



Safety of machinery

Part 1502: Design of safety related parts of control systems—Validation



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 05454.

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Standards may also be withdrawn.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 1502: Design of safety related parts of control systems—Validation

Originated as part of AS 4024.1(Int)—1992.
Previous edition part of AS 4024.1—1996.
Revised in part and redesignated as AS 4024.1502—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 7484 9

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 13849-2:2003, *Safety of machinery—Safety-related parts of control systems—Part 2: Validation*. 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>
1 SCOPE	4
2 OBJECTIVE	4
3 REFERENCED DOCUMENTS	4
4 VALIDATION PROCESS	5
5 VALIDATION BY ANALYSIS	9
6 VALIDATION BY TESTING	10
7 VALIDATION OF SAFETY FUNCTIONS.....	12
8 VALIDATION OF CATEGORIES.....	12
9 VALIDATION OF ENVIRONMENTAL REQUIREMENTS.....	14
10 VALIDATION OF MAINTENANCE REQUIREMENTS.....	14
APPENDICES	
A VALIDATION TOOLS FOR MECHANICAL SYSTEMS	15
B VALIDATION TOOLS FOR PNEUMATIC SYSTEMS.....	20
C VALIDATION TOOLS FOR HYDRAULIC SYSTEMS	31
D VALIDATION TOOLS FOR ELECTRICAL SYSTEMS	40

STANDARDS AUSTRALIA

Australian Standard
Safety of machinery

Part 1502: Design of safety related parts of control systems—Validation

1 SCOPE

This Standard specifies the procedures and conditions to be followed for the validation by both analysis and testing of the safety functions provided, and the category achieved for the safety related parts of the control system in compliance with AS 4024.1501, using the design rationale provided by the designer.

This Standard does not give complete validation requirements for programmable electronic systems and therefore can require the use of other standards.

NOTE: Requirements for programmable electronic systems, including embedded software, are given in the AS 61508 series.

2 OBJECTIVE

The objective of this Standard is to provide designers, manufacturers, suppliers, installers and users of safety related parts of control systems with the means of minimizing risks to the health and safety of those working with or otherwise near machinery fitted with safety related parts within their control systems.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard.

AS

1447	Hot-rolled spring steels
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 of risk assessment
4024.1501	Part 1501: Design of safety related parts of control systems—General principles for design
4024.1602	Part 1602: Design of controls, interlocks and guarding—Interlocking devices associated with guards—Principles for design and selection
4024.1603	Part 1603: Design of controls, interlocks and guarding—Prevention of unexpected start up
4024.1604	Part 1604: Design of controls, interlocks and guarding—Emergency stop—Principles for design
60204	Safety of machinery—Electrical equipment of machines
60204.1	Part 1: General requirements (IEC 60204-1 Ed.5 (FDIS) MOD)
60269	Low-voltage fuses
60269.1	Part 1: General requirements
60529	Degrees of protection provided by enclosures (IP Code)
60947	Low-voltage switchgear and control gear
60947.2	Part 2: Circuit-breakers

AS

- 60947.4.1 Part 4.1: Contactors and motor-starters—Electromechanical contactors and motor-starters
- 60947.5.1 Part 5.1: Control circuit devices and switching elements—Electromechanical control circuit devices
- 60947.6.2 Part 6.2: Multiple function equipment—Control and protective switching devices (or equipment) (CPS)
- 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems (series)

ISO

- 4079 Rubber hoses and hose assemblies—Textile reinforced hydraulic types—Specifications
- 4079-1 Part 1: Oil-based fluid applications

IEC

- 60664 Insulation coordination for equipment within low-voltage systems
- 60664-1 Part 1: Principles, requirements and tests
- 60947 Low-voltage switchgear and control gear
- 60947-5-3 Part 5-3: Control circuit devices and switching elements—Requirements for proximity devices with defined behaviour under fault conditions
- 61558 Safety of power transformers, power supply units and similar
- 61558-1 Part 1: General requirements and tests

4 VALIDATION PROCESS

4.1 Validation principles

4.1.1 Purpose

The purpose of the validation process is to confirm the specification and the conformity of the design of the safety-related parts of the control system within the overall safety requirements specification of the machinery.

