IEC TR 62246-3

Edition 1.0 2018-06

TECHNICAL REPORT

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 It also gives information on projects, replaced and withdrawn publications.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

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

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

REED SWITCHES –

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

FOREWORD

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.

3.4.2
SIL capability of function unit(s)
characteristic of a function unit(s) to which the capability of SIL 1, 2, 3 or 4 is allocated

Note 1 to entry: The allocation is done respectively under specified conditions and circumstances in accordance with IEC 61508-2 and IEC 61508-3.

[SOURCE EC 60079-29-3:2014, 3.15, modified – Addition of "of function unit(s)" in the term.]

4 Approach adopted for this document

4.1 General

The approach adopted is to raise the following necessities.

In fields such as process industries, machine manufacturing industries, transportation, general household electrical appliances applying reed switch-devices, there is a growing demand for functional safety assessment (FSA).

Reed switch manufacturers should do some assessment of their final assembly (reed switch-devices) and provide important reliability data relating to their reed switch-devices to other product manufacturers, system integrators or users.

This document describes the process which should be applied in accordance with the structure of the applications described in this document.

4.2 Application of reed switches in accordance with IEC 62246 (all parts)

When applying reed switches into the following specific products as switching elements, the contact ratings are intended to be used in conjunction with IEC 62246-1-1:2018 unless otherwise specified in the detail specifications:

a) reed relays:

   electromechanical control circuit devices, consisting of reed switches and coil fitting into a housing which could be plastic or metal (see IEC 61810-1:2015 and IEC 61811-1:2015);

b) reed switches for electromechanical control circuit devices, consisting of reed switches and magnet actuator fitting into a housing which could be plastic or metal (see IEC 60947-5-1:2016);

c) magnetic proximity switches:

   electromechanical control circuit devices without external power supply, consisting of reed switches and magnet actuator, either separated or in the same housing which could be plastic or metal; they can detect the presence of magnetic objects without contact (see IEC 60947-5-2:2007);

d) magnetic safety switches:

   guard interlocking devices that are designed to protect both people and machines, consisting of reed switches, overcurrent protection, non-coded or coded magnet actuator in a separate housing which could be plastic or metal (see IEC 60947-5-3:2013 and ISO 14119:2013);

e) reed sensors:

   electromechanical control circuit devices built using reed switches with additional functionalities such as the ability to withstand higher shock, easier mounting, additional intelligent circuitry, etc. (see IEC 60947-5-9:2006).

EXAMPLE 1 Shock reed sensor: a ring magnet is mounted on a very precise tension spring and this assembly is slid over a reed switch. Depending on the impact to trigger the reed switch, different tension springs are used.

EXAMPLE 2 Thermal reed sensor: a reed switch is enclosed in special ferrite compound which loses its magnetic permeability at its Curie temperature, and is sandwiched between two permanent magnets.

EXAMPLE 3 Pressure reed sensor: a magnet actuator in mounted on a very precise tension spring and this assembly is a distance away from a reed switch. Pressure drops cause the spring with attached magnet actuator to move towards the reed switch, causing the contacts to close.

4.3 Application in accordance with ISO 13849 (all parts), IEC 62061 and IEC 61508 (all parts)

Reed switch-device manufacturers should provide reliability data such as λ_{D1} values when they are applied into machinery systems based on the requirements from ISO 13849-1 and IEC 62061.

When applied into E/E/PE systems, where no application sector standard exists, they should provide reliability data such as field failure rates: λ_s, λ_{D2} and SFF based on the requirements from IEC 61508 (all parts).

4.4 Application of the design of the E/E/PE safety-related system

The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, programmable electronics, ASICs, embedded software, application software, data, etc.), shall meet all of the following requirements (see Table 2, Table 3 and Table 4).

For hardware safety integrity, these include:

– the architecture constraints on hardware safety integrity, and
– the requirements for quantifying the effect of random failures.

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safety failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % to < 90 %	SIL 2	SIL 3	SIL 4
90 % to < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 Refer to IEC 62061 which gives SIL3 max. and PL e and category 4, however when using IEC 61508 (all parts), it is possible to achieve SIL 4 only.

NOTE 2 This table is based on IEC 61508-2:2010, Table 2.

Table 3 – Performance level

PL	Average probability of dangerous failure per hour [PFH_D]
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

NOTE This table is based on ISO 13849-1:2015, Table 3.

Table 4 – Architectural constraints on subsystems: maximum SIL that can be claimed for a safety-related control function (SRCF) using this subsystem

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed (for exception see Note 3)	SIL 1	SIL 2
60 % to < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 2	SIL 3	SIL 3 (see Note 2)
≥ 99 %	SIL 3	SIL 3 (see Note 2)	SIL 3 (see Note 2)

NOTE 1 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this document. For SIL 4 see IEC 61508-1.

NOTE 3 See IEC 62061:2005 and IEC 62061:2005/AMD2:2015, 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see IEC 62061:2005, IEC 62061:2005/AMD1:2012 and IEC 62061:2005/AMD2:2015, 6.7.7.

NOTE 4 This table is based on IEC 62061:2005, Table 5.

4.5 Application of SIL capability to function units

4.5.1 General

The procedures to allocate SIL capability to function units of reed switch-devices are intended to be specified based on the agreement between system and reed switch-devices manufacturers for the realization of an E/E/PE safety-related system.

4.5.2 Procedures

The allocation of SIL capability to function units of the component is intended to meet the following requirements a) to c):

a) those for quantifying the effect of random hardware failures, i.e., IEC 61508-2:2010, 7.4.5;

b) safety function(s) and element safety function(s) are identified and designated for the allocation of SIL capability to the element safety function concerned taking three types of safe system states, i.e., invariable, intrinsically variable and reciprocally variable safe states into consideration;

c) those for the avoidance of systematic faults, i.e., IEC 61508-2:2010, 7.4.6.

4.5.3 Random hardware failures

To quantify the effect of random hardware failures, the following a) and b) are intended to be required:

a) the failure modes of the element due to random hardware failures (that are detected or not detected by diagnostic tests);

b) for every failure mode, an estimated failure rate with respect to specified operating conditions.

Any of 1) to 3) can be applied to the evaluation procedure:

1) implementation of a failure modes and effects analysis (FMEA) of the design using element failure data from a recognized industry source(s) (see IEC 61508-2:2010, 7.4.9.5 a)); or

2) experience of the previous use of the element in a similar environment(s) (see IEC 61508-2:2010, 7.4.10); or

3) evidence that the equipment is proven in use (see IEC 61508-2:2010, 7.4.10.1).

4.5.4 Systematic faults

To quantify the effect of systematic faults, the following a) and b) are intended to be required (see IEC 61508-2:2010, 7.4.2.2 c)):

a) failure modes owing to the following:
   - residual design and manufacturing faults in the component,
   - residual installation faults in the component,
   - human-errors in the operation of the component,
   - environmental stresses, including electromagnetic disturbances applied to the component (see IEC 61508-2:2010, 7.4.7.1. b)).

b) for every failure mode, an estimated failure rate.

Any of 1) to 3) can be applied to the evaluation procedure:

1) evidence that the equipment is proven in use; or
2) effects analysis from authorized industry data sources; or
3) experience of the previous use of the element in a similar environment (see IEC 61508-2:2010, 7.4.10).

4.5.5 Safety manual

It will be necessary for a supplier of a component, claimed as being compliant with IEC 61508 (all parts), to calculate random hardware failure rates available to the designer of an E/E/PE safety-related system in the component safety manual, see see IEC 61508-2:2010, 7.4.9.4 and Annex D.

De-rating should be considered. Justification for operating at the limits shall be documented (see IEC 61508-2:2010, 7.4.2.13).

4.5.6 Application of SIL capability for the allocation of SIL to systems

In order to allocate SIL to the overall systems, PFD_{avg} for the low demand mode of operation and PFH for the high demand mode and continuous mode of operation could be calculated based on the formulas shown in IEC 61508-6 using dangerous failure rates in accordance with the requirements provided in 4.5.1 and 4.5.2, taking the following metrics into account:

1) arrangement of dangerous and safe failure modes for ON/OFF failures;
2) safe failure fraction (SFF);
3) hardware fault tolerance (HFT);
4) diagnostic coverage (DC);
5) proof testing duration (T);
6) common cause failure (CCF): beta (β) factor.

5 Examples of reliability data for reed switch-devices

Examples of safety systems applied to reed switch-devices operating in a low demand operation, in a high demand operation or continuous mode of operation, safety and reliability requirements are given in Clauses 1 of Annexes A to F.

Typical group safety and industrial standards, national standards and regulations are selected in Clauses 2 of Annexes A to F.

Typical safety applications, architectures and control circuits of reed switch-devices are given in Clauses 3 of Annexes A to F.

Usage conditions of end-users, E/E/PE system manufacturers and reed switch-device manufacturers are given in Clauses 4 of Annexes A to F.

Failure rates based on the requirements from ISO 13849-1 and IEC 62061 or field failure rates and safety failure fraction based on the requirements from IEC 61508 (all parts) are given in Clauses 5 of Annexes A to F.

