OMRON

SAFETY,
TECHNOLOGY
& INNOVATION

SAFETY SOLUTION

ADVANCED GUIDE

First Edition

realizing

⚠ Warnings

Serious injury may possibly occur due to loss of required safety functions.
When building the system, observe the following warnings to ensure the integrity of the safety-related components.

●Setting Up a Risk Assessment System

The process of selecting these products should include the development and execution of a risk assessment system early in the design development stage to help identify potential dangers in your equipment and optimize safety product selection.

- Related International Standards:
  ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction

●Protective Measure

When developing a safety system for the equipment and devices that use safety products, make every effort to understand and conform to the entire series of international and industry standards available, such as the examples given below.

- Related International Standards:
  ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
  IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
  ISO 13849-1, -2 Safety-related Parts of Control Systems
  ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection
  IEC/TS 62046 Application of Protective Equipment to Detect the Presence of Persons

●Role of Safety Products

Safety products incorporate standardized safety functions and mechanisms, but the benefits of these functions and mechanisms are designed to attain their full potential only within properly designed safety-related systems. Make sure you fully understand all functions and mechanisms, and use that understanding to develop systems that will ensure optimal usage.

- Related International Standards:
  ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection
  ISO 13857 Safety Distances to Prevent Hazard Zones being Reached by Upper and Lower Limbs

●Installing Safety Products

Qualified engineers must develop your safety-related system and install safety products in devices and equipment. Prior to machine commissioning verify through testing that the safety products works as expected.

- Related International Standards:
  ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
  IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
  ISO 13849-1, -2 Safety-related Parts of Control Systems
  ISO 14119 Interlocking Devices Associated with Guards - Principles for Design and Selection

●Observing Laws and Regulations

Safety products must conform to pertinent laws, regulations, and standards. Make sure that they are installed and used in accordance with the laws, regulations, and standards of the country where the devices and equipment incorporating these products are distributed.

●Observing Usage Precautions

Carefully read the specifications and precautions as well as all items in the Instruction Manual for your safety product to learn appropriate usage procedures. Any deviation from instructions will lead to unexpected device or equipment failure not anticipated by the safety-related system.

●Transferring Devices and Equipment

When transferring devices and equipment, be sure to retain one copy of the Instruction Manual and supply another copy with the device or equipment so the person receiving it will have no problems with operation and maintenance.

- Related International Standards:
  ISO 12100 General Principles for Design - Risk Assessment and Risk Reduction
  IEC 60204-1 Electrical Equipment of Machines - Part 1: General Requirements
  ISO 13849-1, -2 Safety-related Parts of Control Systems
  IEC 62061 Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems
  IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

Terms and Conditions Agreement

Read and understand this catalog.

Please read and understand this catalog before purchasing the products. Please consult your OMRON representative if you have any questions or comments.

Warranties.

(a) Exclusive Warranty. Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

(b) Limitations. OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right. (c) Buyer Remedy. Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

See http://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc.

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Suitability of Use.

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer's application or use of the Product. At Buyer's request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer's application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY OR IN LARGE QUANTITIES WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products.

Omron Companies shall not be responsible for the user's programming of a programmable Product, or any consequence thereof.

Performance Data.

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications.

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions.

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Table of Contents

Chapter 1

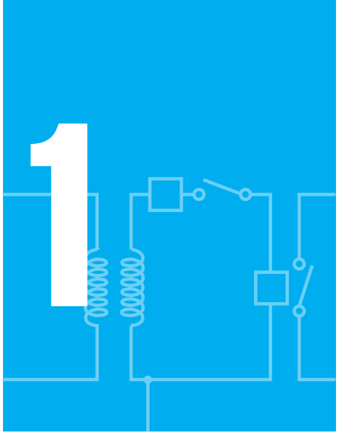
Performance Level 5
1. What Is a Performance Level (PL)? 6
2. Relationship between Risk Assessment and PL 7
3. Procedure for Evaluating the PL for SRP/CS 10
4. Parameters for PL Evaluation 15
5. Reliability Evaluation of Independent Subsystems 31
6. PL Determination 32
7. Basic Safety Functions for Risk Reduction in the Event of Failures 34
8. Concept of Fault Exclusion 41
9. Validation for Programmable Devices 43
10. Deployment of SRP/CS in Machines into a Block Diagram 44
11. Appendix 48

Chapter 2

Safety Circuit Examples & PLE Evaluation Cases 55
1. Introduction 56
2. Safety Circuit Examples & PL Evaluation Cases 58

Chapter 3

Regulations and Standards 71
1. Regulations and Standards by Country 72
2. Description of Safety Component-related Standards 86



Chapter 1

Performance Level

1. What Is a Performance Level (PL)?....6

Data used for PL evaluation....6

PL_r and PL....6

2. Relationship between Risk Assessment and PL....7

Risk assessment procedure and iterative risk reduction process....7

Organizing safety functions and hazards....8

Determining PL_r....9

3. Procedure for Evaluating the PL for SRP/CS....10

4. Parameters for PL Evaluation....15

(1) Safety category (category)....16

(2) $MTTF_D$ (Mean Time to Dangerous Failure)....20

(3) DC (Diagnostic Coverage) and DC_{avg}....24

(4) CCF (Common Cause Failure)....28

(5) PFH_D (Probability of Dangerous Failure per Hour)....30

5. Reliability Evaluation of Independent Subsystems....31

6. PL Determination....32

7. Basic Safety Functions for Risk Reduction in the Event of Failures....34

8. Concept of Fault Exclusion....41

9. Validation for Programmable Devices....43

Design processes for the software of SRP/CS....43

10. Deployment of SRP/CS in Machines into a Block Diagram....44

(1) Division according to safety function....44

(2) Deploying into a block diagram....45

11. Appendix....48

(1) PL evaluation procedure....48

(2) Relation between parameters, PFH_D, and PL in Table K.1 in Annex K of ISO 13849-1:2015....50

(3) Design processes for the software of SRP/CS....52

1. What Is a Performance Level (PL)?

If a risk reduction measure is based on control, the safety performance according to the magnitude of the risk is required for both hardware and software in the safety-related parts of control systems (SRP/CS). The level of this performance is defined as the performance level (PL) in the international standard, ISO 13849-1.
To conform to the EU Machinery Directive, individual safety functions satisfy the required PL and its validity must be confirmed.
ISO 13849-1 is harmonizing with national standards in various countries around the world. This ISO standard is recognized as providing a standard method to evaluate the safety functions of machine control. In Japan, JIS B 9705-1:2011, which contains the same regulations as those of ISO 13849-1:2006, has been published as an identical standard.

