



Safety of machinery

Part 1501: Design of safety related parts of control systems—General principles for design



This Australian Standard® was prepared by Committee SF-041, General Principles for the Guarding of Machinery. It was approved on behalf of the Council of Standards Australia on 11 April 2006.

This Standard was published on 29 June 2006.

The following are represented on Committee SF-041:

- Australian Chamber of Commerce and Industry
 - Australian Electrical and Electronic Manufacturers Association
 - Department for Administration and Information Services, SA
 - Department of Consumer and Employment Protection, WorkSafe Division, WA
 - Department of Primary Industries, Mine Safety, NSW
 - Engineers Australia
 - Federal Chamber of Automotive Industries
 - Human Factors and Ergonomics Society of Australia
 - Institution of Instrumentation, Control and Automation Australia
 - National Electrical and Communications Association
 - National Safety Council of Australia
 - Office of the Australian Safety and Compensation Council
 - Safety Institute of Australia
 - The University of Melbourne
 - Tractor and Machinery Association of Australia
 - Victorian WorkCover Authority
-

This Standard was issued in draft form for comment as DR 05442.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

Safety of machinery

Part 1501: Design of safety related parts of control systems—General principles for design

Originated as part of AS 4024.1(Int)—1992.
Previous edition part of AS 4024.1—1996.
Revised in part and redesignated as AS 4024.1501—2006.
Reissued incorporating Amendment No. 1 (November 2015).

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7413 X

PREFACE

This Standard was prepared by the Standards Australia Committee SF-041, as a revision, in part, of AS 4024.1—1996, *Safeguarding of machinery, Part 1: General principles*.

This Standard incorporates Amendment No. 1 (November 2015). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

A1 | This Standard is technically equivalent to ISO 13849-1:1999, *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design*. This will maintain consistency with other machine-specific Australian Standards.

This edition has been published as a series of Parts rather than the single Standard previously published as AS 4024.1. In doing this, the Committee has cleared the way for simple revisions in the future. When a new edition of a relevant Standard becomes available at the international level, it will be adopted and published within the framework of AS 4024 with a minimum delay, so ensuring continued international alignment.

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

CONTENTS

	<i>Page</i>
FOREWORD.....	4
1 SCOPE.....	5
2 OBJECTIVE	5
3 REFERENCED DOCUMENTS	5
4 DEFINITIONS	6
5 GENERAL CONSIDERATIONS	7
6 CHARACTERISTICS OF SAFETY FUNCTIONS	12
7 CATEGORIES	16
8 FAULT CONSIDERATION	22
9 VALIDATION.....	23
10 VALIDATION REPORT	25
11 MAINTENANCE.....	25
12 INFORMATION TO BE PROVIDED TO THE USER.....	25
APPENDICES	
A QUESTIONNAIRE FOR USE DURING THE DESIGN PROCESS	26
B RELATIONSHIP BETWEEN SAFETY, RELIABILITY AND AVAILABILITY FOR MACHINERY	28
C GUIDANCE FOR SELECTION OF CATEGORIES.....	29
D EXAMPLES OF SIGNIFICANT FAULTS AND FAILURES FOR VARIOUS TECHNOLOGIES	32

FOREWORD

Certain parts of machinery control systems are frequently assigned safety functions; these are called the safety related parts. These parts can consist of both hardware and software, and they are intended to provide the safety functions of control systems. They can be separate or integrated parts of the control system.

The performance of a safety-related part of a control system with respect to the occurrence of faults is classified in this Standard into five categories (B, 1, 2, 3 and 4) which should be used as reference points. These categories (see Clause 7.2) are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.

The categories can be applied to—

- (a) control systems for all kinds of machinery, from simple, e.g. small kitchen appliances, to complex manufacturing installations, e.g. packaging machinery, printing machines, presses; and
- (b) control systems for protective equipment, e.g. two-hand control devices, interlocking devices, electro-sensitive protective devices (e.g. photoelectric barriers) and pressure sensitive mats.

The category selected will depend upon the machine and the extent to which control means are used for the protective measures.

