PD IEC/TS 61508-3-1:2016

BSI Standards Publication

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

bsi.

National foreword

This Published Document is the UK implementation of IEC/TS 61508-3-1:2016.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 90008 2
ICS 25.040.40; 35.240.50

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 August 2016.

Amendments/corrigenda issued since publication

Date	Text affected

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

CONTENTS

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.

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.

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.

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,