Data used for PL evaluation

The PL is evaluated from the structure of the control circuit of the safety function and the reliability of the components.
The PL is evaluated by the designers in machine manufacturers. The PL of the safety function is evaluated by calculating it by applying reliability data specific to the control devices to the structural elements (safety category and CCF) usage conditions (n_{op} and DC_{avg}) of the SRP/CS, which can be known only to the designers. Reliability data for control devices required for such PL evaluation is provided by control device manufacturers in many cases.

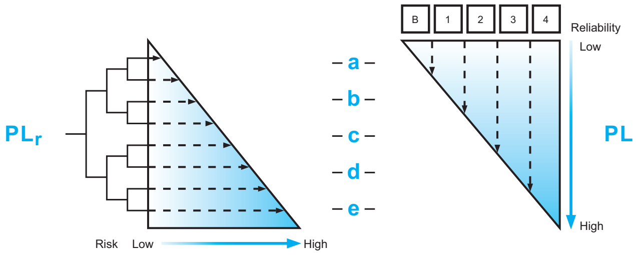
PL evaluation mainly uses data related to the following parameters. For details of these parameters, see "4. Parameters for PL Evaluation".

- Categories
- $MTTF_D$
- DC_{avg}
- CCF
- PFH_D

PL_r and PL

There are two types of PL, the performance required in the SRP/CS according to the magnitude of the risk (PL_r) and the performance resulting from actually evaluating the validity of the SRP/CS (PL). Both are evaluated on a scale of five from "a" to "e".

- Performance level required in the SRP/CS: PL_r (Required Performance Level)
- Performance resulting from evaluating the validity of the SRP/CS: PL (Performance Level)



The performance resulting from evaluating the validity of the SRP/CS (PL) is required to be always equal to or greater than the required performance level (PL_r).

2. Relationship between Risk Assessment and PL

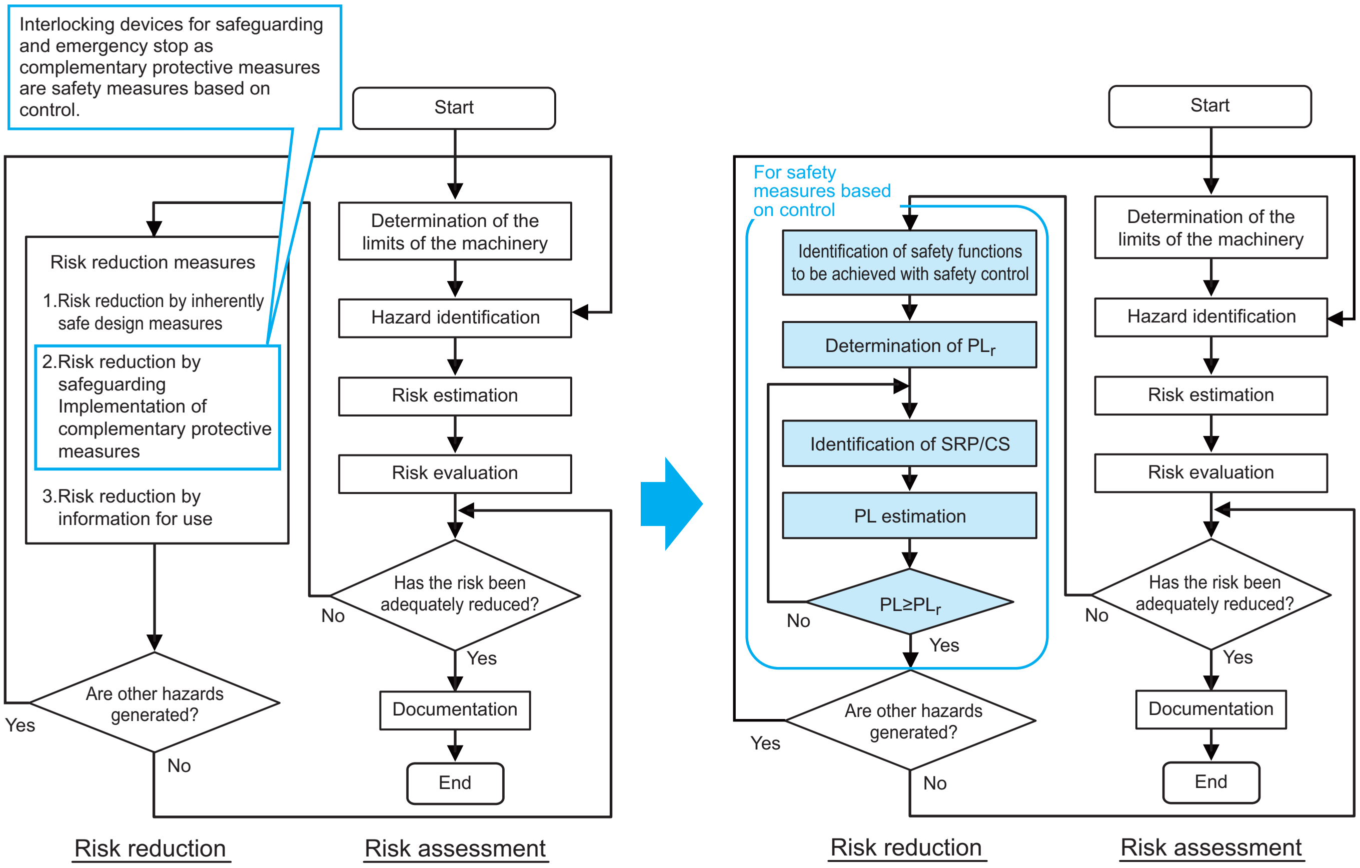
Risk assessment procedure and iterative risk reduction process

This section describes the relationship between risk reduction measures and PL of the SRP/CS.
The machine risk reduction procedure in ISO 12100:2010 follows a series of flows for risk reduction subsequent to risk analysis.
As described in Chapter 2 of Basic Guide, risk reduction measures contain the following three steps.

1. Inherently safe design measures
2. Safeguarding and complementary protective measures
3. Information for use

Of the steps above, interlocking devices such as safety switches and safety light curtains, as well as safety devices such as emergency stop devices, are often used for safeguarding and complementary protective measures. These devices rarely work individually. Usually, SRP/CS is composed of logic (control) devices that accept input signals from these devices and output devices to which their results are transmitted.

In such a case, risk reduction measures are subject to PL evaluation only if they are based on control. ISO 13849-1 embodies a design process of control-based risk reduction as shown in the diagram below for conformity to ISO 12100.


