



JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS B 9705-1 : 2011

(ISO 13849-1 : 2006)

(JMF)

**Safety of machinery—Safety-related
parts of control systems—Part 1:
General principles for design**

ICS 13.110

Reference number : JIS B 9705-1 : 2011 (E)

PROTECTED BY COPYRIGHT

Date of Establishment: 2000-11-20

Date of Revision: 2011-07-25

Date of Public Notice in Official Gazette: 2011-07-25

Investigated by: Japanese Industrial Standards Committee
Standards Board

Technical Committee on Industrial Machinery

JIS B 9705-1:2011, First English edition published in 2012-02

Translated and published by: Japanese Standards Association
4-1-24, Akasaka, Minato-ku, Tokyo, 107-8440 JAPAN

In the event of any doubts arising as to the contents,
the original JIS is to be the final authority.

© JSA 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

Printed in Japan

PROTECTED BY COPYRIGHT

Contents

	Page
Introduction.....	1
1 Scope.....	3
2 Normative references	4
3 Terms, definitions, symbols and abbreviated terms	5
3.1 Terms and definitions	5
3.2 Symbols and abbreviated terms	10
4 Design considerations	11
4.1 Safety objectives in design	11
4.2 Strategy for risk reduction.....	13
4.3 Determination of required performance level (PL _r)	17
4.4 Design of SRP/CS	17
4.5 Evaluation of the achieved performance level PL and relationship with SIL	18
4.6 Software safety requirements	24
4.7 Verification that achieved PL meets PL _r	30
4.8 Ergonomic aspects of design	30
5 Safety functions	31
5.1 Specification of safety functions.....	31
5.2 Details of safety functions	33
6 Categories and their relation to MTTF _d of each channel, DC _{avg} and CCF	36
6.1 General.....	36
6.2 Specifications of categories	37
6.3 Combination of SRP/CS to achieve overall PL	45
7 Fault consideration, fault exclusion	46
7.1 General.....	46
7.2 Fault consideration	46
7.3 Fault exclusion.....	47
8 Validation	47
9 Maintenance	47
10 Technical documentation.....	47
11 Information for use	48
Annex A (informative) Determination of required performance level (PL _r)	50
Annex B (informative) Block method and safety-related block diagram	53

Annex C (informative)	Calculating or evaluating $MTTF_d$ values for single components	55
Annex D (informative)	Simplified method for estimating $MTTF_d$ for each channel	63
Annex E (informative)	Estimates for diagnostic coverage (DC) for functions and modules	65
Annex F (informative)	Estimates for common cause failure (CCF)	68
Annex G (informative)	Systematic failure	70
Annex H (informative)	Example of combination of several safety-related parts of the control system	73
Annex I (informative)	Examples	76
Annex J (informative)	Software	84
Annex K (informative)	Numerical representation of figure 5	87
Bibliography		90

Foreword

This translation has been made based on the original Japanese Industrial Standard revised by the Minister of Health, Labour and Welfare and the Minister of Economy, Trade and Industry through deliberations at the Japanese Industrial Standards Committee as the result of proposal for revision of Japanese Industrial Standard submitted by The Japan Machinery Federation (JMF) with the draft being attached, based on the provision of Article 12 Clause 1 of the Industrial Standardization Law applicable to the case of revision by the provision of Article 14.

Consequently **JIS B 9705-1:2000** is replaced with this Standard.

This **JIS** document is protected by the Copyright Law.

Attention is drawn to the possibility that some parts of this Standard may conflict with a patent right, application for a patent after opening to the public or utility model right which have technical properties. The relevant Ministers and the Japanese Industrial Standards Committee are not responsible for identifying the patent right, application for a patent after opening to the public or utility model right which have the said technical properties.

Safety of machinery—Safety-related parts of control systems—

Part 1: General principles for design

Introduction

This Japanese Industrial Standard has been prepared based on the second edition of **ISO 13849-1** published in 2006 without modifying the technical contents.

The portions with dotted underlines are the matters not given in the corresponding International Standard.

The structure of safety standards in the field of machinery is as follows as stated in **JIS B 9700-1**.

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

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-hand controls, interlocking devices, pressure sensitive devices, guards).

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

JIS B 9705-1 is a Type-B-1 standard as stated in **JIS B 9700-1**.

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.

JIS B 9705-1 is intended to give guidance to those involved in the design and assessment of control systems, and to those developing Type-B2 or Type-C standards.

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 and 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 of 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 Standard 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 Standard 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.

JIS B 9961 and this Standard specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. The following table summarizes the scopes of **JIS B 9961** and this Standard.

Table 1 Recommended application of JIS B 9961 and JIS B 9705-1

Technology implementing the safety-related control function(s)		JIS B 9705-1	JIS B 9961
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 SIL3
C	Complex electronics, e.g. programmable	Restricted to designated architectures ^{a)} and up to PL = d	All architectures and up to SIL3
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 ^{a)} and up to PL = d	All architectures and up to SIL3
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 Standard shown in the column heading.			
Notes ^{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 Standard up to PL = d or any architecture according to JIS B 9961 . ^{c)} For non-electrical technology, use parts in accordance with this Standard as subsystems.			

1 Scope

This Standard 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 Standard 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 (programmable logic controllers), 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 Standards, e.g. **JIS B 9712**, **JIS B 9717-1** and **ISO 13856-2**.

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

NOTE 3 The requirements provided in this Standard 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 **JIS B 9961**.

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

NOTE 5 See also table 1.

NOTE 6 The International Standard corresponding to this Standard and the symbol of degree of correspondence are as follows.

ISO 13849-1:2006 *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design* (IDT)

In addition, symbols which denote the degree of correspondence in the contents between the relevant International Standard and **JIS** are IDT (identical), MOD (modified), and NEQ (not equivalent) according to **ISO/IEC Guide 21-1**.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. The most recent editions (including amendments) indicated below shall be applied.

