IEC TR 63201

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Low-voltage switchgear and controlgear – Guidance for the development of embedded software

IEC TR 63201:2019-05(en)

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and once a month by email.

IEC 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: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TR 63201:2019
https://standards.iteh.ai/catalog/standards/sist/1f7812aa-ad86-48c1-b011-e9b1be7f44ab/iec-tr-63201-2019

IEC TR 63201

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Low-voltage switchgear and controlgear – Guidance for the development of embedded software

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.130.20

ISBN 978-2-8322-7006-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – GUIDANCE FOR THE DEVELOPMENT OF EMBEDDED SOFTWARE

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63201, which is a technical report, has been prepared by subcommittee 121A: Low-voltage switchgear and controlgear, of IEC technical committee 121: Switchgear and controlgear and their assemblies for low voltage.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
121A/256/DTR	121A/287A/RVDTR

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Programmable electronics are now being integrated within switchgear and controlgear. For example, soft-starters, electronic overload relays, circuit-breakers with electronic trip units, proximity switches with built in micro-controllers and some accessories such as extension modules and control panels are using programmable electronics with embedded software called firmware. This embedded software often supports the main functions (see 3.3) provided by the equipment such as overcurrent protection and other important functions, e.g. alarm detection from monitoring devices.

The integration of embedded software within switchgear and controlgear should not degrade the integrity of their main functions compared to purely electromechanical equipment. Therefore, a minimum set of standard requirements for embedded software is provided by this document.

This document takes into account the existing best practices for developing embedded software within safety functions for automation given by IEC 61508-3. Functional safety approach is mainly used in machinery, automotive, automation and process automation where safety functions are implemented with multiple components which should match a consistent level of integrity when combined. In other sectors, such as electric distribution and power control systems, key functions such as over-current release, residual current release, load monitoring, etc. should follow installation rules and coordination rules which are systematically safety and reliability related. Therefore, this document can be seen as providing the principles of the good practice given by IEC 61508-3.

This document is also intended to provide an up-to-date method with regards to the supplement SE of UL 489.

The intention of this document is to provide guidance about:

– risk assessment aspects in relation to embedded software;
– embedded software evaluation method;
– software architecture;
– basic coding rules;
– measures to control software errors;
– software verification and its relationship with the validation of the equipment or system.

In this document, the term “software” is used as a generalized term for embedded software.

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – GUIDANCE FOR THE DEVELOPMENT OF EMBEDDED SOFTWARE

1 Scope

This document provides information, and recommended minimum requirements related to embedded software supporting the main functions of switchgear and controlgear during the whole lifecycle of the equipment. It includes also the parameterization aspects and basics about secure coding standards.

This document can be used in addition to product standard requirements when not already covered.

This document is appropriate for new development or major changes in existing equipment.

This document is not intended to cover the functional safety of control systems for machinery or for automation which are covered by IEC 62061, ISO 13849-1 and IEC 61508 (all parts), neither the cybersecurity risk which are covered by ISO 27005, and IEC 62443 (all parts). It gives only some example of secure coding rules.

NOTE Future new publication IEC TS 63208[1] is under development for implementing embedded cybersecurity measures within switchgear and controlgear based on ISO 27005 and IEC 62443 (all parts).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-1:1993, as well as the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
embedded software
software, supplied by the manufacturer, that is an integral part of the equipment and that is not accessible for partial modification

Note 1 to entry: Firmware and system software are examples of embedded software.

Note 2 to entry: An embedded software can be upgraded by an integral upload.

---

1 Future publication IEC TS 63208 is currently at CD stage.

3.2
programmable electronic
based on computer technology which can comprise hardware, software, and input and/or output units

EXAMPLE The following are all programmable electronics:

- microprocessors;
- micro-controllers;
- programmable controllers;
- application specific digital integrated circuits (ASICs with programmable part);
- programmable logic controllers (PLCs);
- other computer-based devices (for example smart sensors, transmitters, actuators).

Note 1 to entry: This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc.

Note 2 to entry: The term "programmable component" is from ANSI/UL 1998:2013, definition 2.39.The definition in ANSI/UL for programmable component is: "Any microelectronic hardware that can be programmed in the design centre, the factory, or in the field". Here the term "programmable" is taken to be "any manner in which one can alter the software wherein the behaviour of the component can be altered."

[SOURCE: IEC 61508-4:2010, 3.2.12, modified – In the definition, "may" changed by "can", "be" and "of" deleted, and addition of a new Note 2 to entry.]

