IEC TS 61508-3-1

Edition 1.0 2016-07

TECHNICAL SPECIFICATION

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 3-1: Software requirements – Reuse of pre-existing software elements to implement all or part of a safety function

IEC TS 61508-3-1:2016-07(en)

Copyright International Electrotechnical Commission

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 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 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.

Copyright International Electrotechnical Commission

IEC TS 61508-3-1

Edition 1.0 2016-07

TECHNICAL SPECIFICATION

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3-1: Software requirements – Reuse of pre-existing software elements to implement all or part of a safety function

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 25.040.40; 35.240.50

ISBN 978-2-8322-3516-4

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

Copyright International Electrotechnical Commission

CONTENTS

Copyright International Electrotechnical Commission

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 3-1: Software requirements – Reuse of pre-existing software elements to implement all or part of a safety function

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. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

Copyright International Electrotechnical Commission

IEC TS 61508-3-1, which is a technical specification, has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

Enquiry draft	Report on voting
65A/780/DTS	65A/802/RVC

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

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

A list of all parts in the IEC 61508 series, published under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*, can be found on the IEC website.

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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

Copyright International Electrotechnical Commission

INTRODUCTION

The requirements set out in this technical specification deal with the reuse of software elements when they are intended to form part of a safety function.

In many fields of automation, software elements are used today in support of safety functions. Such applications will certainly be further developed and extended. Software engineers, however, do not always wish to write the software for these applications from scratch, but will in many cases use already existing software and integrate it with the new application which might be slightly different from the one for which the software was originally specified.

In IEC 61508-3:2010, a requirement is given in 7.4.2.12. It offers three routes to the achievement of the necessary integrity for the pre-existing software element. The requirements to comply with the second route, Route 2_S, are defined in IEC 61508-2:2010, 7.4.10.

This entails that IEC 61508-3:2010 –dealing solely with software –refers to requirements in IEC 61508-2:2010 which concerns complete systems including hardware but excluding software (see IEC 61508-2:2010, 1.1 enumeration “e“).

This technical specification defines the requirements for software elements explicitly, because IEC 61508-2:2010 excludes software, and is intended to replace the text of the second bullet (“route 2_S”) of a), 7.4.2.12 in IEC 61508-3:2010 in a future revision of IEC 61508-3.

Copyright International Electrotechnical Commission

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 3-1: Software requirements – Reuse of pre-existing software elements to implement all or part of a safety function

1 Scope

This Technical Specification presents requirements by the application of which pre-existing software elements may be claimed to be proven-in-use for all or a part of safety function(s) of SIL1 or SIL 2.

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.

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

3 Terms and definitions

No terms and definitions are listed in this document.

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

4 Requirements

4.1 Notes 1 to 4 below apply to the entire Clause 4 (4.2 to 4.9).

NOTE 1 Any documentation required by a clause in this document could either be available with the pre-existing software or could be included as part of the documentation of the safety related function.

NOTE 2 A reused software function in this document means a function specified on the level of the requirements specification (see IEC 61508-3:2010, 7.2). A reused software function does not refer to a programming language construct.

NOTE 3 Conditions are set for the data on the history of the pre-existing software in 4.2 b) and c). The fulfilment of these conditions does not entail that the software is deterministic: hidden internal states of the software can affect its execution even when the required combination as specified in 4.2 b) and c) is exactly the same. The use of pre-existing software is thus restricted by 4.7.

NOTE 4 In some cases (e.g. input data are analogue data or a clock signal) the demonstration of proven-in-use for software could be difficult.

4.2 An element shall only be regarded as proven-in-use when:

a) its description:
   1) exists and is available;
   2) fulfils the requirements of IEC 61508-3:2010, 7.2;
   3) describes the previous use,

Copyright International Electrotechnical Commission

and

b) the execution of the software with all combinations of all claimed
   – combinations of input data,
   – sequences of execution of the reused software function(s),
   – timing relations within sequences of execution of the reused software function(s)

   which will occur in the intended use are documented;

and

c) combinations of all
   – input data,
   – sequences of execution of the reused software function(s),
   – timing relations within sequences of execution of the reused software function(s)

   which are not part of the proven-in-use claim, comply with 4.8,

and

d) the combinations described in 4.2 b) that will be used in the intended use have occurred in the previous use with the same relative frequency. This future frequency shall be justified in comparison to the previous use and documented.

and

e) there is adequate evidence to demonstrate the completeness of the documentation,

and

f) the element together with the hardware on which it will run will be subject to documented
   – analysis of any operational experience of the integrated hardware and software element;
   – suitability analysis of the hardware and software element;
   – testing of the hardware and software element. This documentation includes:
     - specification of the goals of the test runs from the properties documented in 4.2 a), b) and d) above;
     - details of the testing for each individual goal;
     - an estimate of the confidence with which the testing established each individual goal;
     - a demonstration that the estimated confidence is appropriate to the goal and the test results.