Examples of accident damage reduction are given in Annex C.

6 Examples of classification of involved groups for responsibility

In order to successively set up the maintenance cycle and the basis for safety requirements for each phase of the life cycle, examples of classification of involved groups for responsibility are given in Clauses 6 of Annexes A to F.

Annex A
(informative)

Hydraulic and pneumatic fluid power

A.1 Example of electric actuator in hydraulic fluid power

This application is a typical example of a two-channel system which is used to achieve a higher safety level for a high demand or continuous mode of operation in accordance with the industrial standards listed in Clause A.2.

Cylinder equipment detects the position of a piston which performs motion control of an electric actuator within a mechanical control system.

A.2 Examples of group safety standards

ISO 4413, *Hydraulic fluid power – General rules and safety requirements for systems and their components*

ISO 4414, *Pneumatic fluid power – General rules and safety requirements for systems and their components*

The standards mentioned above specify the use of sequence and position detection. When there is a possibility that a functional defect of pressure control or time control can generate danger or damage in itself, position detection is used.

A.3 Example of safety requirements

The safety-related-control system of a servo press shall be category 4 according to ISO 13849-1:2015. Categories 2 or 3 can be selected according to the risk assessment standard, JIS B 6410:2009, 5.3.

A.4 Example of safety measures for the reed switch-device

A.4.1 Usage conditions of end-user

The architecture of an electric actuator in hydraulic fluid power is shown in Figure A.1.

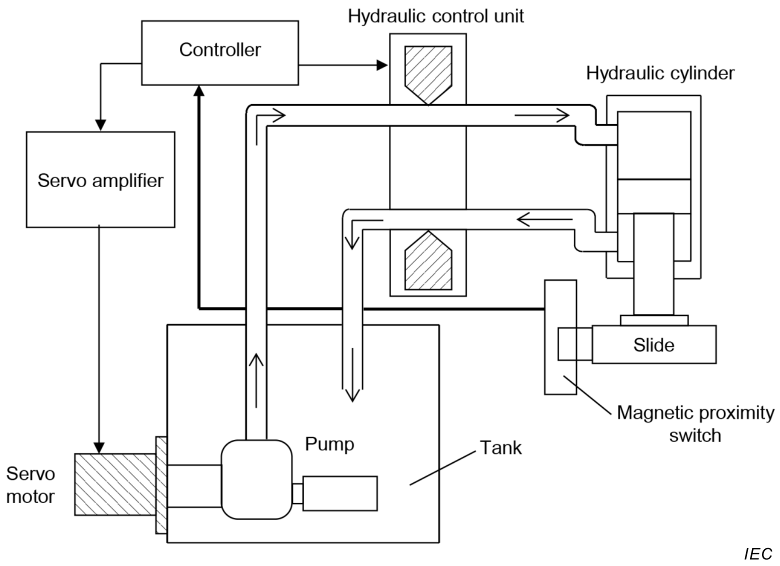


Figure A.1 – Architecture of an electric actuator in hydraulic fluid power

Based on the following technical information, reed switches are used for the contacts of magnetic proximity switches of the E/E/PE system:

– environmental conditions for reed switches' use: the switching load voltage and current of a magnetic proximity switch are signal level to detect the piston position and calculate a movement speed by the controller:
  - vibration: 10 mm $_{\text{p-p}}$ max., 10 Hz to 55 Hz (according to IEC 60068-2-6);
  - shock: 98 m/s^2 (10 g_n) max. (according to IEC 60068-2-27);
  - EMC: specified test levels (according to IEC 61000-4 (all parts));
  - ambient temperature: 0 °C to + 50 °C;

– the system suppliers demand MCTF or B_{10} value from equipment manufacturers;

– preventive maintenance: according to the MCTF or B_{10} value, users confirm and maintain safety by a daily check and replace the device after a specified number of operations.

A.4.2 Usage conditions of the reed switch-device

Usage conditions are specified as follows:

– Switching load: the switching load voltage and current (5 V DC, 1 mA max.) are signal level because the controller only detects the position and calculates a movement speed.

– Failure mode: when the switch is not magnetized, it is regarded as a disconnection of the switch, a cable, a power supply, etc., and it is considered failsafe.

– Diagnostic coverage for reed switches: in order to improve safety, the piston travel time between both switches is monitored by the controller.

The control circuit of reed switches of magnetic proximity switches is shown in Figure A.2.

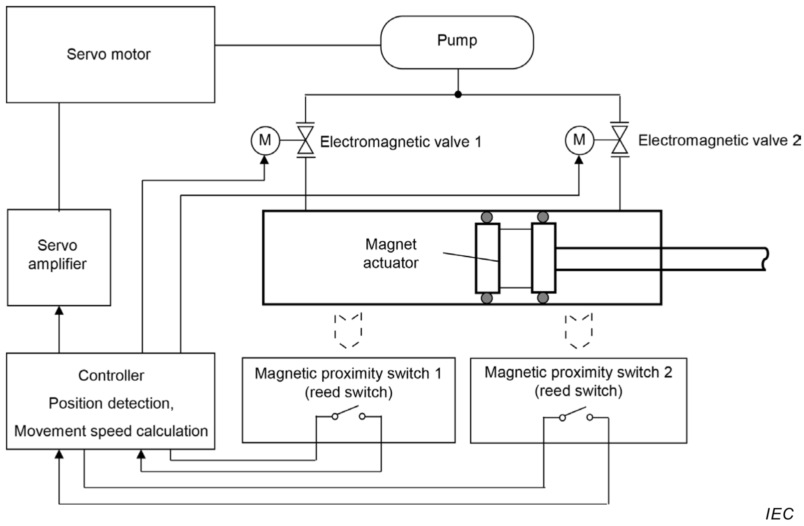


Figure A.2 – Control circuit of reed switches of magnetic proximity switches

A.5 Example of calculation of failure rates for the reed switch-device

A.5.1 Dangerous failure rate of the reed switch-device

$\lambda_{D1} = 5,79 \times 10^{-7}$ (1/h)

See ISO 13849-1:2015, Formula (C.5), where

n_{op} is 60 operations/h, 24 h/day, 360 days per year;

B_{10D} is 10 million cycles (see Figure A.3, estimation of B_{10D} according to IEC 61810-2-1 by the manufacturer of the magnetic proximity switch).

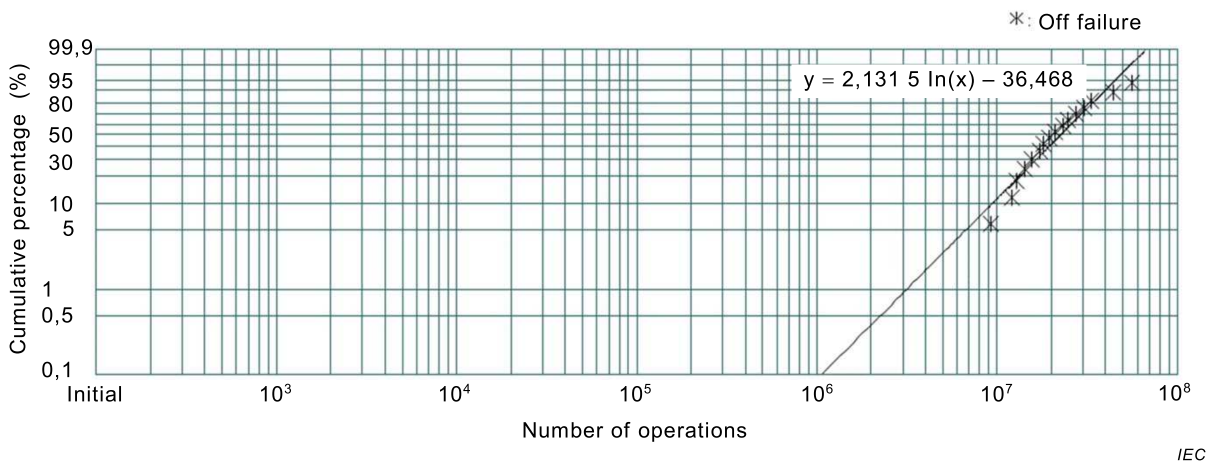


Figure A.3 – B_{10} value estimated by Weibull analysis

NOTE 1 10 switches corresponds to the failure mode 'failure to open' (OFF failure according to IEC 62246-1-1:2018, D.2.3).

NOTE 2 $B_{10D} = B_{10} \times \frac{10}{10}$

A.5.2 Estimates for diagnostic coverage (DC)

90 % to 99 %, indirect monitoring (e.g. monitoring by electrical position monitoring of actuators).

A.5.3 Estimates for common cause failure (CCF)

A comprehensive procedure for measures against CCF for the switches and separately for control logic is given, for example, in ISO 13849-2 and IEC 61508-6:2010, Annex D.

A.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table A.1.

Table A.1 – Possible sharing of responsibility on an electric actuator

Feature	Manufacturer of the reed switch	Manufacturer of the magnetic proximity switch	Manufacturer of E/E/PE systems according to ISO 13849 (all parts)	Manufacturer of the equipment (machine)	Owner/ user of the equipment (machine)	Operator of the equipment (machine)	Maintainer of the equipment (machine)
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	yes	yes	yes
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	yes	no
Replacement cycle	no	no	no	no	no	no	yes

[a] Contact ratings of reed switches standards are available. The B_{10D} value is specified by the manufacturer of safety devices.

