IEC TR 61508-3-3

Edition 1.0 2025-07

TECHNICAL REPORT

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 3-3: Object-oriented software in safety-related systems

ICS 13.110; 25.040.40

ISBN 978-2-8327-0556-8

IEC Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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 3-3: Object-oriented software in safety-related systems

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

This TR is a supplement to the IEC 61508 standard series. It has to be read in conjunction with IEC 61508-3 and proposes a way how the use of object-oriented software in safety relevant applications can be justified.

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

Draft	Report on voting
65A/1176/DTR	65A/1181/RVDTR

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 Report 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

This document addresses specific concepts associated with object-oriented (OO) software. It deals only with OO software in general without referencing any specific language. Each of the concepts is discussed under separate clauses, one addressing fundamentals – i.e. benefits, disadvantages and counter-measures to the disadvantages, the others detailing guidance on the attributes to be satisfied in safety-related systems, according to the systematic capability to be achieved.

It is useful to consider addressing the language-specific best practice contained in guidelines, coding rules, handbooks etc. for each OO language. If an object-oriented module is modified, it is proposed that the entire module conform to the guidance within this document. Further, it is useful to consider assessing the interfaces, interactions and side effects on unchanged modules to determine that there is no impact on other unchanged modules and their integration. See also IEC 61508-3:2010, Annex D.

This document is intended as a supplement to the existing requirements in the IEC 61508 series which continue to apply.

1 Scope

This part of IEC 61508, which is a Technical Report, makes a proposal as to which topics to consider and which methods and techniques to use when designing object-oriented software to ensure suitable quality for use in functional safety applications.

Object-oriented languages are perceived as "state-of-the-art" nowadays. Such languages seem to be excluded from use by several statements in IEC 61508-3. However there are additions in some tables such as in IEC 61508-3:2010, Table B.1, where notes are added under which their use might be justified. Such exceptions that would allow, for example, dynamic objects, name the main concerns such as memory allocation and predictable timing issues and guide the user to safe use of object-oriented languages. These considerations are taken up in this document to specify methods and techniques that allow the reduction of systematic faults to the levels required by the respective systematic capabilities.

This document is not intended to replace any part of IEC 61508-3. Rules that exist in IEC 61508-3 are valid here as well and are not repeated, including rules that concern:

- the software life cycle,
- involvement of the assessor,
- modularization,
- principle of information hiding,
- proving and conventional testing,
- basic aspects of documentation,
- low coupling and high cohesion,
- responsibilities and training of people,
- operational experience as described in IEC 61508-4 and IEC 61508-7.

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 61508-1:2010 *Functional Safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*

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