# Introduction



This conformity assessment template is for the assessment of machinery safety-related control systems (SCS) to IEC 62061:2021, *Safety of machinery – Functional safety of safety-related control 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* 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 62061:2021+A1:2024), 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 full SCS safety lifecycle aspects from IEC 62061. When FVL (software level 2) is being used, this template may need support from selected FVL software aspects from the CASS IEC 61508-3 TOEs. Software level 3 is not covered and requires compliance with IEC 61508-3 (see CASS-508-SW).
2. Software development for FVL requires much greater effort plus requires verification & validation of much greater rigor than software development for LVL.
3. For every TOE, generally the rigour shall increase with increasing SIL.

# References

* CASS-508-FSM – Functional Safety Management (IEC 61508-1)
* CASS-508-SW – Software (IEC 61508)

# Acronyms

The following acronyms are used in this template:

|  |  |
| --- | --- |
| CASS | Conformity assessment of safety-related systems |
| Cl. | Clause |
| COTS | Commercially of the shelf |
| FMEA | Failure mode and effect analysis |
| FTA | Fault tree analysis |
| FSM | Functional safety management |
| FVL | Full variability language |
| HFT | Hardware fault tolerance |
| LVL | Limited variability language |
| RA | Risk assessment (incl. hazard analysis) |
| SCS | Safety-related control system |
| SF | Safety function |
| SFF | Safe failure fraction |
| SIL | Safety integrity level |
| SRS | Safety requirements specification |
| SSRS | Software safety requirements specification |
| TOE | Target of evaluation |
| T&M | Techniques & Measures |

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of change |
| V1 | 24/02/2023 | First issue. |
| V2 | 25/02/2025 | Updated naming convention and corrections. |
|  |  |  |
|  |  |  |