NOTE 1 Suitability analysis and testing focuses on the demonstration of a hardware and software element's performance within the intended application. The results of existing analyses and testing could be taken into account. This includes functional behaviour, accuracy, behaviour in the case of a fault, time response, response to overload, usability (e.g., avoidance of human error) and maintainability.

NOTE 2 A mathematical partitioning of the input data can be helpful to identify all proven-in-use combinations.

NOTE 3 By "input data" is meant all input data to the software element. For example, it can be that the hardware on which the software element runs generates internal data that are input to the software, such as diagnostics.

NOTE 4 The timing relations most often found and most in need of verification are linear timing relations of the form (fastest possible time <= execution time <= longest possible time). There are practical methods for verifying and checking the mutual consistency of timing requirements of such a form.

4.3 The documentary evidence required by 4.2 shall

a) demonstrate that the following features and phenomena of the previous experience evaluated for the proven-in-use claim are identical in the intended use of the element:
   – hardware (e.g. processor, memory, clock, bus behaviour) and demand profiles;

Copyright International Electrotechnical Commission

– configuration (e.g., compiler options used in compiling the source code for the proposed use, initialisation of program variables and constants, the hardware configuration on which the software will execute);

– software interfaces;

– libraries (including source code libraries as well as libraries of binary code);

– operating system, interpreters (for example, those used to emulate processor architectures on processors which do not share that architecture);

– translator (compiler), linker, code generators;

and

b) contain a complete description of the conditions of use of the pre-existing software.

NOTE 1 The conditions of use (operational profile) include all the factors that can trigger systematic faults in the hardware and software of the element. For example additional modes of use, functions performed, human factors.

NOTE 2 Much of this information can be located in the safety manual (see IEC 61508-3:2010, 7.4.2.12).

4.4 The documentary evidence required by 4.2 shall demonstrate that there was a comprehensive failure detection in the observation period, that is, for the time period in which the behavior of all

– proven-in-use combinations of input data,

– sequences of execution of the reused software function(s),

– timing relations within sequences of execution of the reused software function(s)

was observed. It shall be demonstrated that any individual failure caused by the software would have been detected and reported.

The documentation of, analysis of, and evaluation of the consequences of reported failures shall be provided.

NOTE 1 The collection of evidence for proven-in-use elements requires an effective system for reporting failures.

NOTE 2 This technical specification does not use the concept of probabilistic failure rate for software.

4.5 Differences between the previous conditions of use (see 4.3 Note 1) and those that will be experienced by the PE safety-related system shall be documented. An impact analysis on the differences shall be carried out and documented using a combination of appropriate analytical methods as well as specific testing, in order to demonstrate that the likelihood of systematic faults which could cause dangerous failures is low enough that the required safety integrity level(s) of the safety function(s) using the element is achieved.

4.6 A proven-in-use safety justification shall be documented, using the information available from 4.3, that the element supports the required safety function with the required SIL. This shall include:

a) derivation from the software safety requirements specification (see IEC 61508-3:2010, 7.2) of the PE safety-related system;

b) the results of testing the element for the intended application;

c) the documentary evidence as described in 4.3;

d) the proof that the element has adequate previous use.

Copyright International Electrotechnical Commission

4.7 The requirements of this document shall only be used when reusing software for SIL 1 and SIL 2.

NOTE The limitation of the use of proven-in-use software to SIL 1 and SIL 2 is due to the fact that the methods classified as HR from the tables in IEC 61508-3 2010, Annexes A and B, up to SIL 2 mainly address only black-box aspects of behaviour.

4.8 Evidence shall be given that reused software functions of the pre-existing software that have not been adequately (in accordance with 4.2, 4.3 and 4.4) covered in the proven-in-use demonstration, have no adverse affect on the safety integrity of the E/E/PE safety-related system.

NOTE This requirement can be achieved by ensuring that the reused software functions are physically or electrically disabled or demonstration that the input data for the software are restricted in a way that these functions are excluded from the operational configuration, or by other forms of arguments and evidence.

4.9 After any modification at all, the formerly proven-in-use software shall no longer be taken to be proven-in-use. Any future modification to proven-in-use software shall comply with the requirements of IEC 61508-3:2010, 7.8.

NOTE Modified software is not any more “proven-in-use”, and therefore falls outside the scope of this document.

Copyright International Electrotechnical Commission

Bibliography

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

_____

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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

Copyright International Electrotechnical Commission