[b] The architecture of the system is given by the design. The owner/user, operator and maintainer have to ensure that the given safety standard has not changed.

Annex B
(informative)

Safety of machinery

B.1 Example of guard interlocking device

This application is a typical example of a dual channel system which is used to achieve higher safety performance in accordance with the industrial standard listed in Clause B.2.

In order to improve the safety level, additional measures, such as an over-current protection device and dual channel monitoring system are included in the guard interlocking switches.

B.2 Example of group safety standards

ISO 14119, *Safety of machinery – Interlocking devices associated with guards – Principles for design and selection*

B.3 Example of safety requirements for the system

B.3.1 Description of Type 3 interlocking device – example

A Type 3 interlocking device consists of one or more non-mechanically actuated position switch(es) (magnetic switch) actuated by an uncoded actuator linked to a movable guard (see Figures B.1 and B.2).

To fulfil requirements for safety integrity in most cases, two single position switches with monitoring will be required unless the single position switch is designed to meet the requirements of IEC 60947-5-3 (see also ISO 14119:2013, 5.4).

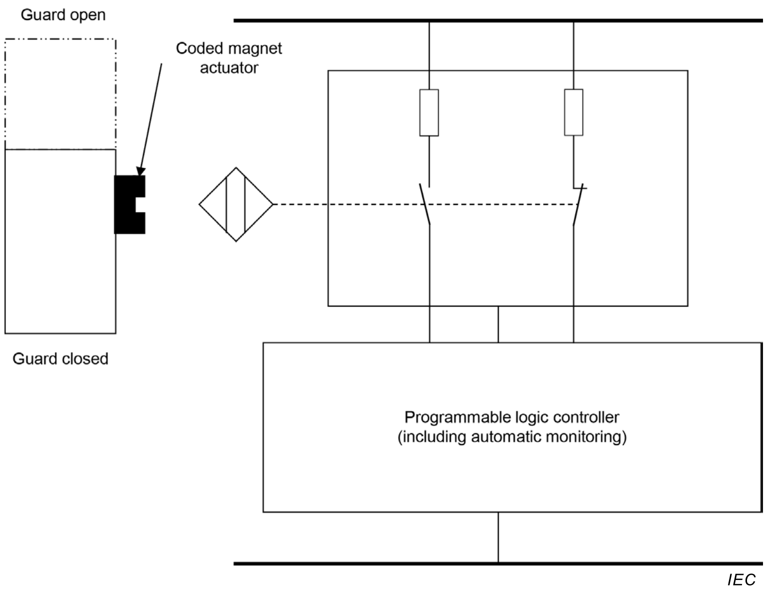


Figure B.1 – Electric interlocking device with a proximity switch actuated by a magnet actuator

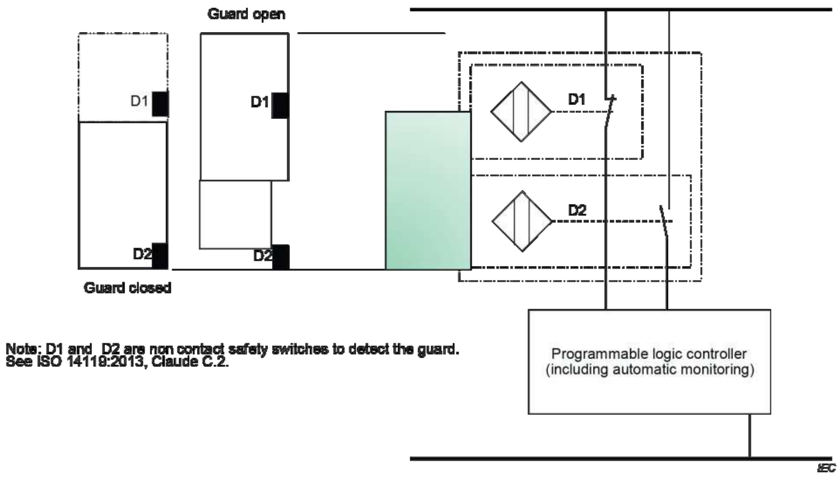


Figure B.2 – Electric interlocking device with two proximity switches

B.3.2 Typical characteristics

See ISO 14119:2013, Clause C.2.

– no moving parts;

– high resistance to dust, liquids;

– easily kept clean;

– due to the lack of coding, additional measures against defeating are required;

– limited application possibilities.

B.3.3 Remarks

For measures to minimize defeating, see ISO 14119:2013, Clause 7.

B.3.4 Description of Type 4 interlocking device – example

A Type 4 interlocking device with a position switch actuated by a coded magnet actuator associated with the movable guard opens its contacts when the guard is not closed (see ISO 14119:2013, Figure D.1).

B.3.5 Typical characteristics

- no moving parts;
- high resistance to dust, liquids;
- easily kept clean;
- due to the lack of coding, additional measures against defeating are required;
- limited application possibilities.

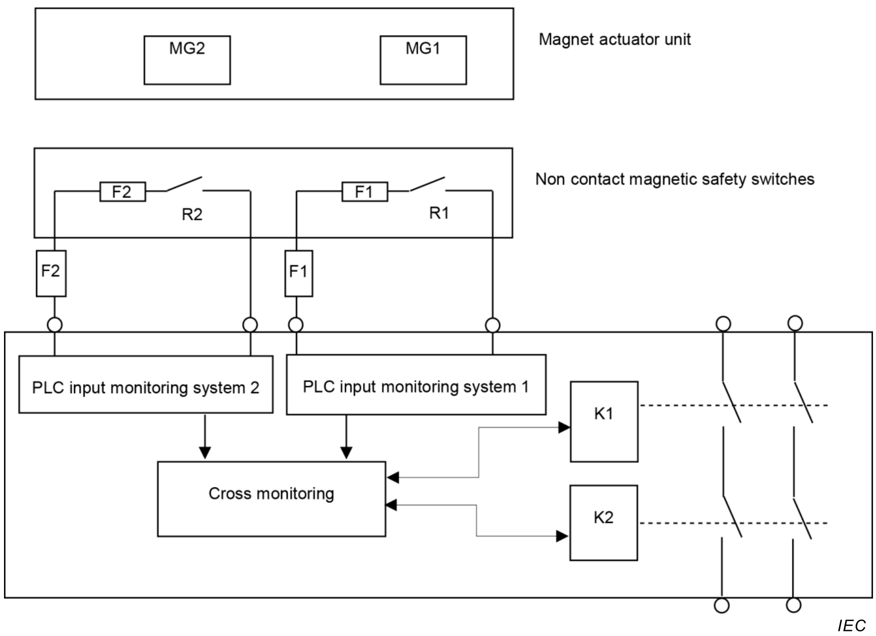
B.3.6 Remarks

For measures to minimize defeating, see ISO 14119:2013, Clause 7.

B.4 Example of safety measures for the reed switch-device

B.4.1 Usage conditions of end-user

A typical architecture is shown in Figure B.3.



Key

MG1, MG2	magnetic actuators
R1, R2	reed switches
F1, F2	contact welding protection devices (fuses a, b)
K1, K2	electromagnetic contactors
a	See IEC 62246-1:2015, 6.27, and IEC 62246-1-1:2018, Table 2, Test no. A.4.
b	See quick acting high breaking capacity fuse type FH in accordance with IEC 60127-2:2014, standard sheet 1.

Figure B.3 – Typical architecture of guard interlocking device

Based on the following basic technical information, reed switches are used for the contacts of non-contact magnetic safety switches that are designed to interlock hinged, sliding or removable guard doors:

– Environmental conditions for reed switches' use:
  - vibration: 10 mm $_{p-p}$ max., 10 Hz to 55 Hz (according to IEC 60068-2-6);
  - shock: 98 m/s^2 (10 g_n) max. (according to IEC 60068-2-27);
  - EMC: specified test levels (according to IEC 61000-4 (all parts));
  - ambient temperature: 0 °C to + 50 °C.
– Preventive maintenance: monthly – check alignment of actuator and look for signs of mechanical damage to the switch casing. Check wiring for signs of damage. Check each switch function by operating and closing each guard individually in turn and ensuring that the appropriate LEDs on the safety relay are illuminated when the switch is closed and are extinguished when the switch is open. Check that the machine stops and cannot be re-started when either switch is open. Never attempt to repair any switch, actuator or integral cables. Replace any switch displaying signs of mechanical damage to the casing or cables.

B.4.2 Usage conditions of the reed switch-device

The reed switches of guard interlocking devices are used under the following conditions:

– typical switching load: 24 V DC, 200 mA, inductive load;
– failure mode: when the switch is not magnetized, it is regarded as a disconnection of the switch, a cable, a power supply, etc., and it is considered failsafe;
– diagnostic coverage for reed switches: automatic monitoring by a programmable logic controller and cross-monitoring between the two systems are performed by the PLC.