The validation shall demonstrate that each safety-related part meets the requirements of AS 4024.1501 in particular the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale, and the requirements of the specified category according to AS 4024.1501.

Validation should be carried out by persons who are independent of the design of the safety-related part(s).

NOTE: Independent person does not necessarily mean that a third party test is required.

The degree of independence should reflect the safety performance of the safety-related part.

4.1.2 Process

Validation consists of applying analysis (see Clause 5) and, if necessary, executing tests (see Clause 6) in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between analysis and testing depends on the technology.

The analysis should be started as early as possible and in parallel with the design process, so that problems can be corrected whilst they are still relatively easy to correct. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

For large systems, due to the size, complexity or integrated form (with the machinery) of the control system, special arrangements may be made for validation of the safety-related parts of the control system separately before integration including simulation of the appropriate input and output signals, and validation of the effects of integrating safety-related parts into the remainder of the control system within the context of its use in the machine.

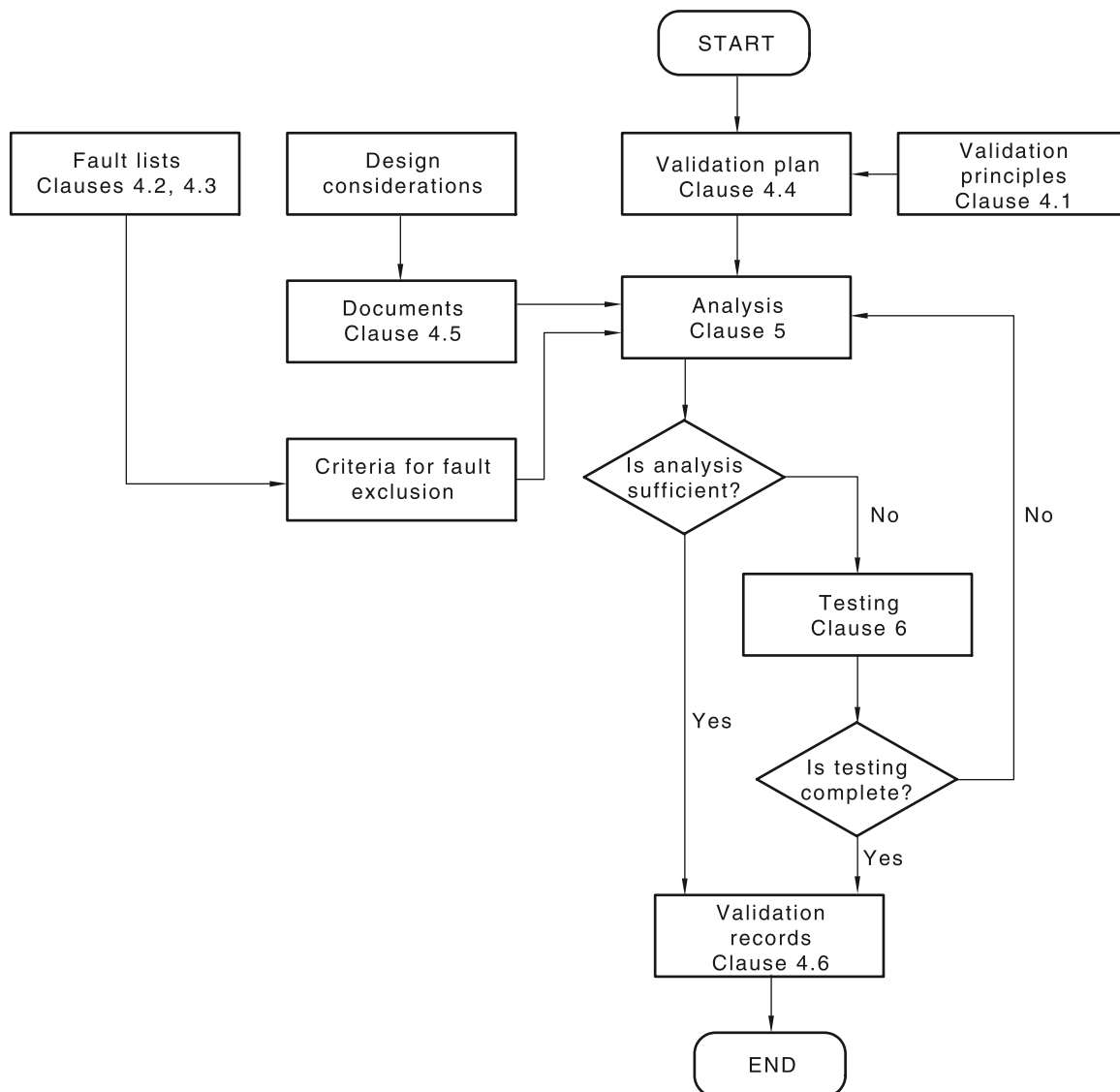


FIGURE 1 OVERVIEW OF THE VALIDATION PROCESS

4.2 Generic fault lists

The validation process involves consideration of behaviour of the safety-related part(s) of the control system for all faults to be considered. The generic fault lists contain—

- (a) the components/elements to be included, e.g. conductors/cables;
- (b) the faults to be taken into account, e.g. short circuits between conductors;
- (c) the permitted fault exclusions; and
- (d) a remarks section giving the reasons for the fault exclusions.

Only permanent faults are taken into account.

NOTE: A basis for fault consideration is given in Appendices A, B, C and D.

4.3 Specific fault lists

A specific product-related fault list shall be generated as a reference document for the validation process of the safety-related part(s). The list can be based on the appropriate generic list(s) found in the Appendices.

Where the specific product-related fault list is based on the generic list(s) it shall state—

- (a) the faults taken from the generic list(s) to be included;
- (b) any other relevant faults to be included but not given in the generic list (e.g. common mode faults); and
- (c) the faults taken from the generic list(s) that may be excluded and can meet at least the criteria given in the generic list(s).