JIS B 9700-1 *Safety of machinery—Basic concepts, general principles for design—Part 1: Basic terminology, methodology*

NOTE : Corresponding International Standard: ISO 12100-1 *Safety of machinery—Basic concepts, general principles for design—Part 1: Basic terminology, methodology* (IDT)

JIS B 9700-2 *Safety of machinery—Basic concepts, general principles for design—Part 2: Technical principles*

NOTE : Corresponding International Standard: ISO 12100-2 *Safety of machinery—Basic concepts, general principles for design—Part 2: Technical principles* (IDT)

JIS B 9702 *Safety of machinery—Principles of risk assessment*

NOTE : Corresponding International Standard: ISO 14121 *Safety of machinery—Principles of risk assessment* (IDT)

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

IEC 60050-191 *International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*, Amd.1:1999 and Amd.2:2002

IEC 61508-3 *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements* and Corr.1:1999

IEC 61508-4 *Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4: Definitions and abbreviations* and Corr.1:1999

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in **JIS B 9700-1** and **IEC 60050-191** and the following apply.

3.1.1 safety-related part of a control system, SRP/CS

part of a control system that responds to safety-related input signals and generates safety-related output signals

NOTE 1 The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

NOTE 2 If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

3.1.2 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, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

3.1.3 fault

state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE 1 A fault is often the result of a failure of the item itself, but may exist without prior failure.

(See **IEC 60050-191, 05-01.**)

NOTE 2 In this Standard, “fault” means random fault.

NOTE 3 “Fault” is translated into Japanese as “HUGUAI (SYÔGAI)” in **JIS B 9700-1** which has the same meaning as “SYÔGAI” defined in this Standard. “HUGUAI” is mainly used for machineries.

3.1.4 failure

termination of the ability of an item to perform a required function

NOTE 1 After a failure, the item has a fault.

NOTE 2 “Failure” is an event, as distinguished from “fault”, which is a state.

NOTE 3 The concept as defined does not apply to items consisting of software only.

(See **IEC 60050-191, 04-01.**)

NOTE 4 Failures which only affect the availability of the process under control are outside of the scope of this Standard.

3.1.5 dangerous failure

failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

NOTE : Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

(Adapted from **IEC 61508-4**, definition **3.6.7**.)

3.1.6 common cause failure, CCF

failures of different items, resulting from a single event, where these failures are not consequences of each other

(See **IEC 60050-191** Amd.1, **04-23**.)

NOTE : Common cause failures should not be confused with common mode failures.

3.1.7 systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

(See **IEC 60050-191**, **04-19**.)

NOTE 3 Examples of causes of systematic failures include human error in

- the safety requirements specification,
- the design, manufacture, installation, operation of the hardware, and
- the design, implementation, etc., of the software.

3.1.8 muting

temporary automatic suspension of a safety function(s) by the SRP/CS

3.1.9 manual reset

function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.10 harm

physical injury or damage to health

(See **JIS B 9700-1**, **3.5**.)

3.1.11 hazard

potential source of harm

NOTE 1 A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, fire hazard).

NOTE 2 The hazard envisaged in this definition:

- either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);
- or may appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

(See **JIS B 9700-1, 3.6.**)

3.1.12 hazardous situation

circumstance in which a person is exposed to at least one hazard, the exposure having immediately or over a long period of time the potential to result in harm

(See **JIS B 9700-1, 3.9.**)

3.1.13 risk

combination of the probability of occurrence of harm and the severity of that harm

(See **JIS B 9700-1, 3.11.**)

3.1.14 residual risk

risk remaining after protective measures have been taken

See figure 2.

(Adapted from **JIS B 9700-1**, definition **3.12.**)

3.1.15 risk assessment

overall process comprising risk analysis and risk evaluation

(See **JIS B 9700-1, 3.13.**)

3.1.16 risk analysis

combination of the specification of the limits of the machine, hazard identification and risk estimation

(See **JIS B 9700-1, 3.14.**)

3.1.17 risk evaluation

judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

(See **JIS B 9700-1, 3.16.**)

3.1.18 intended use of a machine

use of the machine in accordance with the information provided in the instructions for use

(See **JIS B 9700-1, 3.22.**)

3.1.19 reasonably foreseeable misuse

use of a machine in a way not intended by the designer, but which may result from readily predictable human behaviour

(See **JIS B 9700-1, 3.23.**)

3.1.20 safety function

function of the machine whose failure can result in an immediate increase of the risk(s)

(See **JIS B 9700-1, 3.28.**)

3.1.21 monitoring

safety function which ensures that a protective measure is initiated if the ability of a component or an element to perform its function is diminished or if the process conditions are changed in such a way that a decrease of the amount of risk reduction is generated

3.1.22 programmable electronic system, PES

system for control, protection or monitoring dependent for its operation on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, contactors and other output devices

(Adapted from **IEC 61508-4**, definition **3.3.2.**)

3.1.23 performance level, PL

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

NOTE : See **4.5.1.**

3.1.24 required performance level, PL_r

performance level (PL) applied in order to achieve the required risk reduction for each safety function

See figures 2 and **A.1.**

3.1.25 mean time to dangerous failure, MTTF_d

expectation of the mean time to dangerous failure

(Adapted from **JIS B 9961**, definition **3.2.34.**)

3.1.26 diagnostic coverage, DC

measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

NOTE : Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements.

(Adapted from **IEC 61508-4**, definition **3.8.6.**)

3.1.27 protective measure

measure intended to achieve risk reduction

Example 1 Implemented by the designer: inherent design, safeguarding and complementary protective measures, information for use.

Example 2 Implemented by the user: organization (safe working procedures, supervision, permit-to-work systems), provision and use of additional safeguards, personal protective equipment, training.

(Adapted from **JIS B 9700-1**, definition **3.18**.)

3.1.28 mission time, T_M

period of time covering the intended use of an SRP/CS

3.1.29 test rate, r_t

frequency of automatic tests to detect faults in an SRP/CS, reciprocal value of diagnostic test interval

3.1.30 demand rate, r_d

frequency of demands for a safety-related action of the SRP/CS

3.1.31 repair rate, r_r

reciprocal value of the period of time between detection of a dangerous failure by either an online test or obvious malfunction of the system and the restart of operation after repair or system/component replacement

NOTE : The repair time does not include the span of time needed for failure-detection.

3.1.32 machine control system

system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

NOTE : The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic, mechanical).