When selecting a category and designing a safety-related part of a control system, the designer should provide at least the following information about the safety-related part:

- (i) The category(ies) selected.
- (ii) The functional characteristics.
- (iii) The precise role the safety related part plays in the machinery protective measure(s).
- (iv) The exact limits of the part under consideration (see Clause 4.8).
- (v) All safety-relevant faults considered.
- (vi) Those safety-relevant faults not considered, by fault exclusion, and the measures employed to allow their exclusion.
- (vii) The parameters relevant to the reliability of the part, such as environmental conditions.
- (viii) The technology(ies) used.

The use of categories as reference points and a declaration of the rationale followed during the design process is intended to allow this Standard to be used flexibly. It is intended to provide a clear basis upon which the design and performance of any application of the safety-related part of a control system (and the machine) can be assessed, e.g. by a third party, in-house means or an independent test house.

STANDARDS AUSTRALIA

Australian Standard Safety of machinery

Part 1501: Design of safety related parts of control systems—General principles for design

1 SCOPE

This Standard provides safety requirements and guidance on the principles for the design of safety-related parts of control systems. For these parts, it specifies categories and describes the characteristics of their safety functions, including programmable systems for all machinery and for related protective devices.

This Standard applies to all safety-related parts of control systems, regardless of the type of energy used, e.g. electrical, hydraulic, pneumatic, mechanical. It does not specify which safety functions and which categories are to be used in a particular case.

This Standard applies to all machinery applications for both professional and non-professional use. Where appropriate, it can also be applied to the safety-related parts of control systems used in other technical applications.

2 OBJECTIVE

The objective of this Standard is to enable designers, manufacturers, suppliers, employers and users of machinery to minimize risks to the health and safety of employees and others working with or otherwise near machinery by providing technical principles for the design of safety related parts of control systems.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard.

AS

4024	Safety of machinery
4024.1201	Part 1201: General principles—Basic terminology and methodology
4024.1202	Part 1202: General principles—Technical principles
4024.1301	Part 1301: Risk assessment—Principles for risk assessment
4024.1401	Part 1401: Ergonomic principles—Design principles—Terminology and general principles
4024.1502	Part 1502: Design of safety related parts of control systems—Validation
4024.1901	Part 1901: Displays, controls, actuators and signals—Ergonomic requirements for the design of displays and control actuators—General principles for human interactions with displays and control actuators
4024.1902	Part 1902: Displays, controls, actuators and signals—Ergonomic requirements for the design of displays and control actuators—Displays
4024.1903	Part 1903: Displays, controls, actuators and signals—Ergonomic requirements for the design of displays and control actuators—Control actuators
60068	Environmental testing—General and guidance
60068.1	Part 1: General and guidance

AS

60204 Safety of machinery—Electrical equipment of machines

60204.1 Part 1: General requirements (IEC 60204-1, Ed.5 (FDIS) MOD)

60529 Degrees of protection provided by enclosures (IP code)

61508 Functional safety of electrical/electronic/programmable electronic safety related systems (series)

AS/NZS

61000 Electromagnetic compatibility (EMC)

61000.4.1 Part 4.1: Testing and measurement techniques—Overview of immunity tests

IEC

60447 Basic and safety principles for man-machine interface, marking and identification—Actuating principles

60721 Classification of environmental conditions

60721-3-0 Part 3: Classification of groups of environmental parameters and their severities—Introduction

BS EN

1005 Safety of machinery—Human physical performance

1005-3 Part 3: Recommended force limits for machinery operation

4 DEFINITIONS

For the purposes of this Standard the definitions given in AS 4024.1201 and the following apply.

4.1 Category

Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition.

NOTE: Such behaviour is achieved by the structural arrangement of the parts or by their reliability.

4.2 Failure

Termination of the ability of an item to perform a required function.

NOTES:

- 1 After a failure, the item has a fault.
- 2 'Failure' is an event, as distinguished from 'fault' which is a state.
- 3 This concept as defined does not apply to items consisting of software only.
- 4 In practice, the terms fault and failure are often used synonymously.

4.3 Fault

State of an item characterized by inability to perform a required function, except during preventive maintenance or other planned actions or due to lack of external resources.

NOTE: A fault is often the result of a failure of the item itself, but may exist without prior failure.

4.4 Manual reset

Function within the safety-related parts of the control system to manually restore given safety functions before the re-starting of a machine.

4.5 Muting

Temporary automatic suspension of a safety function(s) by safety-related parts of the control system to enable the machine (as a system) to achieve a safe state.