Under exceptional circumstances, the specific product-related fault list may include any other relevant faults, from the generic list but not permitted for exclusion by the generic list(s), together with a justification and a rationale for its exclusion.

Where this list is not based on the generic list(s) the designer shall give the rationale for fault exclusions.

4.4 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process of the specified safety functions and their categories.

The validation plan shall also identify the means to be employed to validate the specified safety functions and categories. It shall set out, where appropriate—

- (a) the identity of the specification documents;
- (b) the operational and environmental conditions;
- (c) the basic safety principles (see Paragraphs A2, B2, C2 and D2);
- (d) the well-tried safety principles (see Paragraphs A3, B3, C3 and D3);
- (e) the well-tried components (see Paragraphs A4 and D4);
- (f) the fault assumptions and fault exclusions to be considered e.g. from the informative fault lists in Paragraphs A5, B5, C5 and D5; and
- (g) the analyses and tests to be applied.

Safety-related parts which have previously been validated to the same specification need only a reference to that previous validation.

4.5 Information for validation

The information required for validation will vary with the technology used, the category(ies) to be demonstrated, the design rationale of the system and the contribution of the safety-related parts of control systems to the reduction of risk. Documents containing sufficient information from the following list shall be included in the validation process to demonstrate the category(ies) and the safety function(s) of the safety-related parts which have been achieved. The list is as follows:

- (a) Specification(s) of the expected performance, of the safety functions and categories.
- (b) Drawings and specifications, e.g. for mechanical, hydraulic and pneumatic parts, printed circuit boards, assembled boards, internal wiring, enclosure, materials, mounting.
- (c) Block diagram(s) with functional description of the blocks.
- (d) Circuit diagram(s) including interfaces/connections.

- (e) Functional description of the circuit diagram(s).
- (f) Time sequence diagram(s) for switching components, signals relevant for safety.
- (g) Description of the relevant characteristics of components previously validated.
- (h) For other safety-related parts (excluding those listed in Item (g)) component lists with item designations, rated values, tolerances, relevant operating stresses, type designation, failure rate data and component manufacturer and any other data relevant for safety.
- (i) Analysis of all relevant faults (see also Clause 4.2) listed e.g. in Paragraphs A5, B5, C5 and D5, including the justification of any excluded faults.
- (j) An analysis of the influence of processed materials.