3.1.33 safety integrity level, SIL

discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE (electric/electronic/programmable electronic) safety-related systems, where safety integrity level 4 (SIL4) has the highest level of safety integrity and safety integrity level 1 (SIL1) has the lowest

(See **IEC 61508-4**, **3.5.6**.)

3.1.34 limited variability language, LVL

type of language that provides the capability of combining predefined, application-specific library functions to implement the safety requirements specifications

(Adapted from **IEC 61511-1**, definition **3.2.81.1.2**.)

NOTE 1 Typical examples of LVL (ladder logic, function block diagram) are given in **JIS B 3503**.

NOTE 2 A typical example of a system using LVL: PLC.

3.1.35 full variability language, FVL

type of language that provides the capability of implementing a wide variety of functions and applications

Example : C, C++, Assembler.

(Adapted from **IEC 61511-1**, definition **3.2.81.1.3**.)

NOTE 1 A typical example of systems using FVL: embedded systems.

NOTE 2 In the field of machinery, FVL is found in embedded software and rarely in application software.

3.1.36 application software

software specific to the application, implemented by the machine manufacturer, and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the SRP/CS requirements

3.1.37 embedded software, firmware, system software

software that is part of the system supplied by the control manufacturer and which is not accessible for modification by the user of the machinery

NOTE : Embedded software is usually written in FVL.

3.2 Symbols and abbreviated terms

See table 2.

Table 2 Symbols and abbreviated terms

Symbol or abbreviation	Description	Definition or occurrence
a, b, c, d, e	Denotation of performance levels	Table 3
AOPD	Active optoelectronic protective device (e.g. light barrier)	Annex H
B, 1, 2, 3, 4	Denotation of categories	Table 7
B_{10d}	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)	Annex C
Cat.	Category	3.1.2
CC	Current converter	Annex I
CCF	Common cause failure	3.1.6
DC	Diagnostic coverage	3.1.26
DC_{avg}	Average diagnostic coverage	E.2
F, F1, F2	Frequency and/or time of exposure to the hazard	A.2.2
FB	Function block	4.6.3
FVL	Full variability language	3.1.35
FMEA	Failure modes and effects analysis	7.2

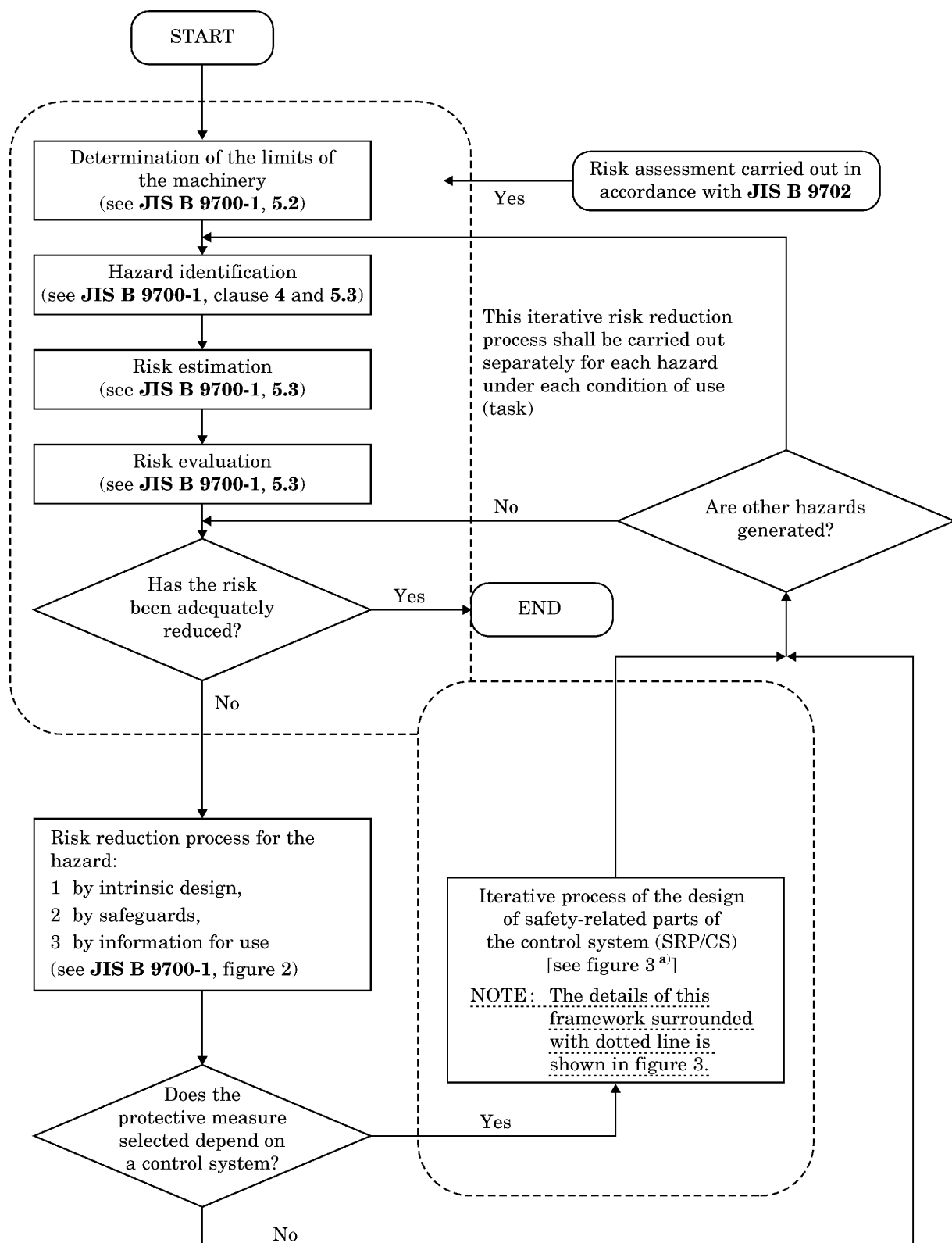
Table 2 (concluded)