| **TOE Ref.** | **Target of Evaluation (TOE)** | **Purpose of TOE / Prompts** | **IEC 62061 reference** | **Auditee’s documents** | **Assessor’s comments** |
| --- | --- | --- | --- | --- | --- |
| 1 | SCS design process (lifecycle) | To ensure the utilisation of an appropriate structured design process, derived from a RA (ISO 12100), and associated tasks to realize each safety function performed by the SCS for a given machine. | 4.2, Figure 2, Figure 3. |  |  |
| 2 | Functional safety plan | To ensure a FSM functional safety plan is drawn up, documented and updated for each SCS design project including: a) identification and scheduling of relevant activities; b) description of policy and strategy for complying with functional safety requirements; c) description of the functional safety approach for safety related software; d) identification of persons / resources responsible for delivering and reviewing relevant activities; e) identification of the procedures / resources to record and maintain information relevant for functional safety; f) description of the approach for configuration management; g) description of the procedure for modification; h) identification of a verification plan; i) identification of a validation plan.  NOTE: A safety-related system culture / FSM is important and the CASS TOEs for IEC 61508-1 FSM can support compliance (CASS-508-FSM). | 4.3. |  |  |
| 3 | Configuration management | To ensure configuration management procedures consistent with the functional safety plan are defined and utilised covering SCS hardware and software. | 4.4, 8.3.8, 8.4.10. |  |  |
| 4 | Modification | To ensure modification procedures (incl. action plan) consistent with the functional safety plan are defined and utilised covering SCS hardware and software including reasoning and impact analysis.  NOTE: Only for modification during design, development, verification and validation. Modification during operation is not covered in IEC 62061:2021. | 4.5, 8.3.8, 8.4.10. |  |  |
| 5 | Safety requirements specification | To ensure the safety requirement specification (SRS), and therefore the functional / integrity requirements specifications, is sufficiently detailed and derived from the RA and used as the basis for the design of the SCS.  NOTE: The SRS is an essential document for validation and shall be checked carefully. The definition of the requirements may be supported by the detailing of assumptions within the SRS. | 5.2. |  |  |
| 6 | Overall SCS design | To ensure the SCS was designed using the SRS with each safety function decomposed into a structure of sub-functions of appropriate integrity.  To ensure the design includes decomposing each safety function into a structure of sub-function(s) that fully describes the functional and integrity requirements of the SCS. | 6.1, 6.2, 6.3, 6.4. |  |  |
| 7 | Avoidance of SCS systematic failures | To confirm the use of measures to avoid systematic hardware failures including: a) SCS designed and implemented to functional safety plan;  b) proper selection, combination, arrangement, assembly and installation of subsystems;  c) SCS used within the manufacturer’s specification;  d) Subsystems with compatible operating characteristics; e) SCS installed / protected to IEC 60204-1, including earth fault detection; f) undocumented modes of component operation are not used;  g) consideration for foreseeable misuse, environmental changes and modification(s); h) manufacturer’s connection instructions applied; i) plus at least one of hardware design review, use of advisory tools or simulation. | 6.5.1. |  |  |
| 8 | Control of SCS systematic faults | To confirm the use of measures to control systematic hardware faults including: a) use of de-energization (safe state of the machine is achieved or maintained);  b) measures to control the effect of temporary subsystem failures (power supply, EMI); c) measures to control the effects of errors and other effects arising from any data communication, including transmission errors; d) fault reaction for fault at an interface occurs before the hazard can occur. | 6.5.2. |  |  |
| 9 | Electromagnetic immunity | To ensure the safety functions or safety-related systems are not affected by external electromagnetic influences in a way that could lead to an unacceptable risk.  To ensure the SCS complies with applicable requirements from IEC 61000-1-2. | 6.6. |  |  |
| 10 | Software based parameterisation | To ensure that any manual software based safety-related parameters for a safety function or sub-function are correctly transferred into the parameterisable element. | 6.7.1, 6.7.2, 6.7.3. |  |  |
| 11 | Parameterisation tool verification | To ensure the basic functionality of the parameterisation tool is verified. | 6.7.4, 6.7.5. |  |  |
| 12 | Security aspects | To ensure security aspects are considered in the lifecycle of the machine (or at a higher system level). | 6.8. |  |  |
| 13 | Periodic testing | To ensure periodic testing for both testing for failed functions and testing in conjunction with inspections for equipment boundary conditions is planned and defined.  To ensure this includes testing from the accumulation of undetected faults (e.g., in a redundant system). | 6.9, 7.3.3.4. |  |  |
| 14 | Subsystem design and development | To ensure that subsystems are designed and developed according to the safety requirements including considerations of requirements for: - functionality; - hardware safety integrity; - systematic integrity; - subsystem fault detection behaviour; - software;  To ensure the reliability calculations for the subsystems and safety functions are detailed, documented and correct (PFH, MTTF, λ, B10).  NOTE: this is a general TOE, other aspects are also considered elsewhere. | 7.1, 7.2, 7.3.4, 7.6. |  |  |
| 15 | Avoidance of subsystem systematic failures | To ensure the use of measures to avoid systematic failures including: - appropriate selection, combination, arrangements, assembly and installation of components (including wiring / interconnections); - use of the subsystem / elements within manufacturer’s specification / instructions; - components with compatible operating characteristics; - specified environmental conditions; - components that are in accordance with an applicable standard and have their failure modes well-defined; - use of suitable materials and adequate manufacturing; - correct dimensioning and shaping;  - plus, one of hardware design review, computer-aided design tools (capable of simulation or analysis), or simulation. | 7.3.2.2. |  |  |
| 16 | Control of subsystem systematic faults | To ensure the use of measures to control systematic faults including: a) measures to control the effects of insulation breakdown, voltage variations and interruptions, overvoltage and undervoltage; b) measures to control or avoid the effects of the physical environment (temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects); c) measures to control or avoid the effects of temperature increase or decrease; d) measures to control the effects of hose breakdown, pressure variations and interruptions, too low or too high pressure.  Plus, the use of the following basic safety principles:  - use of de-energisation;  - measures for controlling the effects of errors and other effects related to data communication.  Plus, the use of the following well-tried safety principles:  - failure detection by automatic tests;  - tests by comparison of redundant hardware;  - diverse hardware;  - operation in the positive mode;  - mechanically linked contacts;  - direct opening action;  - oriented mode of failure;  - over-dimensioning by a suitable factor. | 7.3.2.3. |  |  |
