IEC TS 61508-3-2

Edition 1.0 2024-08

TECHNICAL SPECIFICATION

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3-2: Requirements and guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40 ISBN 978-2-8322-9565-6

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 3-2: Requirements and guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 61508-3-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
65A/1113/DTS	65A/1143/RVDTS

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

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

INTRODUCTION

IEC 61508-1:2010 through IEC 61508-7:2010 forms the series of basic standards for the functional safety of electric, electronic and programmable electronic systems (E/E/PE systems). It covers the life cycle of these systems. The major part of the functionality of such systems is often implemented in software. IEC 61508-3:2010 sets software requirements.

IEC 61508-3:2010 Annex A (normative) and Annexes B and C (informative) contain tables listing various techniques and measures, and provide some guidance to the selection of such techniques for different safety integrity levels (SIL). It lists general categories and gives different levels of recommendation for these, such as "not recommended", "recommended" or "highly recommended", as well as more specific techniques for various phases of software development.

These techniques and measures are a mix of generic and specific. The phrase "Formal Methods" as used in IEC 61508-3 refers to the use of mathematical and logical techniques for specifying, assessing, designing and verifying software. Today, such methods are available for specifying requirements, for the assessment of the design, for checking source code and object code and for the derivation of test suites, and for monitoring the correct operation of software at runtime. In this document, we refer to these methods by using the description as mathematical and logical techniques (M&LT; sometimes doubled as M&LT techniques). Some of the M&LT techniques in this document are not restricted to software development, being equally applicable to other digital-system-based engineering technologies. None of the M&LT techniques are limited to the domain of safety-related software systems, although in this document only safety-related applications of M&LT techniques are explicitly addressed.

Use of the recommended methods of IEC 61508-3:2010, Annexes A, B and C do not rule out, for example, susceptibility of the software to run-time failure. State of the art in software development enables various types of run-time failures to be ruled out through rigorous development of the software. It is possible using techniques identified here to assure freedom from many types of software run-time failures.

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

Part 3-2: Requirements and guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation

1 Scope

This Technical Specification, part of the IEC 61508 series, covers the general assurance of dependable software used in critical operational-technology (OT) which is running on hardware devices which are specified as part of the OT application. It is particularly aimed at safety-related software which is being developed according to the E/E/PE software functional safety standard IEC 61508-3; in particular, the development of the software follows a Formal Safety Requirements Specification. Successful use of some or all of the assurance points specified in this document enhances the confidence that a particular piece of safety-related software meets the requirements of the SIL of the safety function which it (partially or fully) implements, and thereby increases the systematic capability of the software.

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*

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