Symbol or abbreviation	Description	Definition or occurrence
I, I1, I2	Input device, e.g. sensor	6.2
i, j	Index for counting	Annex D
I/O	Inputs/outputs	Table E.1
i_{ab}, i_{bc}	Interconnecting means	Figure 4
K1A, K1B	Contactors	Annex I
L, L1, L2	Logic	6.2
LVL	Limited variability language	3.1.34
M	Motor	Annex I
MTTF	Mean time to failure	Annex C
MTTF _d	Mean time to dangerous failure	3.1.25
$n, N, \tilde{N}$	Number of items	6.3, D.1
N_{low}	Number of SRP/CS with PL _{low} in a combination of SRP/CS	6.3
O, O1, O2, OTE	Output device, e.g. actuator	6.2
P, P1, P2	Possibility of avoiding the hazard	A.2.3
PES	Programmable electronic system	3.1.22
PL	Performance level	3.1.23
PLC	Programmable logic controller	Annex I
PL _{low}	Lowest performance level of an SRP/CS in a combination of SRP/CS	6.3
PL _r	Required performance level	3.1.24
r_d	Demand rate	3.1.30
RS	Rotation sensor	Annex I
S, S1, S2	Severity of injury	A.2.1
SW1A, SW1B, SW2	Position switches	Annex I
SIL	Safety integrity level	Table 4
SRASW	Safety-related application software	4.6.3
SRESW	Safety-related embedded software	4.6.2
SRP	Safety-related part	General
SRP/CS	Safety-related part of a control system	3.1.1
TE	Test equipment	6.2
T_M	Mission time	3.1.28

4 Design considerations

4.1 Safety objectives in design

The SRP/CS shall be designed and constructed so that the principles of **JIS B 9700-1** and **JIS B 9702** are fully taken into account (see figures 1 and 3). All intended use and reasonable foreseeable misuse shall be considered.



Note ^{a)} Refers to this Standard, figure 3.

Figure 1 Overview of risk assessment/risk reduction

4.2 Strategy for risk reduction

4.2.1 General

The strategy for risk reduction at the machine is given in **JIS B 9700-1**, clause 5, and further guidance is given in **JIS B 9700-2**, clauses 4 and 5. This strategy covers the whole life cycle of the machine.

The hazard analysis and risk reduction process for a machine requires that hazards are eliminated or reduced through a hierarchy of measures:

- hazard elimination or risk reduction by design (see **JIS B 9700-2**, clause 4);
- risk reduction by safeguarding and possibly complementary protective measures (see **JIS B 9700-2**, clause 5);
- risk reduction by the provision of information for use about the residual risk (see **JIS B 9700-2**, clause 6).

4.2.2 Contribution to the risk reduction by the control system

The purpose in following the overall design procedure for the machine is to achieve the safety objectives (see 4.1). The design of the SRP/CS to provide the required risk reduction is an integral subset of the overall design procedure for the machine. The SRP/CS provides safety function(s) at a PL which achieves the required risk reduction. In providing safety function(s), either as an inherently safe part of the design or as a control for a safeguard or protective device, the design of the SRP/CS is a part of the strategy for risk reduction. This is an iterative process and is illustrated in figures 1 and 3.

For each safety function, the characteristics (see clause 5) and the required performance level shall be specified and documented in the safety requirements specification.

In this Standard the performance levels are defined in terms of probability of dangerous failure per hour. Five performance levels (a to e) are set out, with defined ranges of probability of a dangerous failure per hour (see table 3).

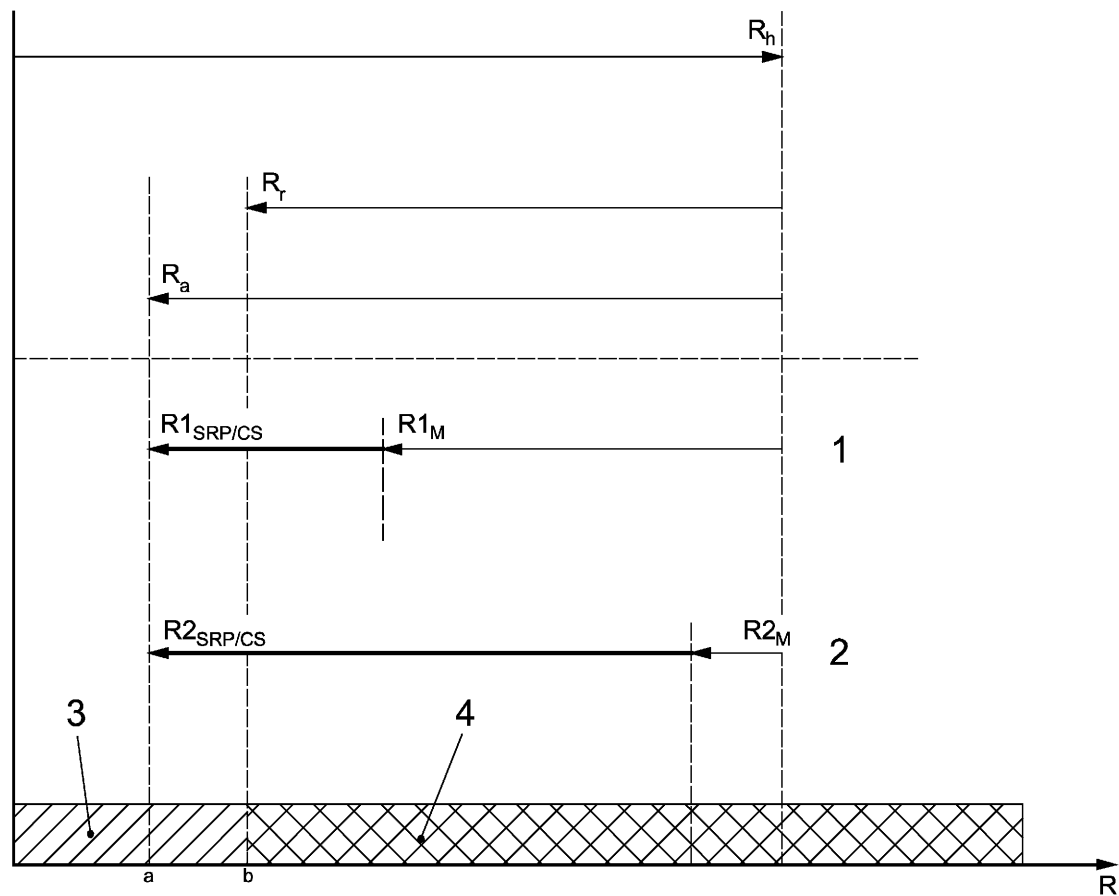
Table 3 Performance levels (PL)

PL	Average probability of dangerous failure per hour (<i>PFH</i> _d) [1/h]
a	$10^{-5} \leq PFH_d < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH_d < 10^{-5}$
c	$10^{-6} \leq PFH_d < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH_d < 10^{-6}$
e	$10^{-8} \leq PFH_d < 10^{-7}$
NOTE : Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.	