4.6 Safety function of a control system

Function initiated by an input signal and processed by the safety-related parts of the control system to enable the machine (as a system) to achieve a safe state.

4.7 Safety of control systems

Ability of safety-related parts of a control system to perform their safety function(s) for a given time according to their specified category.

4.8 Safety-related part of a control system

Part, or subpart(s), of a control system which responds to input signals and generates safety-related output signals.

NOTE: The combined safety-related parts of a control system start at the points where the safety-related signals are initiated and end at the output of the power control elements (see also AS 4024.1201). This also includes monitoring systems.

5 GENERAL CONSIDERATIONS

5.1 Safety objectives in design

The safety-related parts of a control system which provide the safety functions shall be designed and constructed so that the principles of AS 4024.1301 are fully taken into account—

- (a) during all intended use and foreseeable misuse;
- (b) when faults occur; and
- (c) when foreseeable human mistakes are made during the intended use of the machine as a whole.

5.2 General strategy for design

From the risk assessment (see AS 4024.1301) of the machine, the designer shall decide the contribution to the reduction of risk which needs to be provided by each safety-related part of the control system. This contribution does not cover the overall risk of the machinery under control, e.g. not the overall risk of a mechanical press or washing machine, but that part of risk reduced by the application of particular safety functions. Examples of such functions are the stop function initiated by using an electrosensitive protective device on a press, or the door-locking function of a washing machine.

NOTE: A questionnaire which can be used for this purpose is given in Appendix A.

The key objective is that the designer ensure that the safety-related parts of a control system produce outputs which achieve the risk reduction objectives of AS 4024.1301. This is not always achievable, and in such cases the designer shall provide other safety measures. The hierarchy for the strategy in reducing risk is given in AS 4024.1201.

The category and other features, e.g. physical position of parts, isolation, selected by the designer for the safety-related parts will depend upon the contribution made by those parts to the reduction of risk, the design and the technology (see Foreword). The designer shall declare—

- (a) which category is being used as the reference point for the design;
- (b) the exact points at which the safety-related part(s) start and at which it ends; and
- (c) the design rationale, e.g. the faults considered, the faults excluded, within the design to achieve that category(ies).

The greater the dependence of risk reduction upon the safety-related parts of control systems, then the higher is the required ability of those parts to resist faults. This ability — in the understanding that the required function is performed — can be partly quantified by reliability values and by a fault-resistant structure. Both reliability and structure contribute to this ability of safety-related parts to resist faults. A specified resistance to faults can be achieved by specifying levels of reliability of components or with improved structures for the safety-related parts. The contributions of reliability and of structure can vary with the technology used. For example, it is possible for a single channel of safety-related parts of high reliability in one technology to provide the same or higher resistance to faults as a fault-tolerant structure of lower reliability in a different technology.

NOTE: The higher the resistance to faults of the safety-related parts, the lower the probability that the safety-related parts will fail to carry out the required safety functions.

Reliability and safety are not the same. For example, it is possible that the safety of a system with relatively unreliable components, in a redundant structure, is higher than the safety of a system with a simpler structure but with more reliable components. This concept is important because in some applications safety requires the highest priority regardless of the reliability achieved, e.g. when the consequences of failure are always serious and normally irreversible. In such applications, a fault detection (one-cycle fault-tolerant) structure which provides the required safety function after one or two or more faults shall be provided in accordance with the risk assessment.

NOTE: The relationship between safety, reliability and availability is described in Appendix B.

This Standard does not require the calculation of reliability values for complex structures where safety is predominately obtained by improving the structure of the safety-related parts. For less complex structures, where component reliability is important to safety, the calculation of reliability values is a useful indicator of the contribution to the overall risk reduction by the safety-related parts.

In the case of applications with lower risk, measures to avoid faults may be appropriate; for higher risk applications, improving the structure of the safety-related parts of a control system can provide measures to avoid, detect or tolerate faults. Practical measures include redundancy, diversity and monitoring (see AS 4024.1202 and AS 60204.1).

The fault-resistance behaviour achieved of the safety-related parts of the control system is a function of many parameters including the—

- (i) reliability with respect to performing the safety functions;
- (ii) structure (or architecture) of the control system;
- (iii) quality of safety-related documentation;
- (iv) completeness of the specification;
- (v) design, manufacture and maintenance;
- (vi) quality and accuracy of software;
- (vii) extent of functional testing; and
- (viii) operating characteristics of the machine, or part of the machine under control.