3.3
main function

<switchgear and controlgear> defined function of switchgear and controlgear whose failure can result in its unwanted operation which can lead to hazardous situations, in the loss of its protective function, or in the loss of a key functionality defined by the manufacturer

3.4
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in:

- the safety requirements specification;
- the design, manufacture, installation and/or operation of the hardware;
- the design and/or implementation of the software.

[SOURCE: IEC 61508-4, 3.6.6, modified – Deletion of Note 4 to entry.]

3.5
full variability language
FVL
type of language that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: FVL is normally found in embedded software and is rarely used in application software.

Note 2 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

[SOURCE: IEC 61511-1:2016, 3.2.75.3, modified – Deletion of "designed to be comprehensible to computer programmers" and Note 1 to entry, remaining notes to entry renumbered.]

3.6
configuration management
discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the lifecycle at a specific point of time

[SOURCE: IEC 61508-4:2010, 3.7.3, modified – Addition of "at a specific point of time".]

3.7
baseline
<configuration management> agreed set of elements (hardware, software, documentation, tests...) of an equipment at a specific point in time, which serves as a basis for verification, validation, modification and changes

Note 1 to entry: If an element is changed the status of the baseline is intermediate until a new baseline is defined.

3.8
coding rules
coding standard
set of rules and guidelines for the formatting of software source code of a program intended to ensure its readability, maintainability, compatibility and robustness

Note 1 to entry: Typical aspects of coding rules are naming conventions, file naming and organization, formatting and indentation, comments and documentation, classes, functions and interfaces, allowed/forbidden standard library function usages, data types, pointer and reference usage, and testing.

3.9
software unit
separately compilable piece of code

Note 1 to entry: Software unit is also called software module and software component such as in documents from International Software Testing Qualifications Board (ISTQB).

[SOURCE: ISO/IEC 12207:2008, 4.43, modified – Addition of a new Note 1 to entry.]

3.10
integration tests
<software> tests performed during the software units and hardware/software integration process prior to the verification and system validation to verify compatibility of the software and the hardware

[SOURCE: IEC 60880:2006, 3.23, modified – Addition of “software units and”, replacement of “computer-based” and “computer” by “the verification and system validation”.]

3.11
software verification
confirmation by examination (e.g. tests, analysis) that the software, its integration or its units requirements have been fulfilled

3.12
static analysis
<software> examination of source code for features that may indicate the presence of software faults

Note 1 to entry: Static analysis typically reveals unreachable sections of code, unused, misused, doubly-defined or uninitialized variables, and unintended execution paths.

Note 2 to entry: Static analysis normally employs computer aided software engineering tools.

[SOURCE: IEC 60050-192:2015, 192-09-22]

3.13
system validation
confirmation by examination and provision of objective evidence that the requirements for a specific intended use of the equipment or the system are fulfilled

Note 1 to entry: By principle the embedded software is integrated in an equipment or a system. The validation of this equipment or system includes embedded software related verifications.

4 Risk assessment and identification of the main functions

Based on manufacturer experience, a system analysis, in the context of the intended applications of the equipment, including its different modes of operation and the reasonably foreseeable misuse, should determine the list of main functions and their associated degree of risk.

EXAMPLE Sensor detection of an object, overcurrent protective function, continuity of supply, power off a motor system.

A risk assessment method such as IEC Guide 116 should be used for this purpose.

Each software part implementing a main function should be managed according to the method provided in this document.

5 Design management

5.1 Objective

A particular organisation of the software design is necessary to ensure the complete realisation of the main function according to its original specification.

This organisation should be defined by a software management plan which may be a clearly identified part of a global design management plan.

5.2 Software management plan of the main functions

This plan is required for defining the management of the activities along the software development lifecycle for the specification and the verification of the software related to main functions (see 3.3).

The organisation should be defined with the roles and associated responsibilities for the management (starting, controlling) and the execution of the activities.

It should be drawn up, documented and updated as necessary. It is intended to provide measures for preventing incorrect specification, implementation, or modification issues.

The software management plan of the main functions should be adapted to the project.

In particular, the plan should:

a) identify the relevant design activities for the development of the parts related to the main functions (essential design activities and their organisation in appropriate sequences are illustrated in Figure 2);
b) describe the policy and strategy to fulfil the specified requirements related to the main functions;
c) describe the strategy for the development, integration, and verification which may include conformity assessment;