From the risk assessment (see **JIS B 9702**) at the machine, the designer shall decide the contribution to the reduction of risk which needs to be provided by each relevant safety function which is carried out by the SRP/CS(s). 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 is considered, but that part of risk reduced by the application of particular safety functions. Examples of such functions are the stopping function initiated by using an electro-sensitive protective device on a press or the door-locking function of a washing machine.

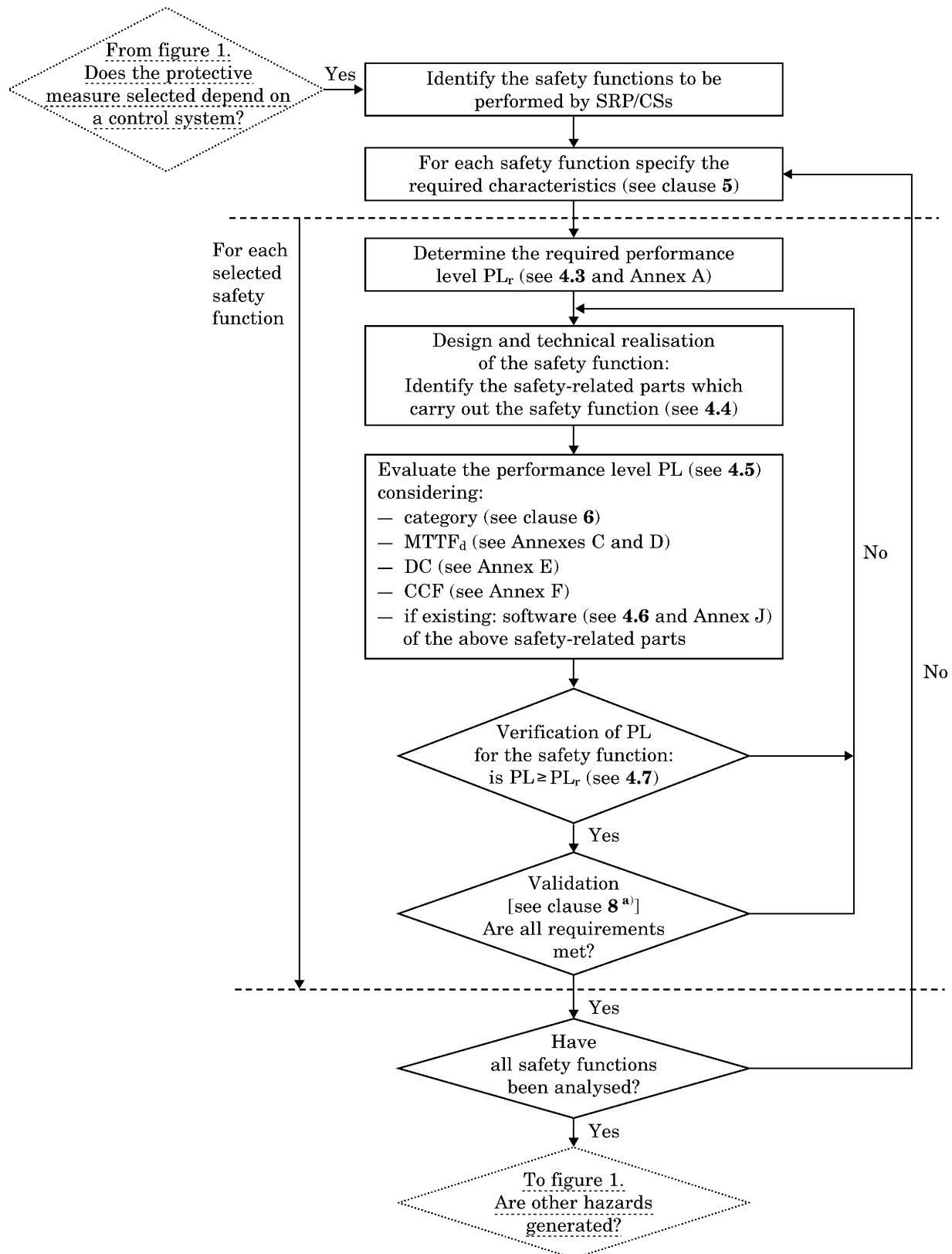
Risk reduction can be achieved by applying various protective measures (both SRP/CS and non SRP/CS) with the end result of achieving a safe condition (see figure 2).



Key

- R_h for a specific hazardous situation, the risk before protective measures are applied
 - R_r risk reduction required from protective measures
 - R_a actual risk reduction achieved with protective measures
 - 1 solution 1 — important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS
 - 2 solution 2 — important part of risk reduction due to the SRP/CS (e.g. light curtain), small part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures)
 - 3 adequately reduced risk
 - 4 inadequately reduced risk
 - R risk
 - a residual risk obtained by solutions 1 and 2
 - b adequately reduced risk
 - $R1_{SRP/CS}$, $R2_{SRP/CS}$ risk reduction from the safety function carried out by the SRP/CS
 - $R1_M$, $R2_M$ risk reduction from protective measures other than SRP/CS (e.g. mechanical measures)
- NOTE : See **JIS B 9700** series for further information on risk reduction.

Figure 2 Overview of the risk reduction process for each hazardous situation



Note ^{a)} ISO 13849-2 provides additional help for the validation.