Category specific information shall be provided, as required by Table 2. Additionally, where software is relevant to the safety function(s), the software documentation shall include—

- (i) a specification which is clear and unambiguous and states the safety performance the software is required to achieve;
- (ii) evidence that the software is designed to achieve the required safety performance; and
- (iii) details of tests (in particular test reports) carried out to prove that the required safety performance is achieved.

4.6 Validation record

Validation by analysis and testing shall be recorded. The record shall demonstrate the validation process for each of the safety requirements. Cross-reference may be made to previous validation records, provided they are properly identified.

For any safety-related part which has failed part of the validation process, the validation record shall describe the part(s) of the validation tests and/or analysis which have been failed.

TABLE 2
DOCUMENTATION REQUIREMENTS FOR CATEGORIES

Documentation requirement	Category for which documentation is required				
	B	1	2	3	4
Basic safety principles	X	X	X	X	X
Expected operating stresses	X	X	X	X	X
Influences of processed material	X	X	X	X	X
Performance during other relevant external influences	X	X	X	X	X
Well-trying components	—	X	—	—	—
Well-trying safety principles	—	X	X	X	X
The check procedure of the safety function(s)	—	—	X	—	—
Checking intervals, when specified	—	—	X	—	—
Foreseeable, single faults considered in the design and the detection method used	—	—	X	X	X
The common mode failures identified and how prevented	—	—	—	X	X
The foreseeable, single faults excluded	—	—	—	X	X
The faults to be detected	—	—	X	X	X
The variety of accumulations of faults considered in the design	—	—	—	—	X
How the safety function is maintained in the case of each of the fault(s)	—	—	—	X	X
How the safety function is maintained for each of the combination(s) of faults	—	—	—	—	X

NOTES:

- 1 The categories mentioned in Table 2 are those given in AS 4024.1501.
- 2 X = documentation is required for the category.
- 3 — = Documentation is not required for the category.

5 VALIDATION BY ANALYSIS

5.1 General

The validation of safety-related parts of control systems shall be carried out by analysis. Inputs to the analysis are—

- (a) the hazards identified during analysis at the machine;
- (b) the reliability;
- (c) the system structure;
- (d) the non-quantifiable, qualitative aspects which affect system behaviour; and
- (e) deterministic arguments.

Validation of the safety functions by analysis rather than testing requires the formulation of deterministic arguments. Deterministic arguments differ from other evidence in that they show that the required properties of the system follow logically from a model of the system. Such arguments can be constructed on the basis of simple, well-understood concepts, such as the correctness of a mechanical interlock.

NOTE: A deterministic argument is an argument based on qualitative aspects (e.g. quality of manufacture, failure rates, experience of use). This consideration is depending on the application. This and other factors can affect the deterministic arguments.

5.2 Analysis techniques

The technique of analysis to be chosen depends upon the goal to be achieved. Two basic types of techniques exist as follows:

- (a) Top-down (deductive) techniques are suitable for determining the initiating events that can lead to identified top events, and calculating the probability of top events from the probability of the initiating events. They can also be used to investigate the consequences of identified multiple faults. Examples of top-down techniques are Fault Tree Analysis (FTA - see IEC 61025) and Event Tree Analysis (ETA);
- (b) Bottom-up (inductive) techniques are suitable for investigating the consequence of identified single faults. Examples of bottom-up techniques are Failure Modes and Effects Analysis (FMEA - see IEC 60812) and Failure Modes, Effects and Criticality Analysis (FMECA).

More information on analysis methods is given in AS 4024.1301.

6 VALIDATION BY TESTING

6.1 General

When validation by analysis is not sufficient to demonstrate the achievement of specified safety functions and categories, testing shall be carried out to complete the validation. Testing is always complementary to analysis and is often necessary.

Validation tests shall be planned and implemented in a logical manner. Particular attention shall be paid to the following:

- (a) A test plan shall be produced prior to the starting of the test and shall include—
 - (i) test specifications;
 - (ii) expected results of test; and
 - (iii) chronology of the tests.
- (b) Test records shall be produced that include—
 - (i) name of the tester;
 - (ii) environmental conditions (see Clause 8);
 - (iii) test procedures and equipment used; and
 - (iv) results of the test.
- (c) The test records shall be compared with the test plan to give assurance that the specified functional and performance targets are achieved.

