured manner (e.g., modularity), justifies the use of previously developed libraries, and details clear ownership / identification. To also ensure AP implementation is traceable to the AP safety requirements. | 12.4,  12.3.4. |  |  |
| 19 | AP methodology and tools | To ensure that the AP development complies with the constraints of the supplier’s safety manual and that a methodology has been defined to reduce / prevent systematic errors.  For all SILs, ensure that there is evidence for compliance with the AP platforms safety manual. Also ensure that there is evidence of defined techniques and measures focussed on systematic failures. | 12.6. |  |  |
| 20 | AP verification and testing | To ensure that the application program is appropriately verified.  For all SILs, ensure that the application program and any decomposition into modules is verified by a combination of analysis, simulation, testing (using written procedures and test specifications). The verification must also ensure that the coding standard has been followed and complied with. To also ensure that the scope of the testing is appropriate for the application. | 12.5.3,  12.5.4,  7.2.2. |  |  |
| 21 | AP review | To ensure that the application program is reviewed by a competent person not involved in the development.  For all SILs, ensure that application program review(s) were structured, undertaken and documented. To also ensure that any review(s) was undertaken by a competent person. | 12.5.2 |  |  |
| 22 | AP subsystem compliance | To ensure that the AP platform is configured and used as per the manufacturer’s requirements and recommendations (e.g., as per any certificate and its safety manual).  For all SILs, ensure that AP program review specifically considers the requirements and recommendations from the AP platforms safety manual. | 12.4.1 |  |  |
| 23 | SIS integration test | To ensure the AP has been successfully integrated onto the target platform / subsystem including interaction with a sample set of field devices and or simulator.  For all SILs, ensure the AP integration is performed, based on the initial integration test requirements, with documented test results. | 13 |  |  |
| 24 | AP modification V&V | To ensure that any modifications have been correctly requested, authorised, planned, and delivered including relevant verification or validation.  For all SILs, ensure the modification procedures (incl. impact analysis) have been followed regardless of the lifecycle phase e.g., modification during testing, modification during operation. | 12.5.5,  16.3.1.6,  17.2.4,  17.2.6,  17.2.8. |  |  |
| 25 | AP validation considerations | To ensure that the AP is a key part of the overall SIS validation and that AP competent persons take part in the SIS validation.  For all SILs, ensure that AP is portion of the validation is carried out as planned and carried out by at least one AP competent person. | 15.2.2. |  |  |
| 26 | AP FS audit | To ensure that software lifecycle and software development activities are subject to FS audit(s).  For all SILs, ensure that relevant aspects of the software lifecycle and software development have been audited in relation to functional safety. | 5.6.2.1,  5.6.2.2,  5.6.2.3. |  |  |
| 27 | AP documentation | To ensure that all AP documents are available and that they have been validated for accuracy, consistency, and traceability of the SIF.  For all SILs, ensure that all the relevant documents are available and have been validated for accuracy, consistency and traceability of the SIF (from the overall design through the AP), including:   * AP safety requirements specification. * AP platform / subsystem safety manual. * AP verification and validation plans. * AP design information (system and AP). * AP coding standard / programming procedures. * AP libraries / pre-used functions list. * AP verification / review records. * AP test procedures. * AP test specifications. * AP testing results. * AP modification information and results. | 12.5.6,  15.2.2,  17.2.5,  17.2.7. |  |  |