AS/NZS 4024.1503:2014
ISO 13849-1:2006
ISO 13849-1:2006/Cor.1:2009

AS/NZS 4024.1503:2014

Australian/New Zealand Standard™

# Safety of machinery

# Part 1503: Safety related parts of control systems – General principles for design




This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee SF-041, General Principles for the Guarding of Machinery. It was approved on behalf of the Council of Standards Australia on 5 June 2014 and on behalf of the Council of Standards New Zealand on 24 April 2014.
This Standard was published on 30 June 2014.

---

The following are represented on Committee SF-041:

Australian Chamber of Commerce and Industry
Australian Industry Group
Australian Manufacturing Workers Union
Department of Mines and Petroleum, WA
Department of the Premier and Cabinet, SA
Engineers Australia
Federal Chamber of Automotive Industries
Human Factors and Ergonomics Society of Australia
Institute of Instrumentation, Control and Automation
National Safety Council of Australia
New Zealand Electrical Institute
NSW Department of Trade and Investment, Regional Infrastructure and Services
Safety Institute of Australia
University of Melbourne
Winery Engineering Association
WorkCover New South Wales
WorkSafe NZ
WorkSafe Victoria

---

## Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Australia Web Site at www.standards.org.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

---

*This Standard was issued in draft form for comment as DR AS/NZS 4024.1503.*

Australian/New Zealand Standard™

# Safety of machinery

# Part 1503: Safety-related parts of control systems—General principles for design

First published as AS/NZS 4024.1503:2014.



ISBN 978 1 74342 756 9

# PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee SF-041, General Principles for the Guarding of Machinery.

It is emphasized that this Standard is part of the AS(/NZS) 4024.1 series and it is imperative that it is used in conjunction with other applicable parts of the series. A complete listing of all current parts of the AS(/NZS) 4024.1 series can be found at the Standards Australia website <www.standards.org.au> and in AS/NZS 4024.1100, *Safety of machinery*, Part 1100: *Application Guide*.

The objective of this Standard is to specify the characteristics of safety-related parts of control systems (SRP/CS). The characteristics include the performance level required for carrying out safety functions. This Standard applies to all types of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.). The performance levels, together with the appropriate category or the category selection alone (specified in AS 4024.1501), may be used.

Performance levels require a determination of the probability of dangerous failure, and this is considered to be a more comprehensive indicator of functional safety.

In Australia, the use of categories of safety-related parts of control systems is becoming more widely understood and there will be a transition period (as occurred in Europe) to allow practitioners time to work with and understand the probabilistic approach described in this Standard. It is envisaged that on completion of the work of JWG 1 of ISO TC 199 and IEC TC 44, combining ISO 13849-1:2006 and IEC 62061, the resulting unified Standard will replace both AS 4024.1501 and AS/NZS 4024.1503, in the next revision of the AS(/NZS) 4024 series.

This Standard is identical with, and has been reproduced from ISO 13849-1:2006, *Safety of machinery—Safety-related parts of control systems*, Part 1: *General principles for design*, and its Corrigendum 1 (2009), which has been added at the end of the source text.

As this Standard is reproduced from an International Standard, the following applies:

(a) In the source text 'this part of ISO 13849' should read 'this Australian/New Zealand Standard'.

(b) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards as follows:

| *Reference to International Standard* | | *Australian/New Zealand Standard* | |
|---|---|---|---|
| ISO | | AS/NZS | |
| 12100 | Safety of machinery—Basic concepts, general principles for design | 4024 | Safety of machinery |
| 12100-1 | Part 1: Basic terminology, methodology | 4024.1201 | Part 1201: General principles for design—Risk assessment and risk reduction |
| 12100-2 | Part 2: Technical principles | 4024.1201 | Part 1201: General principles for design—Risk assessment and risk reduction |
| | | AS | |
| 13849 | Safety of machinery—Safety-related parts of control systems | 4024 | Safety of machinery |
| 13849-2 | Part 2: Validation | 4024.1502 | Part 1502: Design of safety related parts of control systems—Validation |

| | | | |
|---|---|---|---|
| | | AS/NZS 4024 | Safety of machinery |
| 14121 | Safety of machinery—Principles of risk assessment | 4024.1201 | Part 1201: General principles for design—Risk assessment and risk reduction |

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

CONTENTS

*Page*

# INTRODUCTION

The structure of safety standards in the field of machinery is as follows.

a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

   — type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

   — type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of ISO 13849 is a type-B-1 standard as stated in ISO 12100-1.