These parameters can be grouped under three main characteristics:

- (A) Hardware reliability—the level of reliability of the components to avoid faults.
- (B) System structure—the arrangement of the components in the safety-related part of a control system to avoid, tolerate or detect faults.
- (C) Non-quantifiable, qualitative aspects which affect the behaviour of the safety-related part of a control system.

5.3 Process for selection and design of safety measures

5.3.1 General

This Clause sets out a process first for the selection of the safety measures to be provided and then for the design of the safety-related parts of the control system. It is important that the interfaces between the safety-related parts of the control system, the non-safety-related parts of the control system and all other parts of the machine be identified.

Then the contribution to risk reduction provided by the safety-related parts can be specified within the risk assessment of the machine according to AS 4024.1301.

Because there are many ways in which the risk at a machine can be reduced and because there are many ways in which the safety-related parts of the control system can be designed, this process is iterative. Decisions or assumptions made at any step in the procedure may affect decisions or assumptions made at an earlier step. This aspect can be checked by looping back through the procedure at any step. Such checking in the validation step is essential to ensure that the safety performance which is achieved is the same as that set out in the specification.

The process is illustrated in Figure 1. Important aspects which should be considered during the design process may be presented as questions to prompt the designer. These questions illustrate the philosophy which should be followed in the design of the safety-related parts. Not all questions apply to every application. Some applications require additional questions.

NOTE: A typical questionnaire is given in Appendix A.

5.3.2 Step 1: Hazard analysis and risk assessment

Identify the hazards present at the machine during all modes of operation and at each stage in the life of the machine by following the guidance in AS 4024.1201 and AS 4024.1301.

Assess the risk arising from those hazards and decide the appropriate risk reduction for that application in accordance with AS 4024.1201 and AS 4024.1301.

5.3.3 Step 2: Decide measures for risk reduction by control means

Decide the design measures at the machine or the provision of safeguards to provide the risk reduction. Those parts of the control system which contribute as an integral part of the design measures and/or in the control of the safeguards shall be considered safety-related parts.

NOTE: Guidance for the selection of an appropriate category is given in Appendix C.

5.3.4 Step 3: Specify safety requirements for the safety-related parts of the control system

Specify the safety functions to be provided in the control system. Table 1 lists the source reference of the more common safety functions and the characteristics which shall be included if a particular safety function is selected.

Specify how the safety functions will be met and select the category(ies) for each part and combinations of parts within the safety-related parts of the control system (see Clause 7).

5.3.5 Step 4: Design

Design the safety-related parts of the control system according to the specification developed in Step 3 above and to the general strategy for design in Clause 5.2. List the features included in the design which provide the rationale for the category(ies) achieved.

Verify the design at each stage to ensure that the safety-related parts fulfill the requirements from the previous stage in the context of the specified safety function(s) and category(ies).

5.3.6 Step 5: Validation

Validate the achieved safety functions and category(ies) against the specification in Step 3 above. Redesign as necessary (see Clause 9).

It is also necessary to validate the safety-related parts of the control system in conjunction with the entire control system and as part of the machine. The requirements of such validation are not within the scope of this Standard, but should be specified by the machine designer or the appropriate machine specific safety standard.

When programmable electronics are used in the design of safety-related parts of the control systems, other detailed procedures are required (see Clause 9.4.2). These procedures are under consideration.

NOTE: It is believed at present that it is difficult to determine with any degree of certainty, in situations when a significant hazard can occur due to the misoperation of the control system, that reliance on correct operation of a single channel of programmable electronic equipment can be assured. Until such time that this situation can be resolved, it is inadvisable to rely on the correct operation of such a single-channel device (according to AS 60204.1).