The test sample shall be operated as near as possible to its final operating configuration, i.e. with all peripheral devices and covers attached.

Testing can be applied manually or automatically (e.g. by computer).

Where applied, validation of the safety functions by testing shall be carried out by applying inputs, in various combinations, to the safety-related part of the control system. The corresponding outputs shall be compared to the appropriate specified outputs.

It is recommended that the combination of these inputs be applied systematically to the control system and the machine. An example of this logic is: power-on, start-up, operation, directional changes, restart-up. Where necessary, an expanded range of input data shall be applied to take into account anomalous or unusual situations to see how the safety-related parts of the control system respond. Such combinations of input data shall take into account foreseeable incorrect operation(s).

The objectives of the test will be determined by the environmental conditions for that test. The conditions may be—

- (i) the environmental conditions of intended use;
- (ii) conditions at a particular rating; or
- (iii) a given range of conditions if drift is expected.

NOTE: The range of conditions which is considered stable and over which the tests are valid should be agreed between the designer and the person(s) responsible for carrying out the tests and should be recorded.

6.2 Measurement uncertainty

The uncertainty of measurements during the validation by testing shall be appropriate to the test being carried out. In general, these measurement uncertainties shall be within 5 K for temperature measurements and 5% for the following:

- (a) Time measurements.
- (b) Pressure measurements.
- (c) Force measurements.
- (d) Electrical measurements.
- (e) Relative humidity measurements.
- (f) Linear measurements.

Deviations from these measurement uncertainties shall be justified.

6.3 Higher requirements

If, according to the information in the accompanying documents, the control system fulfils higher requirements than the requirements according to this standard, the higher requirements shall apply.

NOTE: Such higher requirements can apply if the control system has to withstand particularly adverse service conditions, e.g. rough handling, humidity effects, hydrolysis, ambient temperature variations, effects of chemical agents, corrosion, high strength of electromagnetic fields, for example due to close proximity of transmitters.

6.4 Number of test samples

Unless otherwise specified, the tests shall be made on a single production sample of the safety-related part(s) which should withstand all the relevant tests.

Safety-related part(s) under test shall not be modified during the course of the tests.

Some tests can permanently change the performance of some components. Where the permanent change in the components causes the safety-related part(s) to be outside its design specification a new sample(s) shall be used for subsequent tests.

Where a particular test is destructive and equivalent results can be obtained by testing part of the safety-related part(s) of the control system providing the safety function in isolation, a sample of that part may be used instead of the whole safety-related part(s) for the purpose of obtaining the results of the test. This approach shall only be applied where it has been shown by analysis that testing of the safety-related part(s) is sufficient to demonstrate the safety performance of the whole safety-related part providing the safety function.

7 VALIDATION OF SAFETY FUNCTIONS

An important step is the validation of the safety functions provided by the safety-related parts of the control system for complete compliance with their specified characteristics. In the validation process it is important to check for errors and particularly for omissions in the formulated specification, provided with the design rationale.

The aim of validation of the safety functions is to ascertain that the safety-related output signals are correct and logically dependent on the input signals according to the specification. The validation should cover all normal and foreseeable abnormal conditions in static and dynamic simulation.

The specified safety functions (in accordance with AS 4024.1501) shall be validated in all operating modes of the machine. This means that validation shall be carried out to demonstrate correct functionality in different configurations sufficient to ensure that all safety-related outputs are realized over their complete ranges. Tests (e.g. overload tests) may be necessary to validate the specified safety functions; and in response to foreseeable abnormal signal from any input source including power interruption and restoration.

NOTE: Where appropriate, combinations of different configurations should be considered.

8 VALIDATION OF CATEGORIES

8.1 Analysis and testing of categories

The validation of categories shall demonstrate that their requirements are fulfilled. Principally, the following methods are applicable:

- (a) An analysis from circuit diagrams (see Clause 5).
- (b) Tests on the actual circuit and fault simulation on actual components, particularly in areas of doubt, regarding performance identified during the analysis (see Clause 6).
- (c) A simulation of control system behaviour, e.g. by means of hardware and/or software models.