Figure 3 Iterative process for design of safety-related parts of control systems (SRP/CS)

4.3 Determination of required performance level (PL_r)

For each selected safety function to be carried out by an SRP/CS, a required performance level (PL_r) shall be determined and documented (see Annex A for guidance on determining PL_r). The determination of the required performance level is the result of the risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system (see figure 2).

The greater the amount of risk reduction required to be provided by the SRP/CS, the higher the PL_r shall be.

4.4 Design of SRP/CS

Part of the risk reduction process is to determine the safety functions of the machine. This will include the safety functions of the control system, e.g. prevention of unexpected start-up.

A safety function may be implemented by one or more SRP/CS, and several safety functions may share one or more SRP/CS [e.g. a logic unit, power control element(s)]. It is also possible that one SRP/CS implements safety functions and standard control functions. The designer may use any of the technologies available, singly or in combination. SRP/CS may also provide an operational function (e.g. an AOPD as a means of cycle initiation).

A typical safety function diagrammatic presentation is given in figure 4 showing a combination of safety-related parts of control systems (SRP/CS) for

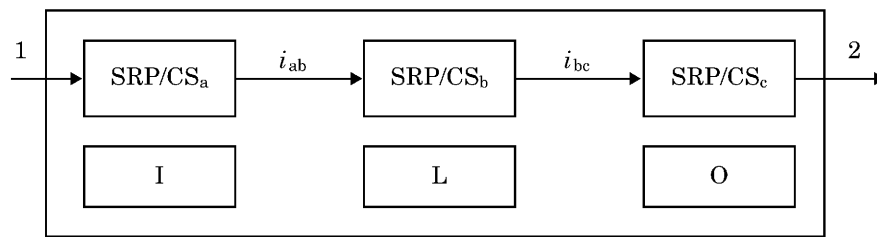
- input (SRP/CS_a),
- logic/processing (SRP/CS_b),
- output/power control elements (SRP/CS_c), and
- interconnecting means (i_{ab} , i_{bc}) (e.g. electrical, optical).

NOTE 1 Within the same machinery it is important to distinguish between different safety functions and their related SRP/CS carrying out a certain safety function.

Having identified the safety functions of the control system, the designer shall identify the SRP/CS (see figures 1 and 3) and, where necessary, shall assign them to input, logic and output and, in the case of redundancy, the individual channels, and then evaluate the performance level PL (see figure 3).

NOTE 2 Designated architectures are given in clause 6.

NOTE 3 All interconnecting means are included in the safety-related parts.



Key

I input

L logic

O output

1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)

2 machine actuator (e.g. motor brakes)

Figure 4 Diagrammatic presentation of combination of safety-related parts of control systems for processing typical safety function

4.5 Evaluation of the achieved performance level PL and relationship with SIL

4.5.1 Performance level PL

For the purposes of this Standard, the ability of safety-related parts to perform a safety function is expressed through the determination of the performance level.

For each selected SRP/CS and/or for the combination of SRP/CS that performs a safety function the estimation of PL shall be done.

The PL of the SRP/CS shall be determined by the estimation of the following aspects:

- the $MTTF_d$ value for single components (see Annexes C and D);
- the DC (see Annex E);
- the CCF (see Annex F);
- the structure (see clause 6);
- the behaviour of the safety function under fault condition(s) (see clause 6);
- safety-related software (see 4.6 and Annex J);
- systematic failure (see Annex G);
- the ability to perform a safety function under expected environmental conditions.

NOTE 1 Other parameters, e.g. operational aspects, demand rate, test rate, can have certain influence.

These aspects can be grouped under two approaches in relation to the evaluation process:

- a) quantifiable aspects ($MTTF_d$ value for single components, DC, CCF, structure);

- b) non-quantifiable, qualitative aspects which affect the behaviour of the SRP/CS (behaviour of the safety function under fault conditions, safety-related software, systematic failure and environmental conditions).

Among the quantifiable aspects, the contribution of reliability (e.g. $MTTF_d$, structure) can vary with the technology used. For example, it is possible (within certain limits) for a single channel of safety-related parts of high reliability in one technology to provide the same or higher PL as a fault-tolerant structure of low reliability in another technology.

There are several methods for estimating the quantifiable aspects of the PL for any type of system (e.g. a complex structure), for example, Markov modelling, generalized stochastic petri nets (GSPN), reliability block diagrams (see, e.g. **IEC 61508** series).

To make the assessment of the quantifiable aspects of the PL easier, this Standard provides a simplified method based on the definition of five designated architectures that fulfil specific design criteria and behaviour under a fault condition (see **4.5.4**).

For an SRP/CS or combination of SRP/CS designed according to the requirements given in clause **6**, the average probability of a dangerous failure could be estimated by means of figure 5 and the procedure given in Annexes A to H, J and K.

For an SRP/CS which deviates from the designated architectures, a detailed calculation shall be provided to demonstrate the achievement of the required performance level (PL_r).

In applications where the SRP/CS can be considered simple, and the required performance level is a to c, a qualitative estimation of the PL may be justified in the design rationale.

NOTE 2 For the design of complex control systems, such as PES designed to perform safety functions, the application of other standards can be appropriate (e.g. **IEC 61508** series, **JIS B 9961** or **JIS B 9704** series).

The achievement of qualitative aspects of the PL can be demonstrated by the application of the recommended measures given in **4.6** and Annex G.

In standards in accordance with **IEC 61508** series, the ability of safety-related control systems to perform a safety function is given through a SIL. Table 4 displays the relationship between the two concepts (PLs and SILs).

PL_a has no correspondence on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury. Since SIL4 is dedicated to catastrophic events possible in the process industry, this range is not relevant for risks at machines. Thus PL_e corresponding to SIL3 is defined as the highest level.

Table 4 Relationship between performance level (PL) and safety integrity level (SIL)

PL	SIL high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

Therefore, protective measures to reduce the risk shall be applied, principally the following.

- Reduce the probability of faults at the component level. The aim is to reduce the probability of faults or failures which affect the safety function. This can be done by increasing the reliability of components, e.g. by selection of well-tried components and/or applying well-tried safety principles, in order to minimize or exclude critical faults or failures (see **ISO 13849-2**).
- Improve the structure of the SRP/CS. The aim is to avoid the dangerous effect of a fault. Some faults may be detected and a redundant and/or monitored structure could be needed.