B.5 Example of calculation of failure rates for the reed switch-device

B.5.1 General

According to the following evaluations, a dual channel interlock device specified in Figure B.3 is designed to meet performance levels PL e or PL d (according to ISO 13849-1:2015) and for use in a SIL 2 or SIL 3 system (according to IEC 62061:2005) depending on application characteristics when applying the basic safety measures specified in Clause B.4.

B.5.2 Dangerous failure rate of reed switch-device

$\lambda_{D1} = 6{,}00 \times 10^{-7}$ (1/h)

See ISO 13849-1:2015, Formula (C.5), where

n_{op} is the 10 operations/h, 24 h/day, 360 days per year;

B_{10D} is 2 million cycles (estimation of B_{10D} according to IEC 61810-2-1 by the manufacturer of the guard interlocking device).

B.5.3 Estimation for diagnostic coverage (DC)

99 %, cross monitoring of input signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits.

B.5.4 Estimates for common cause failure (CCF)

A comprehensive procedure for measures against CCF for the switches and separately for control logic is given, for example, in ISO 13849-2 and IEC 61508-6:2010, Annex D.

B.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table B.1.

Table B.1 – Possible sharing of responsibility on a guard interlocking device

Feature	Manufacturer of the reed switch	Manufacturer of the magnetic safety switch	Manufacturer of E/E/PE systems according to IEC 62061, ISO 13849 (all parts) and ISO 14119	Manufacturer of the equipment (machine)	Owner/ user of the equipment (machine)	Operator of the equipment (machine)	Maintai-ner of the equip-ment (machine)
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	yes	yes	yes
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	yes	no
Replacement cycle	no	no	no	no	no	no	yes

[a] Contact ratings of reed switches standards are available. The B_{10D} value is specified by the manufacturer of safety devices.

[b] The architecture of the system is given by the design. The owner/user, operator and maintainer have to ensure that the given safety standard has not changed.

Annex C
(informative)

Automatic electrical controls for household and similar use

C.1 Example of automatic electrical burner control system

This application is an example taken from Japan of a single channel system for a high demand or continuous mode of operation which is used to achieve a high safety level in accordance with the industrial standards in automatic electrical controls for household and similar use listed in Clause C.2.

A microcomputer type gas meter equipment is an automatic electrical burner control system which supervises measurement and the flow of gas. It also interrupts the flow of gas automatically at a specified time or in the event of an earthquake.

C.2 Examples of group safety standards

IEC 60730-2-5, *Automatic electrical controls – Part 2-5: Particular requirements for automatic electrical burner control systems*

National Japanese standard: *Legal performance standard (law enforcement standard Article 44)*

C.3 Example of safety requirements for the system

Gas meters incorporating automatic shut-off devices triggered by a gas flow sensor and/or seism scopes are a requirement in Japanese national standards.

The reed switch-device (flow sensor) is required for use in a single channel SIL 2 system according to IEC 62061:2005 as input sensor.

Table C.1 shows the basic safety functions which should behave as a safety system (in the event of emergency, detection methods and action to prevent all gas accidents).

Table C.1 – Detection methods and action in the event of emergency

	Emergency usage condition	Risk of accident	Detection method of gas situation	Judgement	Action	Effect
Basic safety system	gas leakage a large amount of gas →	gas explosion →	gas flow sensor (Gas meter) →	abnormal flow quantity →	automatic shut-down →	prevent all gas accidents
	forgot to erase →	gas poisoning fire →	gas flow sensor →	abnormal flow quantity →		
	earth-quake →	fire gas explosion →	seism scope →	more than a specified seismic coefficient →		

C.4 Example of safety measures for the reed switch-device

C.4.1 Usage conditions of end-user

The architecture of a microcomputer type gas meter equipment is shown in Figure C.1.

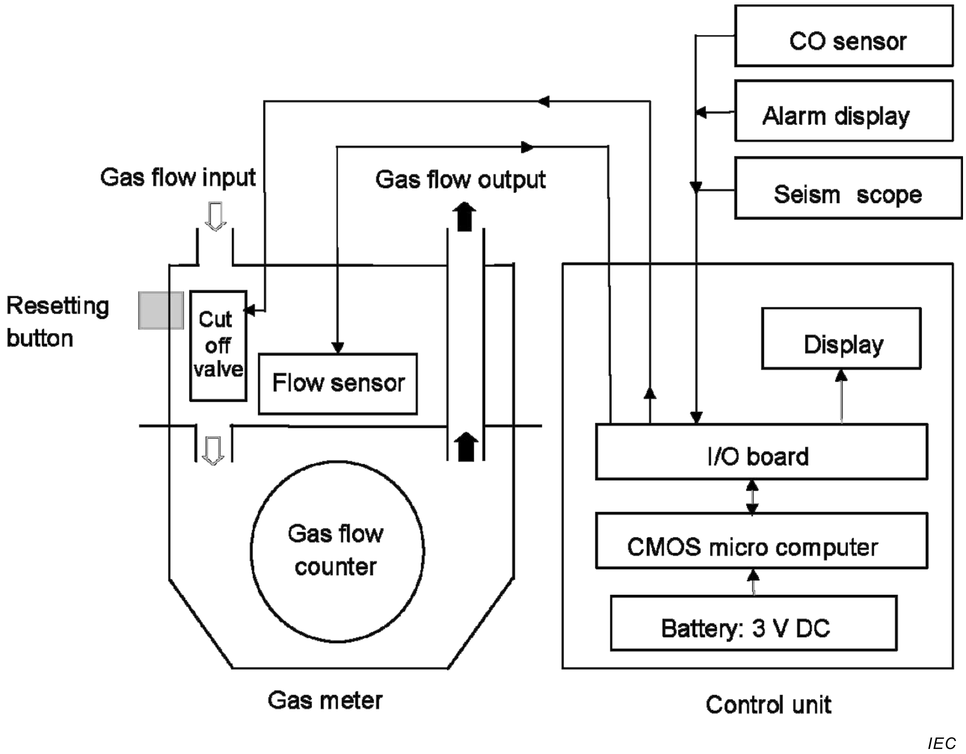


Figure C.1 – Architecture of a microcomputer type gas meter

Based on the following technical information, reed switches are used for the contacts of flow sensors which measure the gas flow of the equipment:

– environmental conditions for reed switches’ use:
  - vibration, shock: the microcomputer type gas meter shall shut-down automatically in the event of an earthquake with a seismic intensity greater than 5 on the 7-point Japanese scale;
  - EMC: withstand with level 2: 3 A/m and/or level 3: 10 A/m (according to IEC 61000-4-6);
  - ambient temperature:-30 °C to +40 °C;

– user checks that the interrupting device operates normally by operation of a controller as a daily check;

– proof test period: at least once a year, a test interruption with a seism scope or a gas-leak alarm machine is performed, to check that the interruption system operates normally;

– preventive maintenance: replacement after a period of 10 years is carried out.

C.4.2 Usage conditions of reed switch-device

Usage conditions are specified as follows:

- Switching load: the switching load voltage and current of a flow sensor are CMOS level (3 V DC, 30 μA max.) to interface with a microcomputer.
- Failure mode: disconnection of the switch, a cable, a power supply, etc. are taken into consideration; when the switch is not magnetized it is considered failsafe (it sends a signal to shut-down, triggers an alarm display and is therefore considered as a safe failure).
- Diagnostic coverage for reed switches: the count difference between a gas measurement and a flow sensor is monitored. It has at least one self-diagnostic function during a continuous mode of operation.

The control circuit of a reed switch in a flow sensor is shown in Figure C.2.

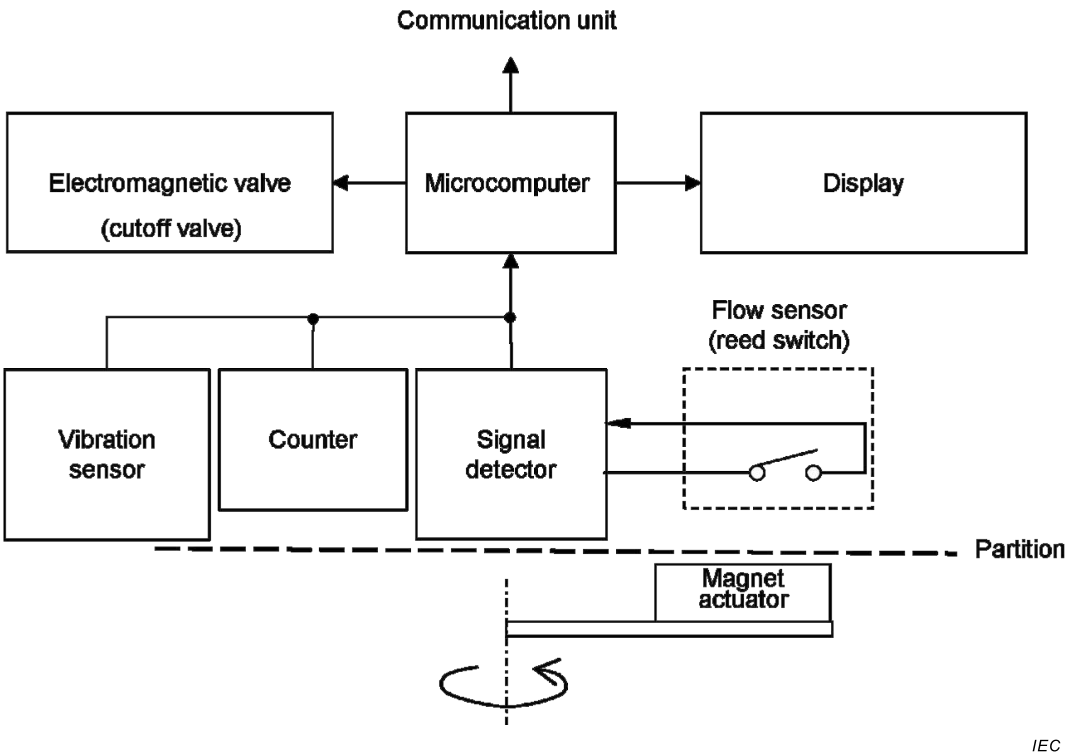


Figure C.2 – Control circuit of a reed switch in flow sensor

C.5 Example of calculation of failure rates for the reed switch-device

C.5.1 Dangerous failure rate of reed switch-device

$\lambda_{D1} = 5{,}79 \times 10^{-7}$ (1/h)