| 17 | Fault consideration and exclusion | To ensure that the subsystem elements are designed to resist faults and to ensure the capability of a subsystem element to reach a certain safe state has been estimated including an analysis of faults and their corresponding failure modes (e.g., FMEA, FTA).  To ensure fault exclusions are justified and documented. | 7.3.3. |  |  |
| 18 | Architecture and constraints | To ensure the subsystem is designed with an appropriate architecture, Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF). | 7.4, 7.5. |  |  |
| 19 | Software level 1 (general) | To ensure IEC 61508 (or similar) pre-designed platforms running limited variability language (LVL) software focuses on the avoidance of faults introduced during the software lifecycle and produces readable, understandable, testable, maintainable and correct software.  This includes to ensure:  a) a software safety lifecycle model (e.g. V-model) with distinct phases has been used to achieve the required level of safety.  b) suitable manufacturer tools including compliance with associated instructions.  c) justified module design, coding and testing, if relevant.  d) coding derived from relevant coding rules (standards), specification and design.  e) planned, managed and documented software testing.  NOTE: Compliance with LVL can often be achieved by selecting an appropriate COTS IEC 61508-3 pre-designed platform (with associated tools) and following the manufacturer’s instructions. It is recommended to check a platforms compliance with IEC 61508 carefully. | 8.1, 8.2, 8.3.1, 8.3.3, 8.3.4, 8.3.5, 8.3.6. |  |  |
| 20 | Software level 2 (general) | To ensure IEC 61508 (or similar) pre-designed platforms running full variability language (FVL) software focuses on the avoidance of faults introduced during the software lifecycle and produces readable, understandable, testable, maintainable and correct software.  This includes to ensure:  a) a “deeper” software safety lifecycle model (e.g. V-model) with distinct phases has been used to achieve the required level of safety (maximum of SIL 2).  b) suitable and justified (see 8.4.1.3) set of tools including compliance with associated instructions.  c) application of T&M from IEC 61508-3 Annex A and B.  c) a detailed module design specification.  d) justified module design, coding and testing.  e) coding derived from relevant detailed coding rules (standards), specification and design.  f) planned, managed and documented software testing (including integration testing).  NOTE: Compliance with FVL (software level 2) requires much greater effort and still relies on selection of a COTS IEC 61508-3 pre-designed platform. It is recommended to check a platforms compliance with IEC 61508 carefully. NOTE: this TOE covers an extensive range of aspects and support may be required from IEC 61508-3 TOEs (CASS-508-SW). | 8.1, 8.2, 8.4.1, 8.4.2, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.4.8, Figure 14. |  | CAUTION: Please review the CASS IEC 61508-3 TOEs (CASS-508-SW) before proceeding. |
| 21 | Software safety requirements specification | To ensure the software safety requirements specification (SSRS) is derived from the SRS and sufficiently detailed to support functional safety including coding guidelines.  For software level 2, this includes selection of a suitable language and requirements for monitoring, diagnostics, control flow and data flow (for the SIL / SCS).  NOTE: The SSRS is an essential document for validation and shall be checked carefully. The definition of the requirements may be supported by the detailing of assumptions within the SSRS.  NOTE: Software level 2 requires greater detail. | 8.3.2.1,  8.3.2.2,  8.4.2.2. |  |  |
| 22 | Software design specification | To ensure the software design specification is derived from, and traceable to, the SSRS and sufficiently detailed to support functional safety including relevant functions (e.g. diagnostics) and test cases.  To ensure the software design was planned, developed, and documented before the coding.  NOTE: Software level 2 requires greater detail. | 8.3.2.3,  8.3.3,  8.4.2.3, 8.4.3.2, 8.4.4.3. |  |  |
| 23 | Software level 2 design | To ensure a suitable software design and to ensure a software system design specification explains the main software aspects.  This includes architecture definition, following a modular approach, limited module sizes (one SF), fully defined interfaces, single entry / exit point and T&M (to avoid systematic failures).  NOTE: this TOE covers an extensive range of aspects and support may be required from IEC 61508-3 TOEs (CASS-508-SW). | 8.4.3, 8.4.4. |  | CAUTION: Please review the CASS IEC 61508-3 TOEs (CASS-508-SW) before proceeding. |
| 24 | Software level 2 systematic failures | To ensure relevant programming techniques are used to avoid systematic failures in FVL software.  NOTE: this TOE covers an extensive range of aspects and support may be required from IEC 61508-3 TOEs (CASS-508-SW). | 8.4.3. |  | CAUTION: Please review the CASS IEC 61508-3 TOEs (CASS-508-SW) before proceeding. |
| 25 | Verification | To ensure that the overall SCS validation is supported by documented verification of key safety integrity aspects for the safety requirement specification, safety-related software (including software and specification reviews) and subsystem architecture. | 9.2.3, 9.5.1, 9.5.2, 9.5.4. |  |  |
| 26 | Validation plan | To ensure the validation plan identifies and describes the requirements for carrying out the validation process and also identifies the means to be employed to validate the specified safety functions.  NOTE: analysis is a key part of validation. | 9.1.1, 9.1.2, 9.1.3. |  |  |
| 27 | Validation information | To ensure that the extensive information required for validation is documented, was made available at the right time, and was correctly used during the validation process.  NOTE: analysis is a key part of validation. | 9.1.4. |  |  |
| 28 | Validation | To confirm by examination (e.g., tests, analysis) that the SCS and safety functions meet the functional safety requirements of the specific application.  Validation shall be carried out by persons who are independent from the design of the SCS.  NOTE: The analysis should be started as early as possible in, and in parallel with, the design process. | 9.1.5, 9.2.1, 9.2.2, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.4, 9.5, Figure 15. |  |  |
| 29 | Technical information and documentation | To confirm that the technical documentation produced as part of SCS development is fit for purpose, available to those involved in the safety lifecycle and contains all relevant descriptions of the SCS design, installation, operation, maintenance and testing. Each document should be accurate, understandable, accessible, maintainable (i.e. editable) and traceable to the SRS and RA. | 8.3.7, 8.4.9, 10.2. |  |  |
| 30 | SCS Information for use | To confirm that the information for use of the SCS details specific information on the safety integrity, subsystem detail and other information important for the safe installation, use and maintenance of the SCS / subsystem. | 10.3. |  |  |
| 31 | Document identification and revision control | To ensure each document is 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. | 4.4. |  |  |
| N/A |  | \*\*\* END OF TABLE \*\*\* |  |  |  |