Interlocking devices for safeguarding and emergency stop as complementary protective measures are safety measures based on control.
Start
Determination of the limits of the machinery
Hazard identification
Risk estimation
Risk evaluation
Has the risk been adequately reduced?
No
Yes
Documentation
End
Risk reduction measures
1.Risk reduction by inherently safe design measures
2.Risk reduction by safeguarding Implementation of complementary protective measures
3.Risk reduction by information for use
Are other hazards generated?
Yes
No
Risk reduction
Risk assessment
For safety measures based on control
Identification of safety functions to be achieved with safety control
Determination of PLr
Identification of SRP/CS
PL estimation
PL≥PLr
No
Yes
Start
Determination of the limits of the machinery
Hazard identification
Risk estimation
Risk evaluation
Has the risk been adequately reduced?
No
Yes
Documentation
End
Are other hazards generated?
Yes
No
Risk reduction
Risk assessment

Performance Level

Risk reduction measures subject to PL evaluation

A risk reduction measure, if not relevant with the control system, is not subject to PL evaluation. Safety measures not based on control, for example, mechanical protection structures such as fixed safety fences or operational methods such as lockout/tagout, are not subject to PL evaluation. For this reason, start PL evaluation by reviewing the machine risk assessment sheet to extract only the items subject to PL evaluation among the risk reduction measures.

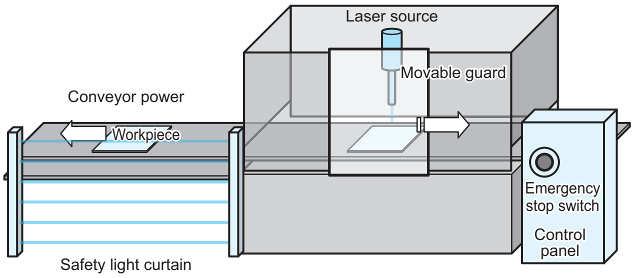
NO	Device name	Hazard	Hazardous event	Risk	Acceptance	Risk reduction measures	Subject to PL evaluation
1	Press machine	Crushing	During press work, another operator puts a hand in from the side to take out a workpiece, resulting in the hand being pinched.	High	×	Provide protection with a photoelectronic safety device.	✓
2	Control panel	Contact with a live part	During parts replacement, an operator comes in contact with a live part by mistake and gets an electric shock.	Medium	×	Install a main disconnecting device on the control panel.	
3	Conveyor	Drawing-in, trapping	An operator has his or her work wear entangled in the conveyor, dragged into it and scraping his or her whole body.	Medium	×	Mount emergency stop switches at certain intervals.	✓
4	Cables	Tripping	Cables are exposed on the floor, and an operator trips over them and falls down.	Medium	×	Lay floor cable covers.	
5	Workpiece table	Unnatural posture	Because of the low height of the workpiece table, an operator hurts his or her lower back due to longtime work.	Medium	×	Adjust the table height.	

Organizing safety functions and hazards

In general, multiple risk reduction measures are cited in a risk assessment. Of such measures, the performance level is required in risk reduction measures based on control, i.e., safety functions.

The following describes the concept whereby from multiple safety functional chains in a single machine, the PL for each of the safety functions can be organized.

The following machine is assumed as an example. There are two hazards: laser source (danger of blindness) and conveyor power (entanglement).



Assume that the following risk reduction measures are taken against these hazards:

- Shut off the laser source if the emergency stop switch is pressed
- Shut off the conveyor power as well if the emergency stop switch is pressed
- Shut off only the laser source if the movable guard is opened
- Shut off the conveyor power if the safety light curtain is blocked

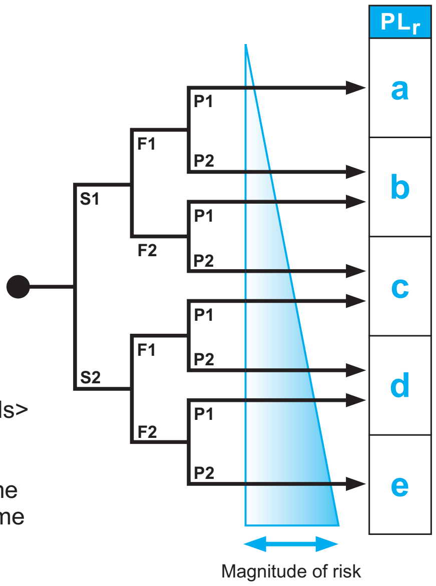
The safety functional chain in this machine can be organized as in the table below.

Safety function		Hazard	
		Laser source	Conveyor power
Risk reduction measure	Emergency stop switch	Safety functional chain 1	Safety functional chain 2
	Movable guard	Safety functional chain 3	-
	Safety light curtain	-	Safety functional chain 4

If a single risk reduction measure serves as a measure against multiple hazards, it is organized as a separate safety functional chain.
PL evaluation is performed on each safety functional chain. This means that a machine having multiple hazards and multiple risk reduction measures has more than one PL. Even if the safety functions are complex in an actual machine, it is recommended to organize the relationships between risk reduction measures and hazards before starting PL evaluation.

Determining PL_r

The required performance level for SRP/CS: PL_r can be judged with a risk assessment. PL_r derived from the results of a risk assessment is the target performance for the design of the SRP/CS.
PL_r is evaluated with the risk graph method from the severity of injury (S), frequency and/or exposure to the hazard (F), and possibility of avoiding the hazard (P). The results are divided into indexes "a" to "e" according to the magnitude of the risk.

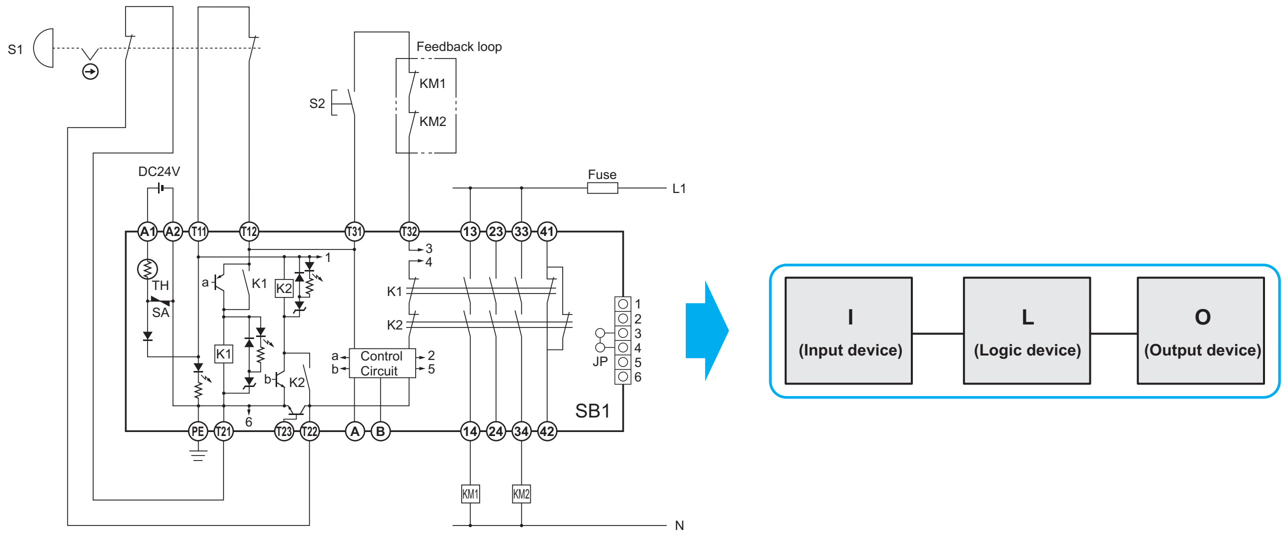


<Meaning of Symbols>
S1: Slight injury
S2: Serious injury
F1: Seldom/short time
F2: Frequent/long time
P1: Avoidable
P2: Unavoidable