See ISO 13849-1:2015, Formula (C.5), where

n_{op} is the 1 200 operations/h, 24 h per day, 360 days per year;

B_{10D} is 100 million cycles (estimation of B_{10D} according to IEC 61810-2-1 by the manufacturer of the flow sensor).

C.5.2 Estimates for diagnostic coverage (DC)

90 %, cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O).

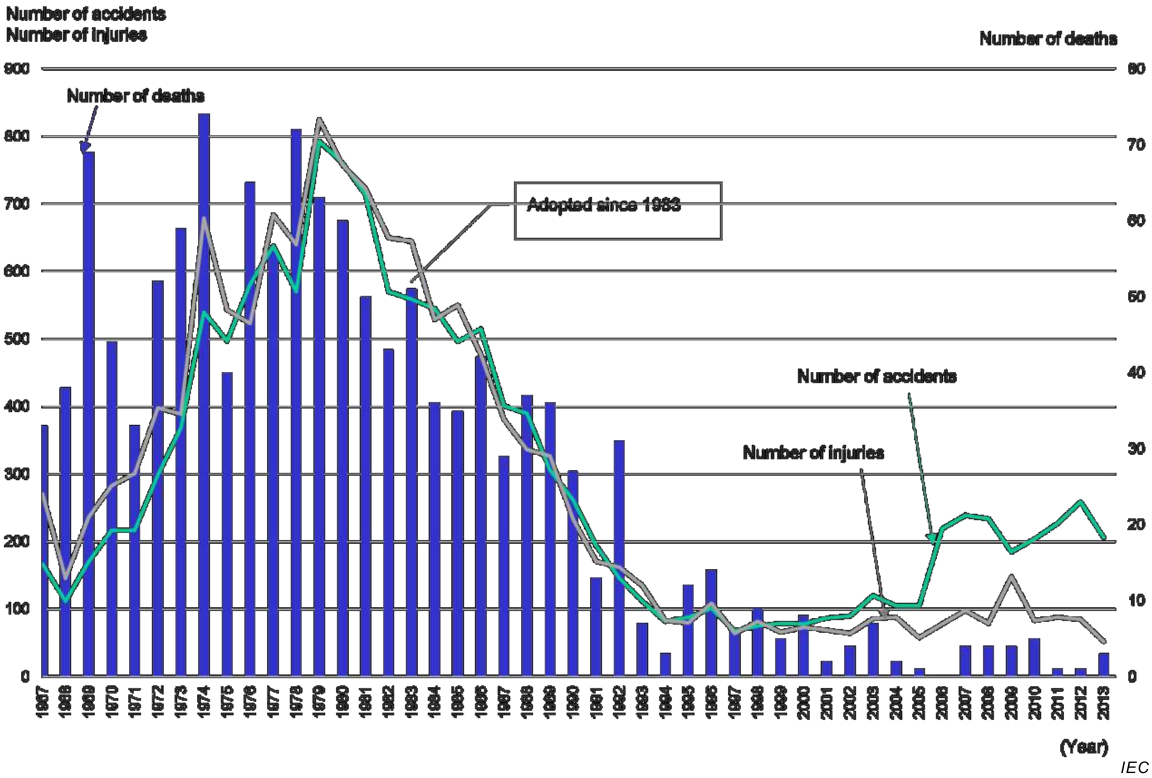
C.5.3 Estimates for common cause failure (CCF)

A comprehensive procedure for measures against CCF for the switches and separately for control logic is given, for example, in ISO 13849-2 and IEC 61508-6:2010, Annex D.

C.5.4 Accident damage reduction

Figure C.3 shows occurrences of fatality and injury LPG accidents in the past in Japan.

The occurrences of fatality and injury LPG accidents have been decreasing since 1993 when the microcomputer type gas meter equipment which carried reed switches were adopted.



SOURCE: Reproduced from the *Annual report on liquefied petroleum gas (LPG) related accidents* (2013 version) with the permission of the High Pressure Gas Safety Institute of Japan (KHK).

Figure C.3 – Accident occurrences and casualties by year (Japan)

C.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table C.2.

Table C.2 – Possible sharing of responsibility on microcomputer type gas meter

Feature	Manufacturer of the reed switch	Manufacturer of the magnetic proximity switch	Manufacturer of the E/E/PE systems according to IEC 62061	Manufacturer of the equipment (machine)	Owner/ user of the equipment (machine)	Operator of the equip-ment (machine)	Maintainer of the equip-ment (machine)
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	no	no	no
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	no	yes
Replacement cycle	no	no	no	no	no	no	yes

[a] Contact ratings of the reed switches standards are available. The B_{10D} value is specified by the manufacturer of safety devices.

[b] The architecture of the system is given by the design.

Annex D
(informative)

Household and similar electric appliances

D.1 Example of automatic electric washing machine

This application is a typical example of a two-channel architecture for a high demand or continuous mode of operation which is used to achieve high safety level in accordance with the industrial standards for household and similar electrical appliances listed in Clause D.2. This application effects an emergency brake application, if the permissible lid opening is exceeded in an automatic electric washing machine.

The lid detecting device of an automatic washing machine refers to the equipment which controls rotation of the laundry drum, by stopping or rotating the drum or preventing it starting to rotate when the lid is opened.

D.2 Examples of group safety standards

IEC 60335-1, *Household and similar electrical appliances – Safety – Part 1: General requirements*

IEC 60335-2-4, *Household and similar electrical appliances – Safety – Part 2-4: Particular requirements for spin extractors*

IEC 60335-2-7, *Household and similar electrical appliances – Safety – Part 2-7: Particular requirements for washing machines*

D.3 Example of safety requirements for the system

The reed switch-device (reed switch) is required for use in a single channel SIL 2 system according to IEC 62061:2005 as input sensor.

D.4 Example of safety measures for the reed switch-device

D.4.1 Usage conditions of end-user

The architecture of an automatic electric washing machine is shown in Figure D.1.

Based on the following basic technical information, reed switches are used for the contacts of magnetic proximity switches which detect the lid position of these machines:

– Environmental conditions for reed switch use: since the switching load voltage and current of a lid detection switch are TTL level to interface with a microcomputer, contact welding does not take place. Moreover, in order to improve safety, when the lid opens more than a specified distance, a brake is applied directly to the motor and the rotation is stopped immediately:
  - vibration: N/A;
  - shock: 0,5 J – 3 times. (according to IEC 60335-1);
  - EMC: specified test levels (according to IEC 61000-4 (all parts));
  - ambient temperature: N/A;

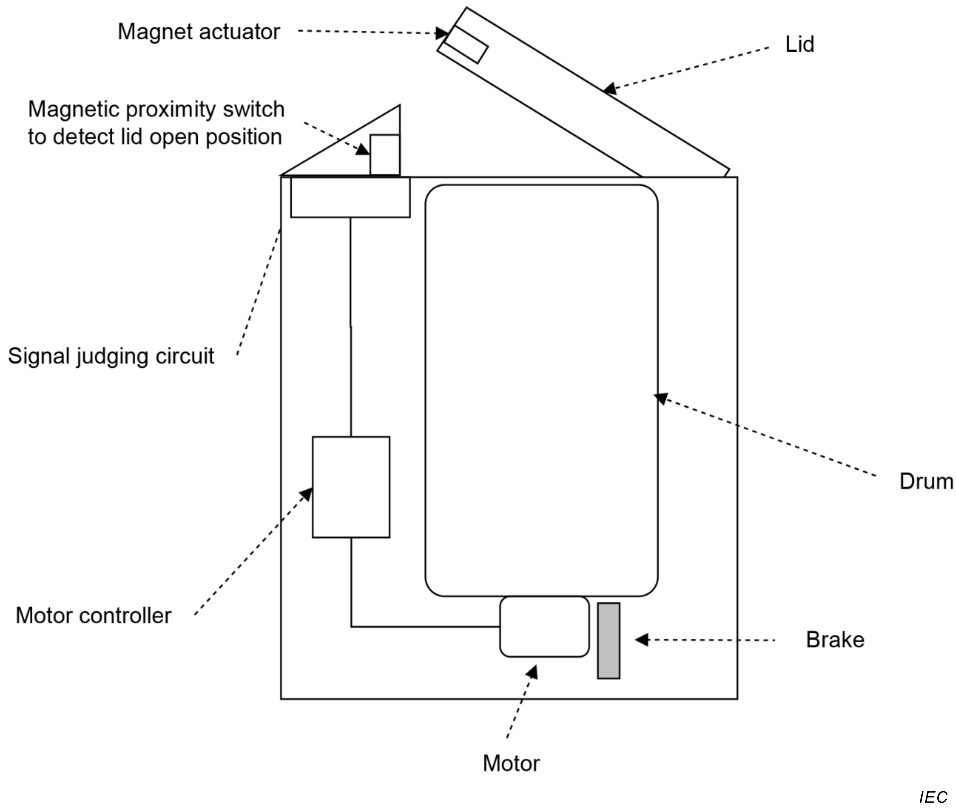


Figure D.1 – Architecture of an automatic electric washing machine

– Preventive maintenance: the automatic electric washing machine is replaced within 10 years to 16 years.