In some applications it may be necessary to divide the connected safety-related parts into several functional groups and to submit these groups and their interfaces to fault simulation tests.

When carrying out validation by testing, the tests may include as appropriate—

- (i) fault injection tests into a production sample;
- (ii) fault injection tests into a hardware model;
- (iii) software simulation of faults; or
- (iv) subsystem failure, e.g. power supplies.

The precise instant at which a fault is injected into a system can be critical. The worst case effect of a fault injection should be determined by analysis and, according to this analysis, the fault should be injected at the appropriate critical time.

8.2 Validation of category specifications

8.2.1 *Category B*

The safety-related parts of control systems to category B shall be validated in accordance with basic safety principles by demonstrating that the specification, design, construction and choice of components are in accordance with AS 4024.1501. This shall be achieved by checking that the safety-related part(s) of control systems are in accordance with its specification as provided in the documents for validation. For the validation of environmental conditions see Clause 6.1.

8.2.2 *Category 1*

Safety-related parts of control systems to category 1 shall be validated by demonstrating the following:

- (a) They meet the requirements of category B.
- (b) Components are well-trying by meeting at least one of the following conditions—
 - (i) they have been widely used with successful results in similar applications; or
 - (ii) they have been made using principles which demonstrate their suitability and reliability for safety-related applications.
- (c) Well-trying safety principles have been implemented correctly.
- (d) Where newly developed principles have been used then validation shall show—
 - (i) how the expected modes of failure have been avoided; and
 - (ii) how faults have been avoided or their probability has been reduced.

Relevant component standards may be used to demonstrate compliance with this Clause.

8.2.3 *Category 2*

Safety-related parts of control systems to category 2 shall be validated by demonstrating the following:

- (a) They meet the requirements of category B.
- (b) The well-trying safety principles used (if applicable) meet the requirements of Clause 8.2.2(c).
- (c) The checking equipment detects all relevant faults applied one at a time during the checking process and generates an appropriate control action which—
 - (i) initiates a safe state; or when this is not possible; and
 - (ii) provides a warning of the hazard.
- (d) The check(s) provided by checking equipment do not introduce an unsafe state.
- (e) The initiation of the check is carried out—
 - (i) at the machine start-up and prior to the initiation of an hazardous situation; and
 - (ii) periodically during operation if the risk assessment and the kind of operations show that it is necessary.

8.2.4 *Category 3*

Safety-related parts of control systems to category 3 shall be validated by demonstrating the following:

- (a) They meet the requirements of category B.
- (b) The well-trying safety principles (if applicable) meet the requirements of Clause 8.2.2(c).
- (c) A single fault does not lead to the loss of the safety function.
- (d) Single faults (including common mode faults) are detected in accordance with the design rationale.

8.2.5 *Category 4*

Safety-related parts of control systems to category 4 shall be validated by demonstrating that—

- (a) they meet the requirements of category B;
- (b) the well-tries safety principles (if applicable) meet the requirements of Clause 8.2.2 (c);
- (c) a single fault (including common mode faults) does not lead to the loss of the safety function;
- (d) the single faults are detected at or before the next demand on the safety function; and
- (e) if it is not possible to meet the requirement at Item (d), an accumulation of faults does not lead to the loss of the safety function(s). The extent of the accumulation of faults considered shall be in accordance with the design rationale.

8.3 Validation of combination of safety-related parts

Where the safety function is implemented by two or more safety-related parts, validation of the combination (by analysis and, if necessary, by testing) shall be undertaken to establish that the combination achieves the performance specified in the design. Existing recorded validation results of safety-related parts can be taken into account.

9 VALIDATION OF ENVIRONMENTAL REQUIREMENTS

The performance specified in the design for the safety-related parts of the control system shall be validated with respect to the environmental conditions specified for the control system.

Validation shall be carried out by analysis and, if necessary by testing. The extent of the analysis and of the testing will depend upon the safety-related parts, the system in which they are installed, the technology used, and the environmental condition(s) which is being validated. The use of operational reliability data on the system or its components, or the confirmation of compliance to appropriate environmental standards (e.g. for waterproofing or vibration protection) may assist this validation process.