3. Procedure for Evaluating the PL for SRP/CS

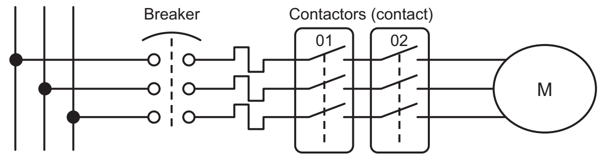
This section describes the PL evaluation procedure to follow after the SRP/CS that achieve individual safety functional chain are designed.

Demands for safety function operation are performed via different transmission paths for different chains. For example, a certain safety function informs the controller that an event of the guard opening occurs and shuts off the hazardous energy. Another safety function informs the controller that the emergency stop switch is pressed and shuts off the hazardous energy. As stated above, even if there are common blocks such as energy shutoff by the controller, the transmission paths differ.
Each transmission path is represented in a block diagram comprised of a detection function I (input device), a judging function L (logic device), a power control function O (output device), and the connection means for each.
Creating a block diagram using patterns as shown below, from the control circuit diagram to identify the chain with which safety functions are transmitted may facilitate PL evaluation.

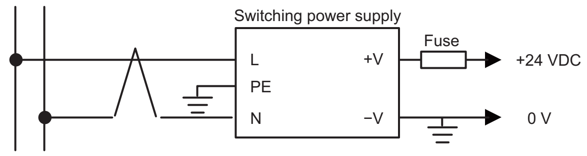


Suppose a control circuit diagram of a safety function that shuts off hazards in stop category 0 with an emergency stop switch. Shown below is a schematic diagram of the control parts related to safety functions that are extracted from the control circuit.

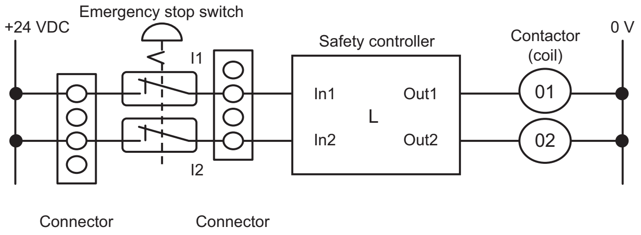
3-phase power supply (200 VAC system)



Single-phase power supply (100 VAC system)



Control power supply (24 VDC system)

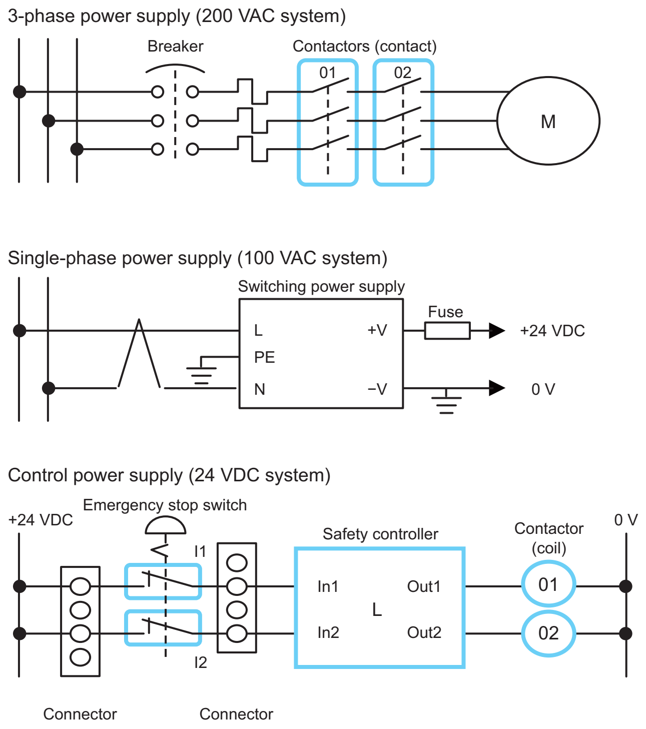


1) Extracting safety-related parts

Representing SRP/CS in a block diagram is started by isolating the parts related to the achievement of the safety function in the control circuit diagram from the parts not related to it. Parts not involved in the safety function or parts whose failures do not cause the loss of the safety function need not be incorporated into PL evaluation even if they are on transmission paths.

Examples:

- Overcurrent protective device, transformer, etc.
  These parts may affect systematic failures and CCFs. You must verify safety by ensuring that each device conforms to IEC 60204-1 or individual product standards. These parts are not, however, represented in a block diagram.
- Cable, connector, signal splitter/divider, etc.
  The need to consider the possibility of the fault of these parts in the evaluation of the safety control circuit is judged on whether the concept "fault exclusion", stipulated in Annex D of ISO 13849-2:2012, can be applied or not. If a fault meets the stipulated exclusion conditions, the fault can be regarded as not affecting the safety of the circuit, so that you need not incorporate it into the final safety category judgment, PL evaluation, etc.


3-phase power supply (200 VAC system)

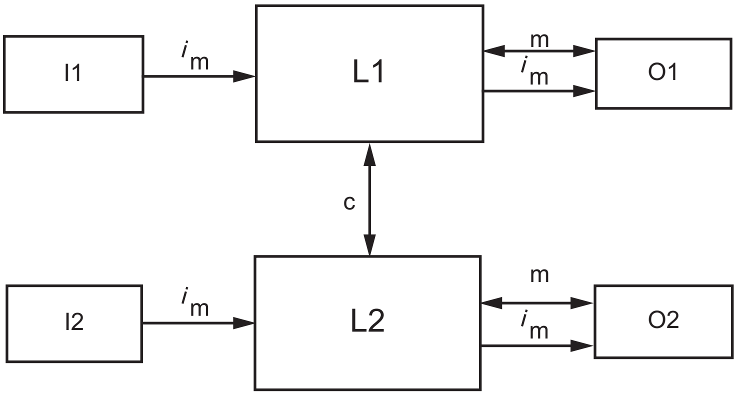
Single-phase power supply (100 VAC system)

Control power supply (24 VDC system)

2) Assigning to a block diagram and judging the safety category

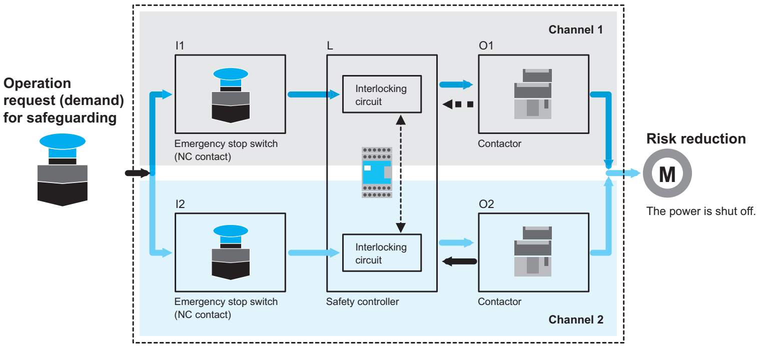
Represent the extracted safety-related parts in an I, L, and O block diagram. It is important to note here how many paths are available to transmit each safety function. Such a path is called a channel. The safety category is judged with the number of channels.
The number of channels on which to judge the safety category is indicated on a structural drawing called a designated architecture.