D.4.2 Usage conditions of reed switch-device

Usage conditions are specified as follows:

– switching load: TTL level (5 V DC, 10 mA max.) to interface with a microcomputer;

– failure modes of poor contact of the lid detection switch, a cable, a power supply, etc. are taken into consideration; if the OFF state occurs without magnetization, it sends a signal to prevent motor operation and is therefore a safe failure;

– diagnostic coverage for reed switches: by the self-diagnosis of the microcomputer;

The control circuit of a magnetic proximity switch is shown in Figure D.2.

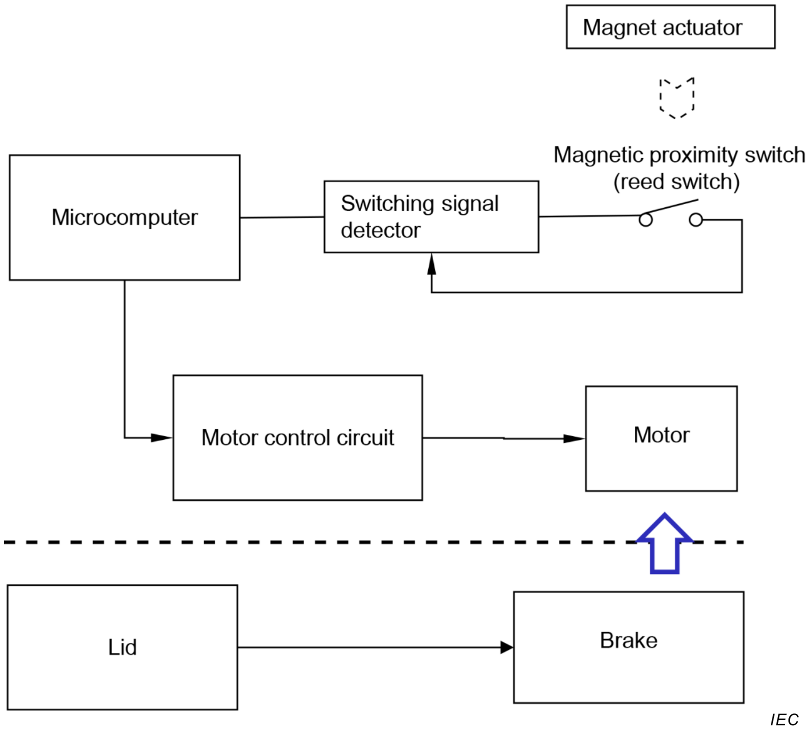


Figure D.2 – Control circuit of a magnetic proximity switch

D.5 Example of calculation of failure rates for the reed switch-device

D.5.1 Dangerous failure rate of reed switch-device

λ_{D1} = 5,97 × 10^{-8} (1/h)

See ISO 13849-1:2015, Formula (C.5), where

n_{op} is the 5 operations/h, 24 h/day, 360 days/year;

B_{10D} is 10 million cycles (estimation of B_{10D} according to IEC 61810-2-1 by the manufacturer of the magnetic proximity switch).

D.5.2 Estimates for diagnostic coverage (DC)

90 % to 99 %, indirect monitoring (electrical position monitoring of actuators).

D.5.3 Estimation for common cause failure (CCF)

A comprehensive procedure for measures against CCF for the switches and separately for control logic is given, for example, in ISO 13849-1 and IEC 61508-6:2010, Annex D.

D.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table D.1.

Table D.1 – Possible sharing of responsibility on an automatic electric washing machine

Feature	Manufacturer of the reed switch	Manufacturer of the magnetic proximity switch	Manufacturer of E/E/PE systems according to IEC 62061	Manufacturer of the equipment (machine)	Owner/ user of the equipment (machine)	Operator of the equip-ment (machine)	Maintai-ner of the equip-ment (machine)
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	no	no	no
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	no	no
Replacement cycle	no	no	no	no	no	no	no

[a] Contact ratings of reed switches standards are available. The B_{10D} value is specified by the manufacturer of the magnetic proximity switch.

[b] The architecture of the system is given by the design.

Annex E
(informative)

Electric power systems

E.1 Example of measuring and protection relay system

This application is an example taken from Japan of a single channel system for a low demand mode of operation which is used to achieve high safety levels and high reliability in accordance with the industrial standards for electric power systems listed in Clause E.2.

The measuring and protection relay is an equipment which issues control signals so that detected abnormal conditions such as a short-circuit to ground in power equipment, a transformer installed in electric power systems, a power line, or a substation, can be quickly (for example, 20 ms) separated from other healthy parts. Reducing the damage to the equipment is indispensable to a stable operation of an electric power system.

E.2 Industrial standards

IEC 60255-1, *Measuring relays and protection equipment – Common requirements*

JEC 2500, *Protection relays for electric power systems*

E.3 Safety requirements for the system – example

A safety related system having a SIL 3 (IEC 61508 (all parts)) with risk reducing measures based on risk assessment has been developed.

E.4 Safety measures for the reed switch device – example

E.4.1 Usage conditions of end-user

The architecture of a measuring and protection relay system is given in Figure E.1.

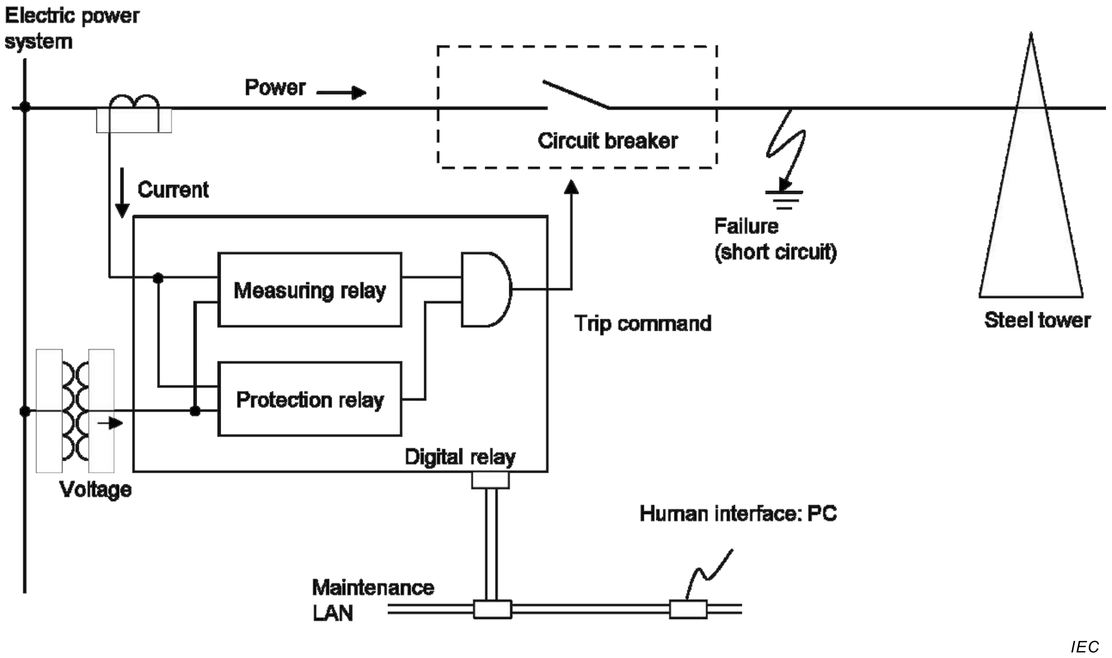


Figure E.1 – Architecture of a measuring and protection relay system

Based on the following technical information, reed switches are used for the contacts of trip command reed relays in measuring and protection relays designed for electric power systems:

– environmental conditions for reed switches' use: operation at high speed with high contact reliability is required since poor contact causes a dangerous failure, and a making capacity of several 10 s of A is needed:
  - vibration: according to IEC 60068-2-6;
  - shock: according to IEC 60068-2-27;
  - impulse voltage: 3 000 V between contacts, 4 500 V between input and output with 1,2 × 50 μs waveform;
  - ambient temperature: 0 °C to +40 °C;
– through a LAN, a PC is utilized to supervise the operating state of measuring and protection relay equipment, and the relay is replaced when necessary;
– proof test period: dependent on the users, the proof test cycle can be 6 years;
– preventive maintenance: under consideration.