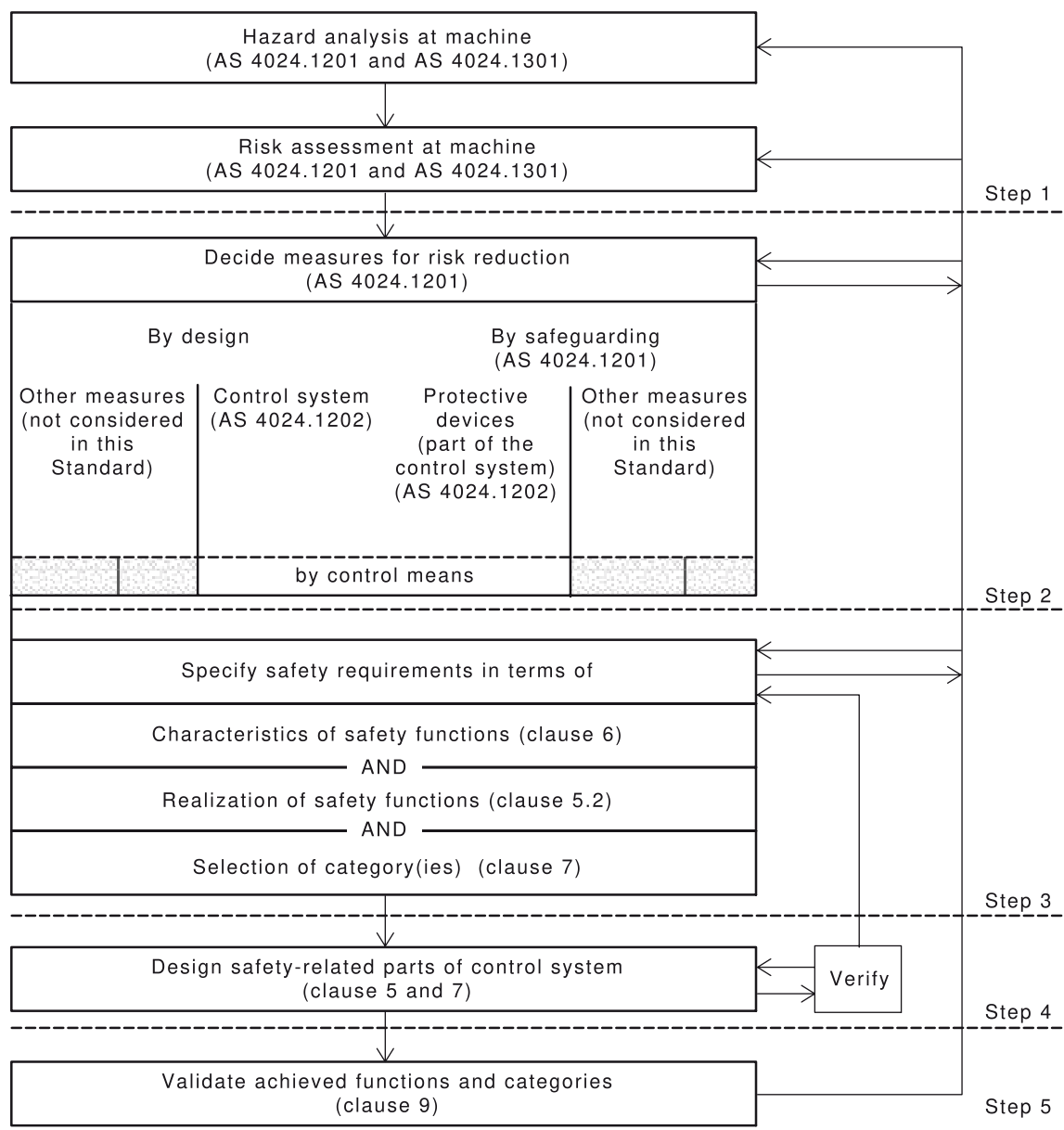


FIGURE 1 ITERATIVE PROCESS FOR THE DESIGN OF SAFETY-RELATED PARTS OF CONTROL SYSTEMS

5.4 Principles for ergonomic design

The interface between persons and the safety-related parts of control systems shall be designed and installed so that no one is endangered during all intended use and foreseeable misuse of the machine (for information see also AS 4024.1201; AS 60204.1; IEC 60447, AS 4024.1401, AS 4024.1901, AS 4024.1902, AS 4024.1903 and BS EN 1005-3).

Ergonomic principles should be used so that the machine and the control system, including the safety-related parts, are easy to use, and so that the operator is not tempted to act in a hazardous manner. The safety requirements for observing ergonomic principles given in AS 4024.1201, should apply.