Designated architecture for category 4



I1, I2:	Input device (e.g. sensor)
L1, L2:	Logic
O1, O2:	Output device (e.g. main contactor)
^{i}m:	Interconnecting means
c:	Cross monitoring
m:	Monitoring

Actually assign the safety-related parts extracted in 1) in the order of I, L, and O, following the block diagram in the designated architecture, to judge the safety category.
In this example, the emergency stop switches (two contacts inside) of I and contactors of O are connected as two channels, respectively.
Because the safety controller of L is duplexed internally, this block diagram can be judged to be in safety category 3 or safety category 4.

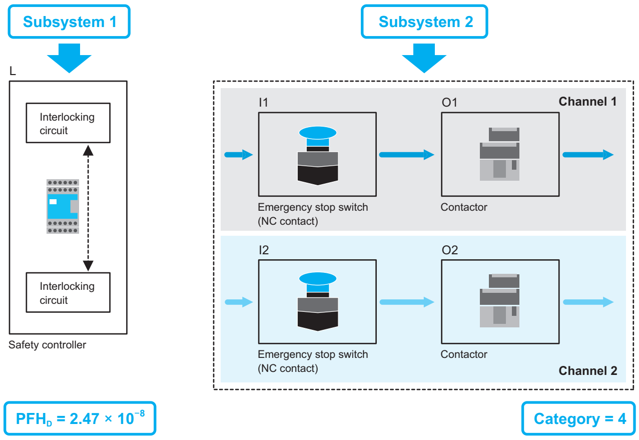


Note that for the final judgment of the safety category, you must make sure that several other requirements are satisfied in addition to the designated architecture indicated in this block diagram. For details, see "4. Parameters for PL Evaluation, (1) Safety category (category)".

3) Dividing into subsystems

Dividing the SRP/CS assigned to a block diagram into functional chunks called subsystems may facilitate PL evaluation. PL evaluation using the concept of subsystems is presented in, for example, ISO/TR 23849, which is an application guide of ISO 13849-1. This is a method for calculating the PL for the SRP/CS by adding together the values of PFH_D evaluated for the individual subsystems.

To divide a block diagram into subsystems, you must check what reliability data the devices to use have. For example, in the safety controller in the diagram below, two channels are configured within the device to provide a failure diagnosis function, so that a PL evaluation value is given for the device. Such a safety device itself can be handled as a single independent subsystem.
Parts such as switches, relays, and contactors, on the other hand, do not themselves have PL evaluation values, and cannot be handled as independent subsystems. These parts are called discrete parts or blocks as parts composing a subsystem. A subsystem consisting of discrete parts (blocks) is represented as a block diagram focusing on channels as in 2) and is evaluated by being applied to the designated architecture.



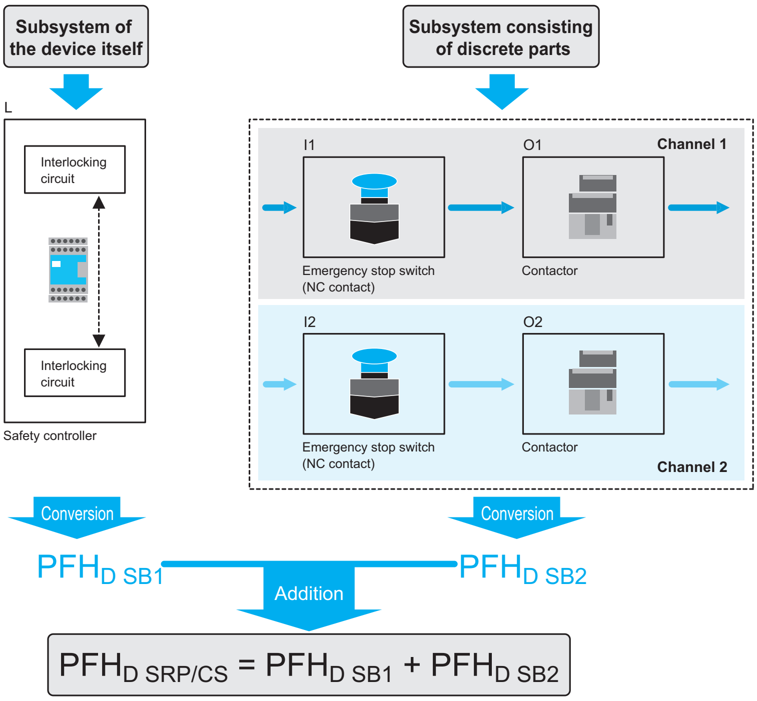
The evaluation of each subsystem uses three parameters, category, $MTTF_D$, and DC_{avg}, as well as the parameter PFH_D, which results from combining them. Reliability data for each of the parameters can be obtained from device manufacturers. For an independent subsystem, PL evaluation values are also provided along with these data.

Reference: Classification of OMRON Safety Components

Classification	Discrete part (block)	Independent subsystem
Features	• No PL is declared for the part itself. • No failure diagnosis function is provided (passive).	• A PL is declared for the device itself. • A failure diagnosis function for itself is provided (active).
Input device	Safety limit switch: D4N series Emergency stop pushbutton switch: A22E Safety-door switch: D4NS Guard lock safety-door switch: D4NL, D4SL-N etc.	Non-contact door switch: D40A, D40Z Safety laser scanner: OS32C Safety light curtain: F3SJ series Safety light curtain: F35G-R series etc.
Logic (Control) device	Relay with forcibly guided contacts: G7SA etc.	Safety relay unit: G9SA series Flexible safety unit: G9SX series Safety controller: G9SP Safety CPU, I/O unit: NX series etc.
Output device		AC servomotor/ servo driver: G5 series Multi-function compact inverter: MX2 series V1 type etc.