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built according to the provisions of the type-C standard.

This part of ISO 13849 is intended to give guidance to those involved in the design and assessment of control systems, and to Technical Committees preparing Type-B2 or Type-C standards which are presumed to comply with the Essential Safety Requirements of Annex I of the Council Directive 98/37/EC, The Machinery Directive. It does not give specific guidance for compliance with other EC directives.

As part of the overall risk reduction strategy at a machine, a designer will often choose to achieve some measure of risk reduction through the application of safeguards employing one or more safety functions.

Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS) and these can consist of hardware and software and can either be separate from the machine control system or an integral part of it. In addition to providing safety functions, SRP/CS can also provide operational functions (e.g. two-handed controls as a means of process initiation).

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). These performance levels are defined in terms of probability of dangerous failure per hour (see Table 3).

The probability of dangerous failure of the safety function depends on several factors, including hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure ($MTTF_d$), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

In order to assist the designer and help facilitate the assessment of achieved PL, this document employs a methodology based on the categorization of structures according to specific design criteria and specified behaviours under fault conditions. These categories are allocated one of five levels, termed Categories B, 1, 2, 3 and 4.

The performance levels and categories can be applied to safety-related parts of control systems, such as

— protective devices (e.g. two-hand control devices, interlocking devices), electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices,

— control units (e.g. a logic unit for control functions, data processing, monitoring, etc.), and

— power control elements (e.g. relays, valves, etc),

as well as to control systems carrying out safety functions at all kinds of machinery — from simple (e.g. small kitchen machines, or automatic doors and gates) to manufacturing installations (e.g. packaging machines, printing machines, presses).

This part of ISO 13849 is intended to provide a clear basis upon which the design and performance of any application of the SRP/CS (and the machine) can be assessed, for example, by a third party, in-house or by an independent test house.

**Information on the recommended application of IEC 62061 and this part of ISO 13849**

IEC 62061 and this part of ISO 13849 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. The following table summarizes the scopes of IEC 62061 and this part of ISO 13849.

**Table 1 — Recommended application of IEC 62061 and ISO 13849-1**

| | Technology implementing the safety-related control function(s) | ISO 13849-1 | IEC 62061 |
|---|---|---|---|
| A | Non-electrical, e.g. hydraulics | X | Not covered |
| B | Electromechanical, e.g. relays, and/or non complex electronics | Restricted to designated architectures [a] and up to PL = e | All architectures and up to SIL 3 |
| C | Complex electronics, e.g. programmable | Restricted to designated architectures [a] and up to PL = d | All architectures and up to SIL 3 |
| D | A combined with B | Restricted to designated architectures [a] and up to PL = e | X [c] |
| E | C combined with B | Restricted to designated architectures (see Note 1) and up to PL = d | All architectures and up to SIL 3 |
| F | C combined with A, or C combined with A and B | X [b] | X [c] |

X indicates that this item is dealt with by the International Standard shown in the column heading.

[a] Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.

[b] For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.

[c] For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.

NOTES

AUSTRALIAN/NEW ZEALAND STANDARD

# Safety of machinery

## Part 1503:
## Safety-related parts of control systems—General principles for design

## 1 Scope

This part of ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.

It does not specify the safety functions or performance levels that are to be used in a particular case.

This part of ISO 13849 provides specific requirements for SRP/CS using programmable electronic system(s).

It does not give specific requirements for the design of products which are parts of SRP/CS. Nevertheless, the principles given, such as categories or performance levels, can be used.

NOTE 1 Examples of products which are parts of SRP/CS: relays, solenoid valves, position switches, PLCs, motor control units, two-hand control devices, pressure sensitive equipment. For the design of such products, it is important to refer to the specifically applicable International Standards, e.g. ISO 13851, ISO 13856-1 and ISO 13856-2.

NOTE 2 For the definition of *required performance level*, see 3.1.24.

NOTE 3 The requirements provided in this part of ISO 13849 for programmable electronic systems are compatible with the methodology for the design and development of safety-related electrical, electronic and programmable electronic control systems for machinery given in IEC 62061.

NOTE 4 For safety-related embedded software for components with $PL_r$ = e see IEC 61508-3:1998, Clause 7.

NOTE 5 See also Table 1.

## 2 Normative references

The following referenced documents are indispensable for the application 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.

ISO 12100-1:2003, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

ISO 13849-2:2003*, Safety of machinery — Safety-related parts of control systems — Part 2: Validation*