Both measures can be applied separately or in combination. With some technologies, risk reduction can be achieved by selecting reliable components and by fault exclusions; but with other technologies, risk reduction could require a redundant and/or monitored system. In addition, common cause failures (CCF) shall be taken into account (see figure 3).

For architectural constraints, see clause 6.

4.5.2 Mean time to dangerous failure of each channel (MTTF_d)

The value of the MTTF_d of each channel is given in three levels (see table 5) and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

According to MTTF_d, a maximum value of 100 years can be taken into account.

Table 5 Mean time to dangerous failure of each channel (MTTF_d)

MTTF _d	
Denotation of each channel	Range of each channel
Low	3 years ≤ MTTF _d < 10 years
Medium	10 years ≤ MTTF _d < 30 years
High	30 years ≤ MTTF _d ≤ 100 years
NOTE 1 The choice of the MTTF_d ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An MTTF_d value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An MTTF_d value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of MTTF_d of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher MTTF_d values can be used for single components (see table D.1). NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.	

For the estimation of MTTF_d of a component, the hierarchical procedure for finding data shall be, in the order given:

- a) use manufacturer's data;
- b) use methods in Annexes C and D;
- c) choose ten years.

4.5.3 Diagnostic coverage (DC)

The value of the DC is given in four levels (see table 6).

For the estimation of DC, in most cases, failure mode and effects analysis (FMEA, see **IEC 60812**) or similar methods can be used. In this case, all relevant faults and/or failure modes should be considered and the PL of the combination of the SRP/CS which carry out the safety function should be checked against the required performance level (PL_r). For a simplified approach to estimating DC, see Annex E.

Table 6 Diagnostic coverage (DC)

DC	
Denotation	Range
None	$DC < 60 \%$
Low	$60 \% \leq DC < 90 \%$
Medium	$90 \% \leq DC < 99 \%$
High	$99 \% \leq DC$
NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in figure 5, clause 6 and E.2. NOTE 2 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 series) dealing with diagnostic coverage of tests. Investigations show that $(100 - DC) \%$ rather than DC itself is a characteristic measure for the effectiveness of the test. $(100 - DC) \%$ 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 %.	

4.5.4 Simplified procedure for estimating PL

The PL may be estimated by taking into account all relevant parameters and the appropriate methods for calculation (see 4.5.1).

This clause describes a simplified procedure for estimating the PL of an SRP/CS based on designated architectures. Some other architectures with similar structure may be transformed to these designated architectures in order to obtain an estimation of the PL.

The designated architectures are represented as block diagrams, and are listed in the context of each category in 6.2. Information about the block method and the safety-related block diagrams are given in 6.2 and Annex B.

The designated architectures show a logical representation of the system structure for each category. The technical realization or, for example, the functional circuit diagram, may look completely different.

The designated architectures are drawn for the combined SRP/CS, starting at the points where the safety-related signals are initiated and ending at the output of the power control elements (see also JIS B 9700-1, Annex A). The designated architectures can also be used to describe a part of subpart of a control system that responds to input signals and generates safety-related output signals. Thus the “input” element can represent, for example, a light curtain (AOPD) as well as input circuits of control logic elements or input switches. “Output” can also represent, for example, an output signal switching device (OSSD) or outputs of laser-scanners.

For the designated architectures, the following typical assumptions are made:

- mission time, 20 years (see clause 10);
- constant failure rates within the mission time;

- for category 2, demand rate $\leq 1/100$ test rate;
- for category 2, $MTTF_{d,TE}$ larger than half of $MTTF_{d,L}$.

NOTE : When blocks of each channel cannot be separated, the following can be applied: $MTTF_d$ of the summarized test channel (TE, OTE) larger than half $MTTF_d$ of the summarized functional channel (I, L, O).

The methodology considers the categories as architectures with defined DC_{avg} . The PL of each SRP/CS depends on the architecture, the mean time to dangerous failure ($MTTF_d$) in each channel and the DC_{avg} .

Common cause failures (CCF) should also be taken into account (for guidance, see Annex F).

For SRP/CS with software, the requirements of **4.6** apply.

If quantitative data is not available or not used (e.g. low complexity systems), the worst case of all relevant parameters should be chosen.

A combination of SRP/CS or a single SRP/CS may have a PL. The combination of several SRP/CS with different PL is considered in **6.3**.

In the case of applications with PL_r a to c, measures to avoid faults can be sufficient; for higher risk applications, PL_r d to e, the structure of the SRP/CS can provide measures for avoiding, detecting or tolerating faults. Practical measures include redundancy, diversity, monitoring (see also **JIS B 9700-2**, clause **3** and **JIS B 9960-1**).

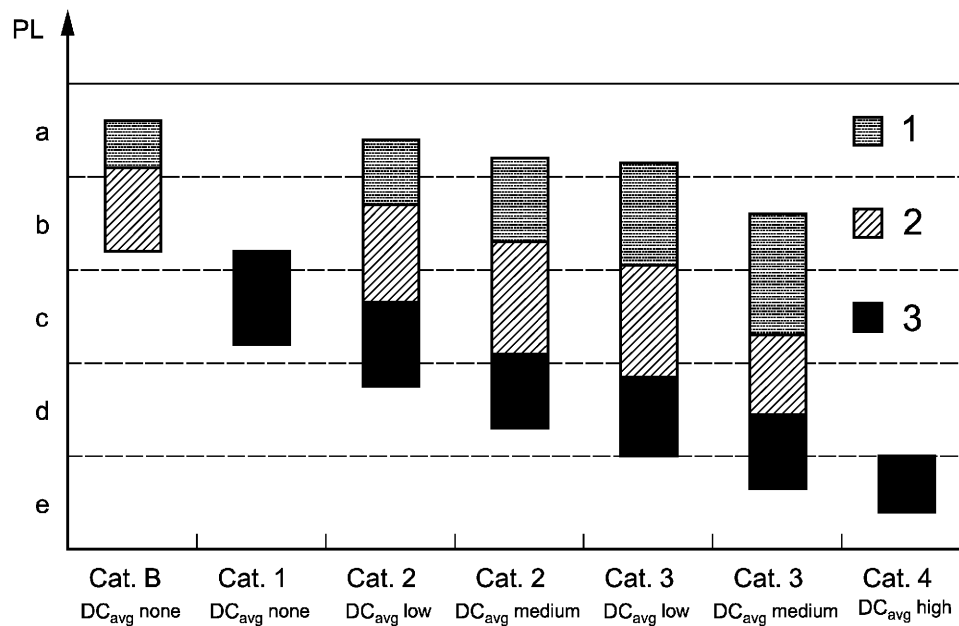
Figure 5 shows the procedure for the selection of categories in combination with the $MTTF_d$ of each channel and DC_{avg} to achieve the required PL of the safety function.