E.4.2 Usage conditions of the reed switch-device

Usage conditions are specified as follows:

– Switching load: the highest contact reliability and quick response are required since a poor contact causes a dangerous failure:
  - operating time: less than 5 ms;
  - limiting making capacity: 10 000 times with 110 V DC, 15 A, 5 ms max. $L/R \leqq 5$ ms;
  - limiting breaking capacity: 100 000 times with 110 V DC, 0,3 A, $L/R = 40$ ms;

  NOTE Contact ratings are according to IEC 62246-1-1:2018, D.2.12.

– Diagnostic coverage for reed relays: automatic monitoring function using a processor.

The control circuit of a reed switch in a measuring and protection relay is shown in Figure E.2.

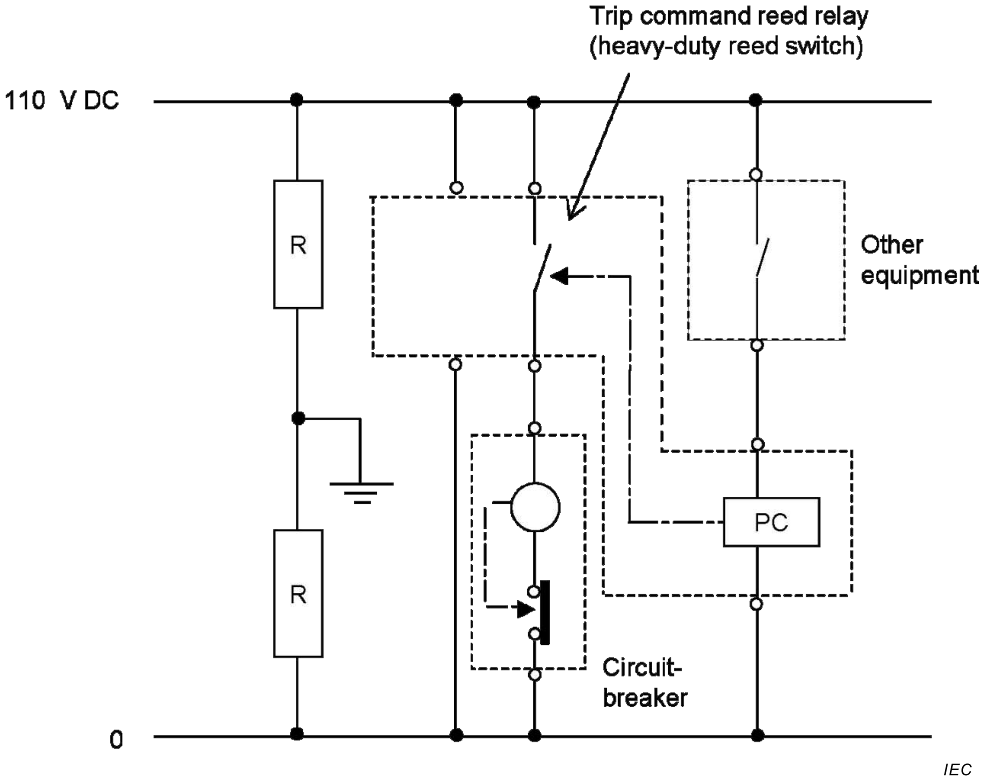


Figure E.2 – Control circuit of a reed switch in a measuring and protection relay

E.5 Example of the calculation of failure rates for the reed switch-device

The field failure rates are provided in use. The example of the field failure data based on the conditions according to Clause E.4 is shown in Table E.1.

Table E.1 – Failure rates of reed relays in a measuring and protection relay system

Symbol	Reliability data	Field failure rates
λ_s	Safety failure rate (1/h)	$9{,}9 \times 10^{-10}$
λ_{D2}	Dangerous failure rate （1/h）	$1{,}9 \times 10^{-9}$
NOTE 1 The filed failure rates and failure mode databases are accumulated results of $21{,}2 \times 10^9$ component hours of field data. NOTE 2 The accumulated operating time is 11 × 12 × 24 h (from 2004 to 2015, 24 hours a day).		

E.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table E.2.

Table E.2 – Possible sharing of responsibility on a measuring and protection relay system

Feature	Manufacturer of the reed switch	Manufacturer of the reed relay	Manufacturer of E/E/PE systems according to IEC 61508	Manufacturer of the equipment	Owner/ user of the equipment	Operator of the equip-ment	Maintai-ner of the equip-ment
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	yes	yes	yes
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	yes	no
Replacement cycle	no	no	no	no	no	no	yes

[a] The contact ratings of reed switches standards are available. Contact ratings are specified by the manufacturer of the measuring and protection relay.

[b] The architecture of the system is given by the design. The owner/user, operator and maintainer have to ensure that the given safety standard has not changed.

Annex F
(informative)

Railway application

F.1 Example of automatic train control (ATC) system

This application is an example taken from Japan of a two-channel system for a high demand or continuous mode of operation which is used to achieve the highest safety level and highest reliability in accordance with the group safety standards for railway signalling systems listed in Clause F.2. This automatic train control (ATC) system supports an emergency brake application if the permissible speed is exceeded by electric trains.

The automatic train control system requires accurate subsystems as all the operating actions are under the control of the system. That is true not only for the system itself but also for the outside data that will make it safe. This includes the speedometer system, the localization, the dynamic and static characteristics of the train, and line data. The system availability is also a dominant factor, so there will be no dramatic change in the fail-safe level with a degraded mode.

F.2 Examples of group safety standards

IEC 62278, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

IEC 62425, *Railway applications – Communication, signalling and processing systems Safety related electronic systems for signalling*

National standards: *The seventy-first article, Shinkansen super-express Bullet train structure regulation (Automatic train control equipment)*

F.3 Example of safety requirements for the system

The ATC system is a requirement in Japanese national standards.

A safety related ATC system having a SIL 4 with risk reducing measures based on risk assessment has been developed according to IEC 62278 and IEC 62425.

F.4 Example of safety measures for the reed switch-device

F.4.1 Usage conditions of end-user

The architecture of the automatic train control system is shown in Figure F.1.

Based on the following basic technical information, reed switches are used for the contacts of reed relays for use in emergency brake applications:

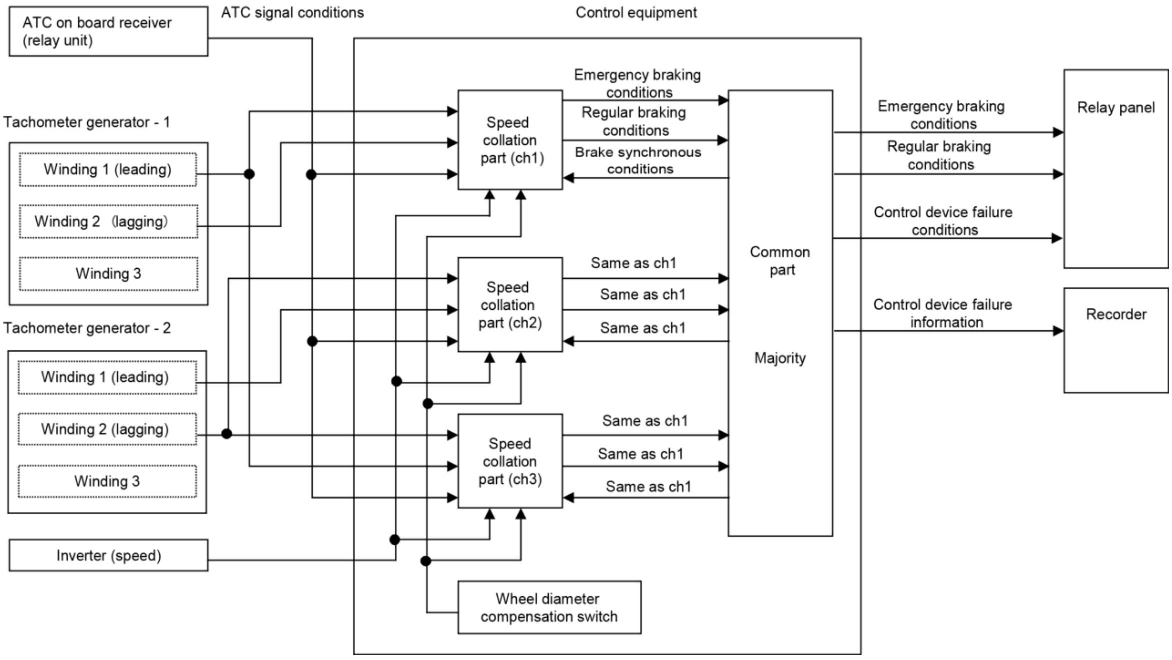
– Environmental conditions for reed switches' use: the reed relays are considered as a two-channel (regular brake and emergency brake) system with two contact pairs connected in series to avoid the risk that contact welding will cause a failure to open:
  - vibration: according to Category I, Class 2 of IEC 61373:2011;
  - shock: according to Category I, Class 2 of IEC 61373:2011;
  - EMC: specified test levels (according to IEC 61000-4 (all parts));
  - ambient temperature: –10 °C to +60 °C.