4) Linking subsystems and determining the PL

For each of the subsystems resulting from the division described in 3), calculate PFH_D based on the data supplied for each parameter. By linking the subsystems into one for which PFH_D values are calculated, you can derive the evaluation of the SRP/CS.
For details of the determination of the PL for the SRP/CS, see "6. PL Determination".


Subsystem of the device itself
Subsystem consisting of discrete parts
L
Interlocking circuit
Interlocking circuit
Safety controller
I1
O1
Channel 1
Emergency stop switch (NC contact)
Contactor
I2
O2
Emergency stop switch (NC contact)
Contactor
Channel 2
Conversion
Conversion
PFHD SB1
PFHD SB2
Addition
PFHD SRP/CS = PFHD SB1 + PFHD SB2

SRP/CS

4. Parameters for PL Evaluation

As stated in "3. Procedure for Evaluating the PL for SRP/CS", the following method is used for the evaluation of the PL for SRP/CS: The SRP/CS are divided into several subsystems according to the characteristics of the parts and the PL for each subsystem is evaluated, thereby calculating the final PL for the SRP/CS.

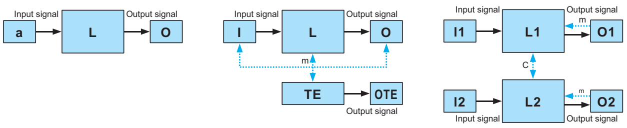
For a discrete part (block), its value as a subsystem can be derived by combining and evaluating data for several related parameters. A discrete part is mainly a part that can cause wear-out failures (such as a switch, relay, and contactor) or a sensor that does not have a failure diagnosis function. Reliability of a subsystem consisting of these discrete parts is evaluated by using the following parameters.

Parameter for PL evaluation

Criteria for determination

Safety category

Architecture of the SRP/CS (configuration of I, L, and O)



B
1
2
3
4
5 categories

$MTTF_D$

B_{10D}

n_{op}*

* The machine designer him or herself need be aware of n_{op}.

① **Part unit**

1. **Use $MTTF_D$ provided by the manufacturer**
2. **Use $MTTF_D$ or B_{10D} specified in Annex C**
3. **10 years if no data is available**

If B_{10D} is provided, use the right-hand side formula to convert it into $MTTF_D$.

$$MTTF_D = \frac{B10d}{0.1 \times n_{op}}$$

② **Channel**

$$MTTF_D = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTF_D i}}$$

③ **Entire subsystem**

If the $MTTF_D$ values of channels 1 and 2 are equal, assume the result of formula ② as the $MTTF_D$ value for the subsystem. Although upper limit on the $MTTF_D$ value for a subsystem is 100 years, the upper limit is 2500 years for a category 4 subsystem.

$$MTTF_D = \frac{2}{3}\left[MTTF_D c1 + MTTF_D c2 - \frac{1}{\frac{1}{MTTF_D c1} + \frac{1}{MTTF_D c2}}\right]$$

High
(30 years or more and 100 years or less*)
* For category 4, 2500 years or less

Medium
(10 or more years and less than 30 years)

Low
(3 or more years and less than 10 years)

3 levels

DC_{avg}

DC

$MTTF_D$

① **Part unit**

Select the relevant DC from Table 1 in Annex E.

② **Entire subsystem**

$$DC_{avg} = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTF_D i}}{\sum_{i=1}^{n} \frac{1}{MTTF_D i}}$$

High
(99% or more)

Medium
(90% or more and less than 99%)

Low
(60% or more and less than 90%)

None
(less than 60%)

4 levels

CCF

The score in the check list in Annex F must be 65 or over.

Yes (65 or more)

No (less than 65)

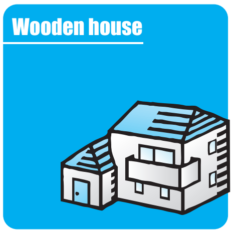
2 levels

(1) Safety category (category)

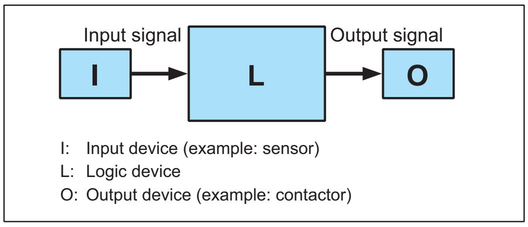
Concept of safety category (category)

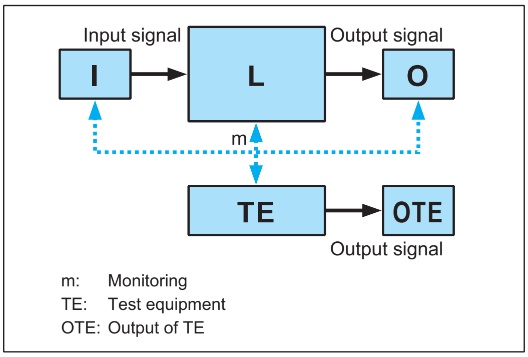
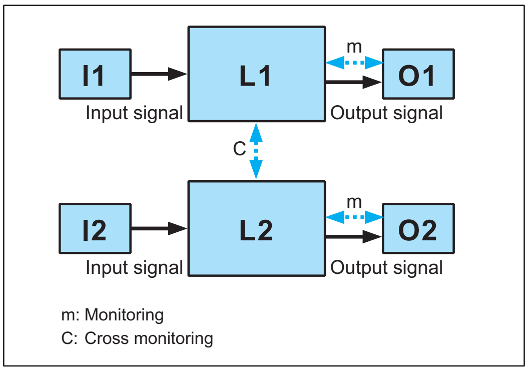
Safety category is a concept representing the structure (architecture) of SRP/CS.
SRP/CS may have different appropriate structures (architectures) depending on the purpose of the machine, the degree of hazards, the scale of the machine, the frequency of usage, and other factors even though they have the common purpose of ensuring the safety of the machine.
Take a "space for preventing rain and wind" as an analogy. There are different types of buildings according to purpose, such as tents, wooden houses, and office buildings, and there are different types of basic structures, such as foundations, skeletons, external walls, and roofs. Such a basic structural pattern in SRP/CS is called a designated architecture, and the structure (architecture) is a basic form for each safety category.
For each safety category, requirements for the dangerous failure probability for SRP/CS are established individually, in addition to such structural requirements.

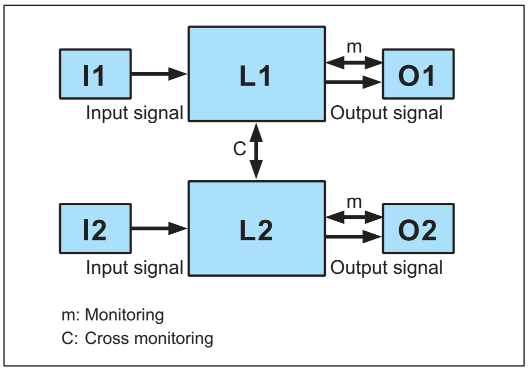
For example...



