IEC TR 62246-3

Edition 1.0 2018-06

TECHNICAL REPORT

colour inside

Reed switches –
Part 3: Reliability data for reed switch-devices in typical safety applications

IEC TR 62246-3:2018-06(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 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 - 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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions 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 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 TR 62246-3

Edition 1.0 2018-06

TECHNICAL REPORT

colour inside

Reed switches –
Part 3: Reliability data for reed switch-devices in typical safety applications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.120.70

ISBN 978-2-8322-5811-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

REED SWITCHES –

Part 3: Reliability data for reed switch-devices in typical safety applications

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 62246-3, which is a Technical Report, has been prepared by IEC technical committee 94: All-or-nothing electrical relays.

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

Draft TR	Report on voting
94/425/DTR	94/429/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.

A list of all parts in the IEC 62246 series, published under the general title *Reed switches*, 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 "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

This Technical Report:

– provides reliability data for reed switch-devices applied to machinery systems and also E/E/PE systems;

– selects typical safety applications for reed switch-devices according to the requirements from typical group safety standards;

– selects references, terms and definitions for machinery systems, E/E/PE systems and reed switch-devices, lifecycle activities, safety integrity and performance level, failures and safety measures for the reed switch-devices from typical group safety standards;

– addresses a way to share the responsibility on the components in the life cycle phases;

– addresses the application of IEC 62246 (all parts);

– considers the relation between safety requirements for the system from industrial standards and basic safety measures for the reed switch-devices of a single E/E/PE safety-related system and for two E/E/PE safety-related systems operating in:

  • a low demand mode of operation,

  • a high demand or continuous mode of operation.

– considers usage conditions at the end-user side:

  • environmental conditions for reed switches' use;

  • proof test period;

  • preventive maintenance.

– considers usage conditions at the E/E/PE system manufacturer side:

  • switching load;

  • failure mode;

  • diagnostic coverage for reed switch-devices.

– considers usage conditions at the component manufacturer side:

– considers how to evaluate the risk of the reed switch-devices fault occurrence based on the requirements from ISO 13849 (all parts), IEC 62061 and IEC 61508 (all parts):

– addresses a way to calculate reliability data of the reed switch-devices based on the requirements from ISO 13849 (all parts), IEC 62061 and IEC 61508 (all parts)

– analyses dangerous failure rates, B_{10D} values of the reed switch-devices according to the switching loads;

– calculates dangerous failure rates of the reed switch-devices based on usage rate per year;

– considers long-term field demonstration tests and operating experiences of the systems.

REED SWITCHES –

Part 3: Reliability data for reed switch-devices in typical safety applications

1 Scope

This part of IEC 62246, which is a Technical Report, provides basic technical background and experience about reliability data for reed switch-devices applied to machinery systems as well as E/E/PE safety-related control systems during the life cycle phases in general and industrial safety applications.

The document selects typical safety applications from group safety standards, and includes national safety standards and regulations accordingly. This document shows major reliability aspects for a proper design according to the standards, but it does not cover all details of an individual design. The responsibility for the verification of system design remains with the system integrator/manufacturer.

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 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*
IEC 62061:2005/AMD1:2012
IEC 62061:2005/AMD2:2015

IEC 62246-1-1:2018, *Reed switches – Part 1-1: Generic specification – Blank detail specification*

ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13849 (all parts), IEC 62061, IEC 61508 (all parts), and 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 Failure of systems

3.1.1
average probability of failure on demand
PFD_{avg}
mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specific safety function when a demand occurs from the EUC or EUC control system

Note 1 to entry: The mean unavailability over a given time interval [t1, t2] is generally noted by U (t1, t2).

Note 2 to entry: Two kind of failures contribute to PFD and PFD_{avg}: the *dangerous undetected failures* that have occurred since the last proof test and genuine *on demand failures* caused by the demands (proof tests and safety demands) themselves. The first one is *time dependent* and characterized by their dangerous failure rate λ_{DU} (t) whilst the second one is dependent only on the number of demands and is characterized by a *probability of failure per demand* (denoted by γ).

Note 3 to entry: As genuine on-demand failures cannot be detected by tests, it is necessary to identify them and take them into consideration when calculating the target failure measures.

[SOURCE: IEC 61508-4:2010, 3.6.18]

3.1.2
probability of dangerous failure per hour
PFH
average probability of dangerous failure per hour in a safety-related control system or subsystem

[SOURCE: IEC 61508-4:2010, 3.6.19, modified – Replacement of "of an E/E/PE safety related system to perform the specified safety function over a given period of time" by " per hour in a safety-related control system or subsystem" and deletion of the notes to entry.]

3.2 Confirmation of safety measures for reed switch-devices

3.2.1
proof test period
periodic test performed to detect failures in a reed switch-device so that, if necessary, the reed switch-device can be restored to an “as new” condition or as close as practical to this condition

Note 1 to entry: The effectiveness of the proof test will be dependent upon how close to the “as new” condition the system is restored. For the proof test to be fully effective, it will be necessary to detect 100 % of all dangerous failures. Although in practice 100 % is not easily achieved for other than low-complexity E/E/PE safety-related systems, this is the target. As a minimum, all the safety functions which are executed are checked according to the E/E/PE safety requirements specification. If separate channels are used, these tests are done for each channel separately.

