IECEE OD-2064

Edition 1.0 2018-06-05

IECEE
OPERATIONAL DOCUMENT

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System)

IECEE Conformity Assessment scheme for functional safety

IECEE OD-2064:2018(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.
Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

CONTENTS

FOREWORD

Document Owner

CMC TF Functional Safety

History of changes

Revision Date	Brief summary of changes
N/A	N/A, as first edition

Effective date	Next maintenance due date
2018-06-05	2021-06-05

1 Purpose and objective of this document

1.1 Purpose

To identify and specify requirements on a CB Conformity Assessment scheme for functional safety (per IEC 61508 and other derived functional safety standards – future state) as it relates to IEC 60947-5-3, IEC 60947-5-5, and IEC 61800-5-2 (STO function related to discreet hardware only).

Only products having no other designated safety sub-function than STO according to clause 4.2.3.2 in IEC 61800-5-2:2016 are covered by this program. (Future state - to be considered will be other safety sub-functions).

Functional Safety evaluations as a part of the Scope of a CBTL are not permitted to be subcontracted.

No stand-alone CBTC shall be issued exclusively for the Functional Safety of components in the scope of IEC 60947-5-3, IEC 60947-5-5 and IEC 61800-5-2.

This covers:

– Assessment activities and capturing of assessment results

1.2 Objective

These requirements shall ensure that the CB Certificate provides adequate confidence in the functional safety of the product:

– Confidence for the user (integrator, end-user) of the product

– Confidence for bodies/organizations who are asked to accept the product

2 Definitions

Product – Safety-related control system (E/E/PE system), subsystem, or element, or single component, (as defined by IEC 61508) to be subjected to Functional Safety CB Conformity Assessment.

Deliverable – Information container such as documents or models (i.e. containing artefacts), or product (part) samples, to be submitted by the manufacturer for functional safety investigation. Deliverables can be product-related (e.g. safety requirements specification, FMEDA, PWB), or process/FSM-related (e.g. safety plan, SW configuration management plan).

3 Requirements of a Conformity Assessment procedure for Functional Safety

To achieve functional safety compliance, evaluation should begin in the early stages (planning) of product development lifecycle. The following requirements shall be satisfied:

- The scope of a Functional Safety Conformity Assessment shall be clearly identified (in terms of the product's position in system hierarchy, and interfaces), and assumptions made shall be clearly specified (e.g. it will often have to be assumed that the functional safety requirements on the product are complete and correct in relation to the intended application of the product).
- Functional Safety Conformity Assessment shall follow a modular top-down approach. The product is decomposed in sub-systems, elements, modules, components, as appropriate, and evaluated following Route 1H as described by IEC 61508:2010. (Routes 1S, 2S, 3S are possible future state)
- The overall process of Functional Safety Conformity Assessment consists of:
    - Investigation, based on deliverables submitted by the manufacturer.
    - Evaluation, based on investigation results.
    - Certification decision, based on the evaluation result (N/A, PASS, or FAIL).

3.1 Investigation

Activities include review, inspection, analysis, testing, and audit:

3.1.1 Review

A complete investigation of a deliverable. Review results are captured (e.g. in checklists, review logs).

- To be applied for key deliverables, such as Safety Requirements Specification, System Architecture Description, System Level FMEDA.
- Objectives: completeness, correctness, compliance.

3.1.2 Inspection

Investigation of selected parts of a deliverable. Selection is done in an informed and documented manner. Rationale for selection is documented, inspection results are captured (e.g. in checklists, review logs).

3.1.3 Analysis

Investigation by (witnessing of) application of analysis techniques and/or tools. Typically it is applied to selected parts of a deliverable. Rationale for selection is documented, analysis results and observations are captured (e.g. in analysis reports).

- To be applied for analysis cases that play a role in the overall safety case, e.g. coding rule enforcement, state-space exploration, test coverage analysis.
- Main objectives: confidence in analysis results submitted by manufacturer. Secondary objectives: completeness, correctness.

3.1.4 Testing

Investigation of deliverables by executing, or by witnessing the execution of, specific and consciously selected test cases as specified in test specifications submitted by the manufacturer, and by reporting the results. Rationale for selection is documented, testing results and observations are captured (e.g. in test reports).

- Test cases selected should cover function test, fault insertion test, environmental impact test, as well as software verification and validation.
- Main objectives: confidence in test results submitted by manufacturer. Secondary objectives: completeness, correctness.