Safety category requirements

Safety category	Overview of requirements	Applicable designated architecture
B	What is required in SRP/CS in safety category B is that the target safety function can be achieved. This requires a design that tolerates the intended usage conditions listed below. • Expected stress related to device operation, such as the breaking capacity and the switching frequency of a contact • Impacts related to materials used, such as corrosion by chemical substances • Other factors such as mechanical vibration, electromagnetic noise, and interruption of or fluctuations in the control power supply circuit To satisfy these requirements, it is necessary to conform to the basic safety principles in addition to the selection of parts conforming to the standards suitable for the application first and then the implementation of measures against external impacts in accordance with the requirements of the standards. In safety category B, which is for a single channel system, the safety function is impaired with the occurrence of a failure. Safety category B has no failure detection function, so its diagnostic coverage (DC_{avg}) is 0%. Common cause failures (CCFs) need not be considered. $MTTF_D$ is from "Low" to "Medium". The maximum PL achievable in safety category B is b. **Note: For details of the basic safety principles, see ISO 13849-2:2012.**	 Input signal Output signal I L O I: Input device (example: sensor) L: Logic device O: Output device (example: contactor) **Note: The block diagram above is a conceptual view of the safety channel flow. The number of blocks may differ from the one in an actual electrical circuit diagram. For example, in category B and in category 1, there are cases where only an input device (I) and an output device (O) are used without a logic device (L). On the contrary, there are cases where there are three or more blocks.**
1	What is required in SRP/CS in safety category 1 is that the safety function is achievable and, in addition, that its reliability is high. This requires that the following be applied to the structure of the SRP/CS, in addition to the requirements in category B. • Use of "well-tried" parts • Use of "well-tried" safety principles "Well-tried" parts are either of the following: a) Part widely used for similar applications in the past and having a good record b) Part suitable for the use for safety-related applications and whose reliability is verified Note that parts such as general PLCs consisting of complex electronic parts are not regarded as "well-tried" parts. In safety category 1, which is for a single channel system, as with safety category B, the safety function is impaired with the occurrence of a failure. It has no failure detection function, its diagnostic coverage (DC_{avg}) is 0%, and common cause failures (CCFs) need not be considered. $MTTF_D$ is "High", which is higher than in safety category B, so the possibility of the impairment of the safety function can be said lower than that in safety category B. The maximum PL achievable in safety category 1 is c. **Note: For details of well-tried parts and the safety principles, see ISO 13849-2:2012.**	

Safety category	Overview of requirements	Applicable designated architecture
2	What is required in SRP/CS in safety category 2 is that if a dangerous failure occurs, impairing the safety function, this can be compensated for with a supplementary checkup function. This requires that they be designed and assembled using the "well-tried" safety principles, in addition to the requirements in safety category B, and that the checkup function possessed by the machine control system perform a checkup on the safety function at appropriate intervals. The checkup function consists of test equipment (TE) and its output device (OTE). The following are required of the checkup on the safety function. • The checkup must be performed at the following times: - At the time of starting up the machine - Before the occurrence of a hazardous situation (for example, before the start of a new cycle and periodically during operation, if required) • Results of the checkup - Operation must be approved if no failure is detected. - If a failure is detected, an appropriate control output must be issued that causes the machine to work on the safety side. If this is impossible (due to, for example, a dangerous failure due to a welded contactor), an alarm must be issued. This state must be retained until the failure is removed. • No hazardous situation (such as an increase in the response time of the safety function) may be caused by the check itself. In safety category 2, which is treated as being for a redundant system because it has an I-L-O control function, as well as a checkup function, the safety function may be impaired with a failure between checkups. Because periodic failure detection is performed with the checkup function, the diagnostic coverage (DC_{avg}) is "Low" or "Medium" (60% or higher and less than 99%). Common cause failures (CCFs) must be taken into account. $MTTF_D$ related to the I-L-O safety functional chain is one of "Low" to "High" depending on PL_r. In any case, the design must be such that $MTTF_D$ of the checkup function (TE) is at least half $MTTF_D$ of I-L-O. The maximum PL achievable in safety category 2 is d. **Note: For information about the appropriate checkup frequency in safety category 2 and the measures to take if the frequency cannot be achieved, see ISO 13849-1:2015.**	 Input signal Output signal I L O m TE OTE Output signal m: Monitoring TE: Test equipment OTE: Output of TE
3	What is required in SRP/CS in safety category 3 is that even if a failure occurs in a portion of the safety function, the safety function is not impaired as a whole. This requires that they be designed and assembled using the "well-tried" safety principles, in addition to the requirements in safety category B, and that the safety function include a failure detection means and, if reasonably implementable, a failure be detected upon the next request for safety function operation or earlier. Safety category 3 has a redundant structure with two channels and ensures the safety by performing cross monitoring between the channels. The safety function is not impaired with a single failure, but it may be impaired with accumulated undetectable failures. Because of this, the diagnostic coverage (DC_{avg}) is "Low" or "Medium" (60% or higher and less than 99%). Common cause failures (CCFs) must also be taken into account. $MTTF_D$ is one of "Low" to "High" according to PL_r. The maximum PL achievable in safety category 3 is e.	 I1 L1 m O1 Input signal Output signal C I2 L2 m O2 Input signal Output signal m: Monitoring C: Cross monitoring