Where applicable validation shall address—

- (a) expected mechanical stresses from shock, vibration or ingress of contaminants;
- (b) mechanical durability;
- (c) electrical ratings and power supplies;
- (d) climatic conditions (temperature and humidity); and
- (e) electromagnetic compatibility (immunity).

When testing is necessary to determine compliance with the environmental requirements, the procedures outlined in the relevant Standards shall be followed as far as required for the application.

After the completion of validation by testing, the safety functions shall continue to be in accordance with the specifications for the safety requirements, or the safety-related parts of the control system shall provide output(s) for a safe state.

10 VALIDATION OF MAINTENANCE REQUIREMENTS

The validation process shall demonstrate that the maintenance requirements as specified in AS 4024.1501 have been implemented.

APPENDIX A

VALIDATION TOOLS FOR MECHANICAL SYSTEMS

(Informative)

A1 INTRODUCTION

When mechanical systems are used in conjunction with other technologies, then relevant tables for basic safety and well-tried safety principles should also be taken into account. For further fault exclusions see Clause 4.3.

A2 LIST OF BASIC SAFETY PRINCIPLES

A list of basic safety principles for mechanical systems is given in Table A1.

TABLE A1
BASIC SAFETY PRINCIPLES

Basic safety principles	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature.
Correct dimensioning and shaping	Consider e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components/systems.
Use of de-energization principle	The safe state is obtained by release of energy. See primary action for stopping in AS 4024.1201. Energy is supplied for starting the movement of a mechanism. See primary action for starting in AS 4024.1202. Consider different modes, e.g. operation mode, maintenance mode. This principle should not be used in special applications, e.g. to keep energy for clamping devices.
Proper fastening	For the application of screw locking consider manufacturer's application notes. Overloading can be avoided by applying adequate torque loading technology.
Limitation of the generation or transmission of force and similar parameters	Examples are break pin, break plate, torque limiting clutch.
Limitation of range of environmental parameters	Examples of parameters are temperature, humidity and pollution at the installation place. See Clause 8 and consider manufacturer's application notes.
Limitation of speed and similar parameters	Consider for example the speed, acceleration, deceleration required by the application
Proper reaction time	Consider for example spring relaxation, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.

(continued)

TABLE A1 (continued)

Basic safety principles	Remarks
Protection against unexpected start-up	Consider unexpected start-up caused by stored energy and after power 'supply' restoration for different modes as operation mode, maintenance mode etc. Special equipment for release of stored energy may be necessary. Special applications, e.g. to keep energy for clamping devices or ensure a position, need to be considered separately.
Simplification	Reduce the number of components in the safety-related system.
Separation	Separation of safety-related functions from other functions.
Proper lubrication	—
Proper prevention of the ingress of fluids and dust	Consider IP rating see AS 60529

A3 LIST OF WELL-TRIED SAFETY PRINCIPLES

A list of well-tried safety principles for mechanical systems is given in Table A2.

TABLE A2
WELL-TRIED SAFETY PRINCIPLES

Well-tried safety principles	Remarks
Use of carefully selected materials and manufacturing	Selection of suitable material, adequate manufacturing methods and treatments related to the application.
Use of components with oriented failure mode	The predominant failure mode of a component is known in advance and always the same, see AS 4024.1202.
Over-dimensioning/safety factor	The safety factors are given in standards or by good experience in safety-related applications
Safe position	The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed for changing the position.
Increased OFF force	A safe position/state is obtained by an increased OFF force in relation to ON force
Carefully selection, combination, arrangement, assembly and installation of components/system related to the application	—
Carefully selection of fastening related to the application	Avoid relying only on friction
Positive mechanical action	Dependent operation (e.g. parallel operation) between parts is obtained by positive mechanical link(s). Springs and similar 'flexible' elements should not be part of the link(s), see AS 4024.1202.
Multiple parts	Reducing the effect of faults by multiplying parts, e.g. where a fault in one spring (of many springs) does not lead to a dangerous condition.

(continued)