– Proof test period: several times a year by users.

NOTE 1 To prove the quality of reed relays in railway applications, operating voltage, release voltage and contact resistance are confirmed according to the periodic proof tests by end-users.

– Preventive maintenance: the automatic train control system is replaced within 10 years to 15 years.

NOTE 2 Based on the report for maintenance cycle of railway signalling devices, 2011-June, Japan Association of Signal Industries



NOTE Based on the architecture of ATS & ATC Railway signalling equipment, April 2012, Japan Railway Electrical Engineering Association.

Figure F.1 – Architecture of the automatic train control (ATC) system

F.4.2 Usage conditions of the reed switch-device

Usage conditions are specified as follows:

– switching load: 100 V DC, 230 mA, L/R = 15 ms inductive load with varistor;

NOTE 1 The contact ratings are according to IEC 62246-1-1:2018, D.2.10.

NOTE 2 n_{op}: usage rate of 360 days/year, 12 h/day, 20 operations/h, less than 100 000 operations/year.

– failure modes such as the disconnection of the relay coil, a cable, a power supply, etc. are taken into consideration; when the output relay is not magnetized, it is considered as a safe failure;

– diagnostic coverage for output including reed switches: the operating status is monitored continuously by CPUs and the failure information of the system is recorded on a paper tape.

NOTE 3 90 % to 99 %, indirect monitoring.

The control circuit of reed relays in the ATC system is shown in Figure F.2.

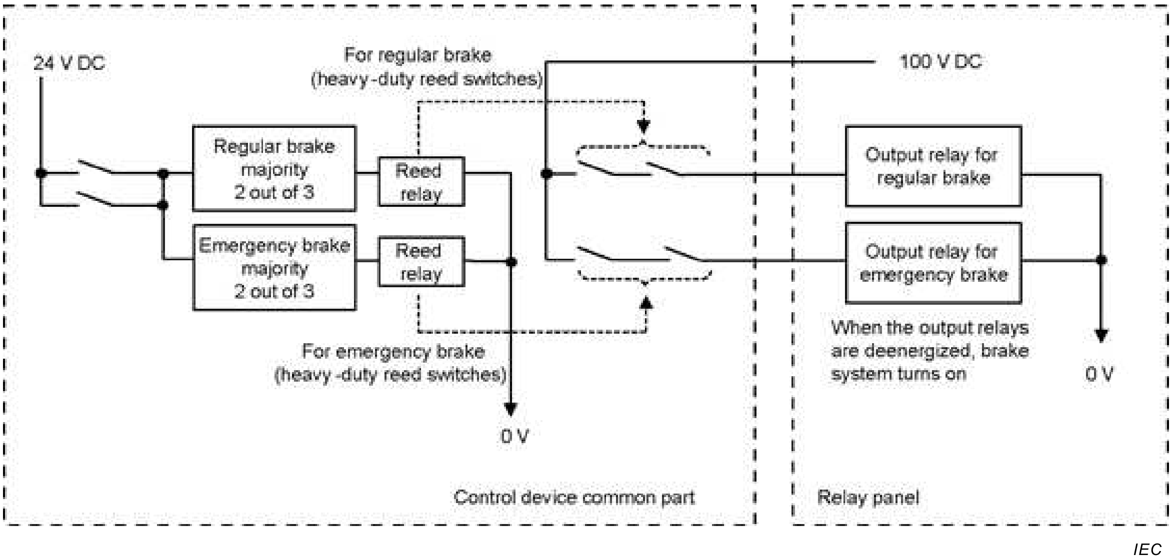


Figure F.2 – Control circuit of reed switches in the ATC system

F.5 Example of calculation of failure rates for the reed switch-device

The field failure rates are proved in use. The example of the field failure data based on the conditions according to Clause F.4 is shown in Table F.1.

Table F.1 – Field failure rates of reed relays in the ATC system

Symbol	Reliability data	Field failure rates
λ_s	Safety failure rate (1/h)	$1,17 \times 10^{-9}$
λ_{D2}	Dangerous failure rate (1/h)	less than $2,9 \times 10^{-10}$
SFF	Safety failure fraction	99 %
NOTE 1 The filed failure rates and failure mode databases are accumulated results of $1,7 \times 10^9$ component hours of field data. NOTE 2 The accumulated operating time is 11 × 12 × 12 h (from 2004 to 2015, 12 hours a day).		

F.6 Example of classification of involved groups for responsibility

An example of classification of involved groups for responsibility is given in Table F.2.

Table F.2 – Possible sharing of responsibility on reed relays in the ATC system

Feature	Manufacturer of the reed switch	Manufacturer of the reed relay	Manufacturer of E/E/PE systems according to IEC 62425	Manufacturer of the equipment (machine)	Owner/ user of the equipment (machine)	Operator of the equipment (machine)	Maintainer of the equipment (machine)
Reed switch standard	yes	yes	no	no	no	no	no
Component standard [a]	yes	yes	no	no	no	no	no
Architecture [b]	no	no	no	yes	yes	yes	yes
Control circuit	no	no	yes	no	no	no	no
Proof test	no	no	no	no	no	yes	no
Replacement cycle	no	no	no	no	no	no	yes

[a] The contact ratings of reed switches standards are available. The B_{10D} value is specified by the manufacturer of the reed relay.

[b] The architecture of the system is given by the design. The owner/user, operator and maintainer have to ensure that the given safety standard has not changed.

Bibliography

International standards

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at http://www.electropedia.org)

IEC 60068-2-6:2007, *Environmental testing – Part 2: Tests – Test Fc: Vibration (sinusoidal)*

IEC 60068-2-27:2008, *Environmental testing – Part 2-27: Tests – Test Ea and guidance: Shock*

IEC 60079-29-3:2014, *Explosive atmosphere – Part 29-3: Gas detectors – Guidance on functional safety of fixed gas detection systems*

IEC 60255-1:2009, *Measuring relays and protection equipment – Common requirements*

IEC 60335-1:2010, *Household and similar electrical appliances – Safety – Part 1: General requirements*

IEC 60335-2-4, *Household and similar electrical appliances – Safety – Part 2-4: Particular requirements for spin extractors*

IEC 60335-2-7, *Household and similar electrical appliances – Safety – Part 2-7: Particular requirements for washing machines*

IEC 60730-2-5, *Automatic electrical controls – Part 2-5: Particular requirements for automatic electrical burner control systems*

IEC 60947-5-1:2016, *Low voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC 60947-5-2:2007, *Low voltage switchgear and controlgear – Part 5-2: Control circuit devices and switching elements – Proximity switches*

IEC 60947-5-3:2013, *Low voltage switchgear and controlgear – Part 5-3: Control circuit devices and switching elements – Requirements for proximity devices with defined behaviour under fault conditions (PDDB)*

IEC 60947-5-9:2006, *Low-voltage switchgear and controlgear – Part 5-9: Control circuit devices and switching elements – Flow rate switches.*

IEC 60127-2:2014, *Miniature fuses – Part 2: Cartridge fuse-links*

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61373:2010, *Railway applications – Rolling stock equipment – Shock and vibration tests*

IEC 61810-1:2015, *Electromechanical elementary relays – Part 1: General and safety requirements*

IEC 61810-2, *Electromechanical elementary relays – Part 2: Reliability*

IEC 61810-2-1, *Electromechanical elementary relays – Part 2-1: Reliability – Procedure for the verification of B_{10} values*

IEC 61811-1:2015, *Electromechanical telecom elementary relays of assessed quality – Part 1: Generic specification and blank detail specification*

IEC 62278, *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

IEC 62425, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

ISO 4413, *Hydraulic fluid power − General rules and safety requirements for systems and their components*

ISO 4414, *Pneumatic fluid power – General rules and safety requirements for systems and their components*

ISO 14119:2013, *Safety of machinery – Interlocking devices associated with guards – Principles for design and selection*

National standards and regulations

JIS B 6410: 2009, *Presswork machinery – Safety requirements of servo presses*

The seventy-first article, Shinkansen super-express Bullet train structure regulation (Automatic train control equipment)

Legal performance standard (law enforcement standard Article 44) about the adequacy of securing of preservation of the liquefied petroleum gas and the business Setting duty of the gas leak alarm for the liquefied petroleum gas which let a law construction standard Article 44 seism scope link

JEC 2500:2010, Protection relays for electric power systems, The Japanese Electro-technical Committee

Databases

ATS & ATC Railway signalling equipment, April 2012, Japan Railway Electrical Engineering Association

Annual report on liquefied petroleum gas (LPG) related accidents (2013 version), The High Pressure Gas Safety Institute of Japan (KHK)

Report for maintenance cycle of railway signalling devices, 2011-June, Japan Association of Signal Industries

____

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