Note 2 to entry: The proof test is not always usable. For example, for reed relays in E/E/PE systems, functional operating characteristics are confirmed according to the periodic proof tests by end-users.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – The term "proof test" has been replaced by "proof test period" and the entire definition and notes to entry have been redrafted.]

3.2.2
diagnostic coverage
DC
fraction of dangerous failures detected by automatic on-line diagnostic tests

Note 1 to entry: The fraction of dangerous failures is computed by using the dangerous failure rate associated with the detected dangerous failures divided by the total rate of dangerous failures

Note 2 to entry: The value of DC is given in four levels (see Table 1).

Table 1 – Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC
NOTE The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508 (all parts)) dealing with diagnostic coverage of tests. Investigations show that (1 – DC) rather than DC itself is a characteristics measure for the effectiveness of the test. (1 – DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called “none”. A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.	

[SOURCE: ISO13849-1:2015, 4.5.3]

3.2.3
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level

Note 1 to entry: Field experience is one of the techniques and measures to avoid faults during E/E/PE system integration and E/E/PE system safety validation. Field experience is referred to as “effectiveness low” in case of a) and “effectiveness high” in case of b) respectively:

a) With no serious failure in terms of experience for at least one year, over at least ten pieces of equipment with an operating time of 10 000 h, and different fields of use, 95 % of statistical correctness, and safety;

b) Detailed documentation of all changes (including minor changes) under experience for at least two years, over at least ten pieces of equipment with an operating time of 10 million hours, and different fields of use, 99,9 % of statistical correctness, and past operation.

Note 2 to entry: "proven in use" is not always usable. For example, applications referred to in IEC 61508 (all parts) are confirmed based on field feedback data.

[SOURCE: IEC 61508-4:2010, 3.8.18, modified – Addition of the notes to entry.]

3.2.4
common cause failure
CCF
failures of different items, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: Common cause failures should not be confused with common mode failures (see ISO 12100-1:2003, 3.34).

3.3 Reliability data of reed switch-devices

3.3.1
dangerous failure
failure of element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode); or

b) decreases the probability that the safety function operates correctly when required

Note 1 to entry: For reed switch-devices, it means OFF failure (failure to open) in high demand mode of operation or continuous mode of operation and ON failure (failure to close) in low demand mode of operation.

Note 2 to entry: For reed switch-devices, it means that the OFF-failure (failure to open) in the high demand or continuous mode of operation and the ON-failure (failure to close) in the low demand mode of operation can be a dangerous failure for the achievement of an invariable safe-state, and both of the OFF- and ON-failures can be a dangerous failure for the achievement of an intrinsically variable safe-state.

Note 3 to entry: Invariable safe-state is the state of the overall system in which the safety control-system concerned can be in one of the activated or inert state to achieve the safe state of the overall system, and the intrinsically variable safe-state is the state of the overall system in which the safety control-system has to change its own state from the activated to the inert or from the inert to the activated or both to achieve the safe state of the overall system.

Note 4 to entry: Activated state is in the lower degree of disorder (i.e., the higher degree of order) and the inert state is in the higher degree of disorder. The measure of disorder of a system is entropy that is also a measure of the "multiplicity" associated with the system state.

[SOURCE: IEC 61508-4:2010, 3.6.7, modified – Addition of the notes to entry.]

3.3.2
B_{10D} value
number of cycles until 10 % of the components have a dangerous failure

Note 1 to entry: The B_{10D} value will be specified by the manufacturer of safety devices.

[SOURCE: ISO 13849-1:2015, Table 1]

3.4 Functional safety of reed switch-devices

3.4.1
element safety function of reed switch-device
function to open and/or close as the input and output devices within the stated safety accuracy in accordance with the following a) to c) applications:

a) the reed switch-device operating its element safety function to materialize an invariable safe state;

b) the reed switch-device operating its element safety function to materialize an intrinsically variable safe state;

c) the reed switch-device operating element safety functions to materialize reciprocally variable safe states

Note 1 to entry: An OFF failure (failure to open) of the form A contact can be a safe failure, an ON failure (failure to close) of the form A contact can be a dangerous failure, an OFF failure (failure to open) of the form B contact can be a dangerous failure, and ON failure (failure to close) of the form B contact can be a safe failure regardless of modes of operation.

Note 2 to entry: For example, a stationary machine is often a safe state for a machinery production system.

Note 3 to entry: All the failure modes of the form A and B contacts can be dangerous failure modes regardless of modes of operation because the reed switch-device has to repeat to contact and open appropriately according to circumstances.

Note 4 to entry: An automated steering gear for automobiles controls variable safe courses in accordance with circumstances, i.e., a variable safe state to prevent collisions.

Note 5 to entry: Any failure mode of the form A and B contacts can be dangerous to one of the safe states but safe to another safe state regardless of modes of operation because the safe states are mutually reciprocal, i.e., a safe open state of contact that can be a dangerous state for another contact and a dangerous closed state of contact that can be a safe state for another contact.

Note 6 to entry: For example, an explosion of air bags for automobiles is a safe situation when an auto crashes but an unexpected explosion is a dangerous situation when the auto is running normally.