For the estimation of the PL, figure 5 gives the different possible combinations of category with DC_{avg} (horizontal axis) and the $MTTF_d$ of each channel (bars). The bars in the diagram represent the three $MTTF_d$ ranges of each channel (low, medium and high) which can be selected to achieve the required PL.

Before using this simplified approach with figure 5 (which represents results of different Markov models based on designated architectures of clause **6**), the category of the SRP/CS as well as DC_{avg} and the $MTTF_d$ of each channel shall be determined (see clause **6** and Annexes C to E).

For categories 2, 3 and 4, sufficient measures against common cause failure shall be carried out (for guidance, see Annex F). Taking these parameters into account, figure 5 provides a graphical method for determining the PL, achieved by the SRP/CS. The combination of category (including common cause failure) and DC_{avg} determines which column of figure 5 is to be chosen. According to the $MTTF_d$ of each channel, one of the three different shaded areas of the relevant column shall be chosen.

The vertical position of this area determines the achieved PL which can be read off the vertical axis. If the area covers two or three possible PLs, the PL achieved is given in table 7. For a more precise numerical selection of PL depending on the precise value of $MTTF_d$ of each channel, see Annex K.



Key

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Figure 5 Relationship between categories, DC_{avg} , $MTTF_d$ of each channel and PL

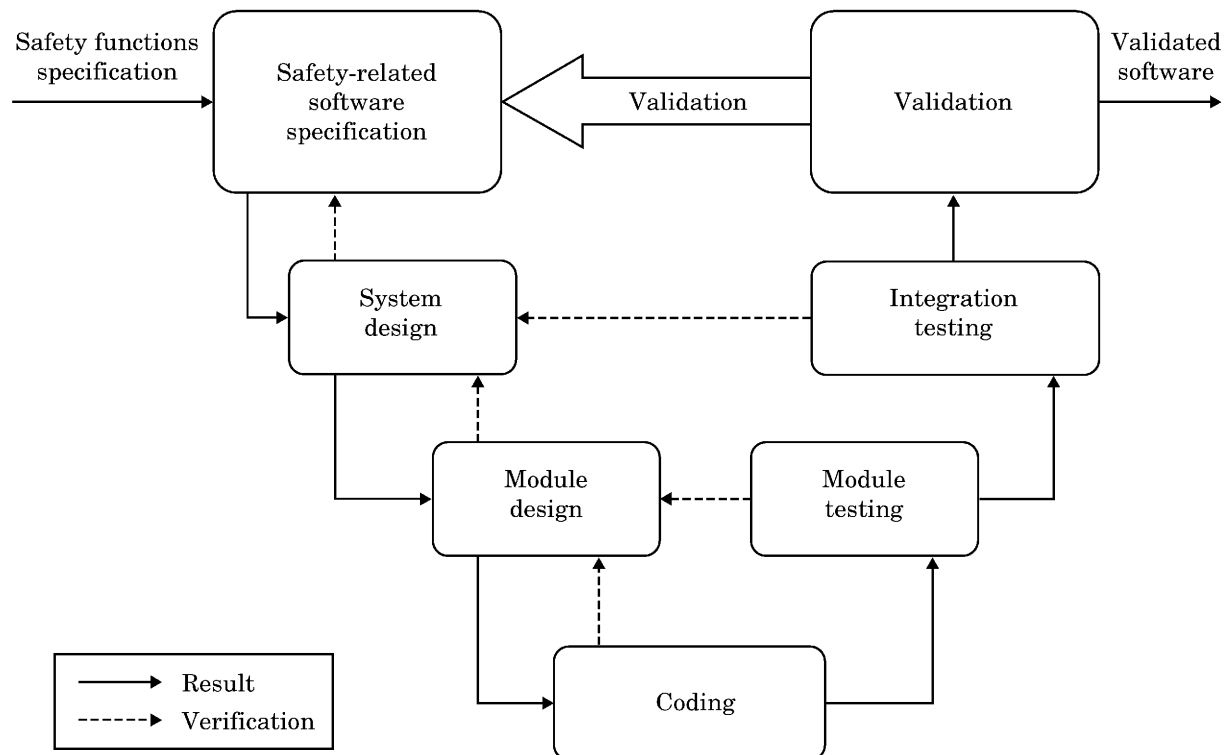
Table 7 Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

4.6 Software safety requirements

4.6.1 General

All lifecycle activities of safety-related embedded or application software shall primarily consider the avoidance of faults introduced during the software lifecycle (see figure 6). The main objective of the following requirements is to have readable, understandable, testable and maintainable software.



NOTE : Annex J gives more detailed recommendations for lifecycle activities.

Figure 6 Simplified V-model of software safety lifecycle

4.6.2 Safety-related embedded software (SRESW)

For SRESW for components with PL_r a to d, the following basic measures shall be applied:

- software safety lifecycle with verification and validation activities, see figure 6;
- documentation of specification and design;
- modular and structured design and coding;
- control of systematic failures (see **G.2**);
- where using software-based measures for control of random hardware failures, verification of correct implementation;
- functional testing, e.g. black box testing;
- appropriate software safety lifecycle activities after modifications.

For SRESW for components with PL_r c or d, the following additional measures shall be applied:

- project management and quality management system comparable to, e.g. **IEC 61508** series or **JIS Q 9001**;
- documentation of all relevant activities during software safety lifecycle;
- configuration management to identify all configuration items and documents related to a SRESW release;