3.1.5 Functional Safety Management (FSM) Audit

Verification of implementation of process/FSM-related deliverables (For the current Standards in the Scope the requirements can be further defined in the TRF. Future state may require additional requirements in this area). Preferentially, an on-site audit is conducted while flexibility to consider a desk-audit is permitted.

3.2 Evaluation

Provides CBTL's judgement on compliance, completeness, and correctness of product in relation to the applied functional safety standards and the functional safety requirements identified for the product, using the investigation results for argumentation. (For complex products, or for long project durations, it is recommended that there be one or more intermediate evaluation reports. Consider for future state)

3.3 Certification decision

In accordance with the IECEE Rules.

Annex A **(Informative)**

Example: **Functional Safety Conformity Assessment** procedure for “simple” (Type A) subsystems (such as it relates to IEC 61800-5-2 (STO function), IEC 60947-5-5, and IEC 60947-5-3)

Deliverables submitted by manufacturer	**Conformity Assessment Investigation Activity + focus areas /**indicative, not exhaustive!*/***	**Pass/Fail/NA**
Safety Requirements Specification (SRS)	Review - compliance and completeness with respect to standard requirements - Systematic integrity addressed? - Correctness	
System design requirements and architecture description (SAD) – hardware level	Review - Safety channels specified? - Diagnostic channels specified? - Independence between safety-related and non-safety related specified? - Power supply and other potential common causes for failures addressed? - Interfaces to other devices specified? Application examples?	
Block-level FMEDA	Review - Diagnostic coverage	
Hardware safety requirements specification (HWSRS)	Review - Correct and complete refinement of SRS? - All information needed for HW design?	
Hardware design documentation (HWDD) - Schematics - BoM - Layout	Review - Structure as in SRS or architecture? - Failure exclusions possible? - Well-tried components?	
HW component-level FMEDA	Review or Inspection - Component reliability data from acceptable source? - Reliability prediction and failure mode distribution? - Failure mode classification? - Diagnostic coverage?	
PFH, SFF calculation	Review - Formula or reliability model consistent with structure? - Common cause failures correctly reflected? - Mission time, proof test interval correctly reflected? - Proof test specified?	
Function and fault insertion test specifications and reports	Review or Inspection	

Deliverables submitted by manufacturer	**Conformity Assessment Investigation Activity + focus areas /**indicative, not exhaustive!*/***	**Pass/Fail/NA**
Environmental impact test specifications and reports	Review or Inspection - Test cases cover actually the safety functionality and the related circuits? - Increased immunity levels considered? - Calibrated test equipment, ISO 17025 labs?	
Instructions for use	Review	
Product, product parts (e.g. PWB unmounted, mounted)	Review - Failure exclusions (spacings, ...) possible? Test - Representative and/or crucial test cases selected and witnessed or executed. o Function test o Fault insertion test o Environmental impact test	

Annex B **(Informative)**

Challenges of **certifying functional safety of a product in accordance with IEC 61508 and derived standards**

- The standards are written for the system designer, rather than for the assessor or certifier (CBTL). A CB Conformity Assessment Procedure and TRF's cannot be directly derived from the standards.
- The standards do not provide explicit or concrete test requirements. The standards prescribe a lifecycle including verification and validation phases and activities. The corresponding verification and validation specifications must be developed and executed accordingly.
    - Assessment of compliance with the standards may therefore not provide the adequate confidence.
    - In order to achieve adequate confidence in the functional safety of a product, also the technical correctness and completeness of the output of the various lifecycle phases must be addressed by the CB Conformity Assessment Procedure.
- Functional safety of a product cannot be evaluated on the basis of pure testing alone (e.g. software can often not be tested completely with reasonable effort). Testing must be supplemented with review, inspection, analysis, and audit. In fact, document-based review and inspection may often represent the bulk of the evaluation effort in a certification project.
- The verification&validation effort in a functional safety development project may be very big. The CBTL may have to sample or spot-check, and a right balance between confidence and evaluation effort must be found.
- Functional safety engineering, and thus also functional safety evaluation, requires competency in many different disciplines, such as embedded systems and software engineering, HW reliability and probabilistic calculation, quality management and process improvement.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
info@iec.ch
www.iec.ch

IEC SYSTEM OF CONFORMITY ASSESSMENT SCHEMES FOR ELECTROTECHNICAL EQUIPMENT AND COMPONENTS (IECEE)

IECEE Secretariat c/o IEC
3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
secretariat@iecee.org
www.iecee.org