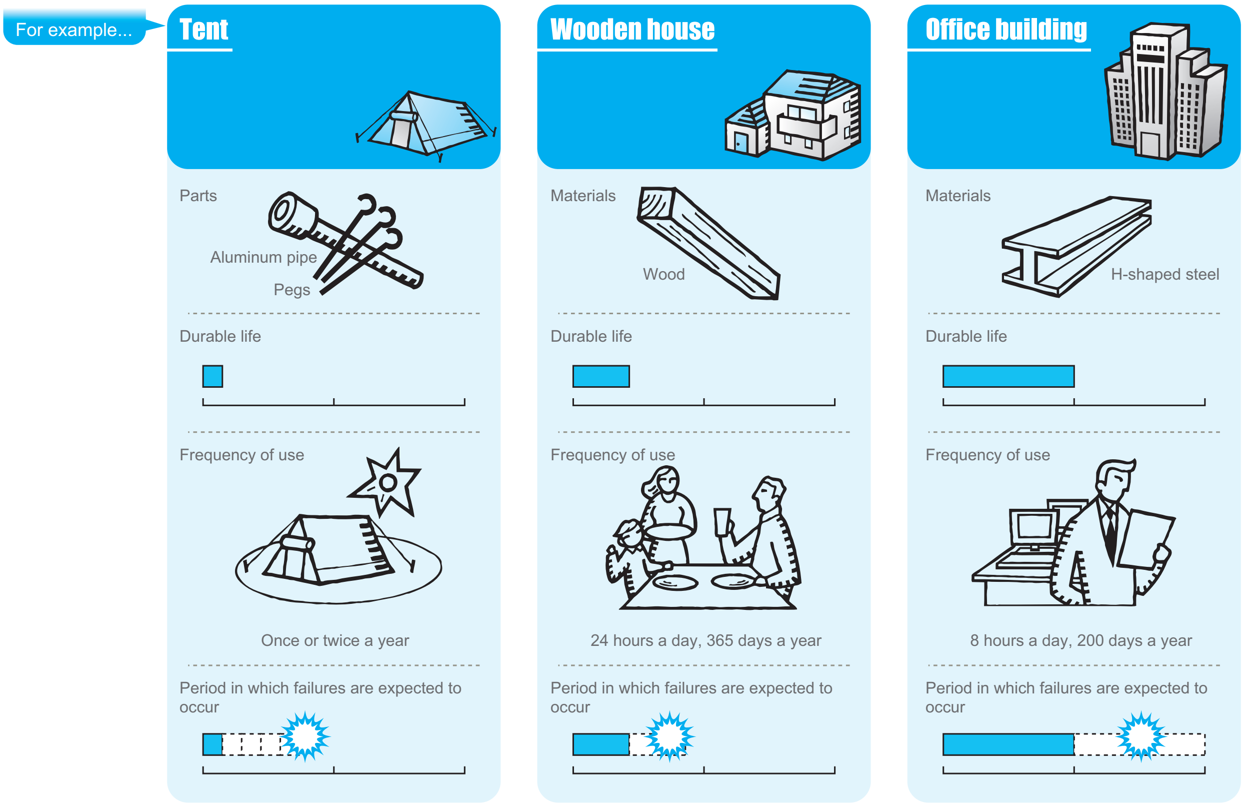
Safety category	Overview of requirements	Applicable designated architecture
4	What is required in SRP/CS in safety category 4 is that the safety function is not impaired even with a certain level of accumulation of failures in the safety function. This requires that they be designed and assembled using the "well-tried" safety principles, in addition to the requirements in safety category B, and that the safety function include a failure detection means and a failure be detected upon the next request for safety function operation or earlier. As with safety category 3, safety category 4 has a redundant structure with two channels and ensures the safety by performing cross monitoring between the channels. The failure detection capability is higher than that of safety category 3, and the possibility of the impairment of the safety function due to an accumulation of failures in addition to a single failure can be said extremely low. Because of this, the diagnostic coverage (DC_{avg}) is "High" (99% or higher). Common cause failures (CCFs) must also be taken into account. $MTTF_D$ must be "High". The maximum PL achievable in safety category 4 is e.	 I1 L1 O1 m Input signal Output signal C I2 L2 O2 m Input signal Output signal m: Monitoring C: Cross monitoring **Note: It has the same basic structure as safety category 3, but its DC_{avg} and $MTTF_D$ must be "High". The continuous line indicating monitoring in the designated architecture diagram represents a diagnostic coverage higher than that of safety category 3.**

* Complex structures not applicable to these diagrams, for example, a structure having inputs of three or more channels and based on majority decision logic, cannot be handled with ISO 13849-1. Such structures must be evaluated with other standards such as IEC 62061.

(2) MTTF_D (Mean Time to Dangerous Failure)

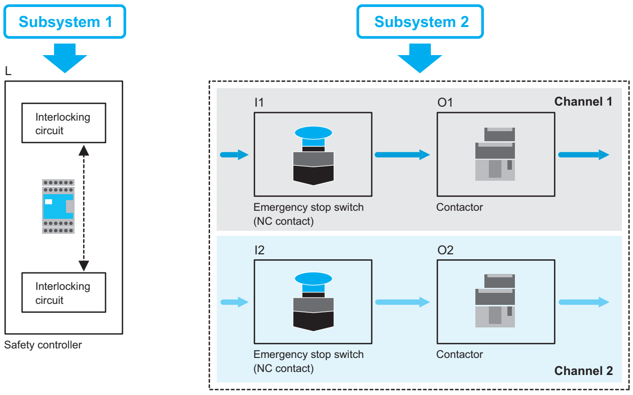
Concept of MTTF_D

MTTF_D refers to a mean time that an SRP/CS takes until it causes a dangerous failure.
Tents, wooden houses, and office buildings serve the same function of preventing rain and wind. Each building has its own life expectancy, after which its functions will no longer effective. The life expectancy varies depending on the type. Each of the parts comprised in the building (for example, tent supports, beams of a wooden house, and steel frames of a building) has its own inherent failure rate due to its materials. Even if the predetermined replacement period is observed, the time after which rain and wind can no longer be prevented varies depending on the frequency of its use.
The same is true with the control devices in SRP/CS. Even if they continue to be used by being replaced at certain intervals, the safety may not be ensured due to a random failure, etc., leading to a so-called dangerous failure situation. MTTF_D represents an estimated time after which such a dangerous failure occurs. It should be noted that it is not the same as the durable life of the part.



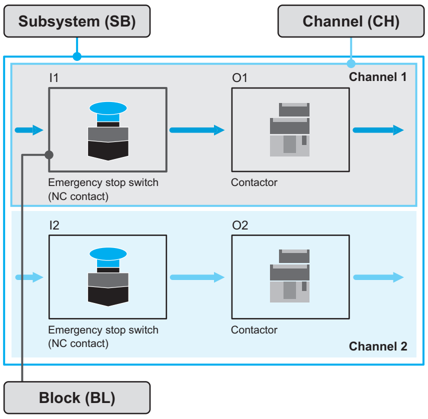
Layers of MTTF_D

A block diagram contains boxes representing the parts composing each subsystem. Because MTTF_D is to be given to each and every one of these boxes, you need to calculate MTTF_D for the entire subsystems based on each MTTF_D value in order to finally evaluate the SRP/CS.
For subsystem 2 shown below, two discrete parts (blocks) or boxes are on the same channel. In this case, MTTF_D for the channel is the average of MTTF_D values of the two parts. The same applies to a case with three or more boxes on the same channel; MTTF_D for the channel can be derived by taking the average of their values. For category 3 or 4, in which a subsystem contains two channels, the same applies to MTTF_D for the subsystem; the value can be obtained by taking the average of the two channels.



MTTF$_D$ of a discrete part (block)

To each and every one of the boxes on the block diagram into which the SRP/CS are deployed, allocate MTTF$_D$ data. Here, consider a subsystem consisting of discrete parts (blocks).



MTTF$_D$ of a discrete part (block) can be obtained with one of the following methods:

1. Obtain data for the devices used from the part manufacturers.
2. Calculate data from Annexes C and D of ISO 13849-1:2015.
3. Assume that MTTF$_D$ is 10 years.

For some parts, you can obtain MTTF$_D$ values themselves from the data supplied. For others, you may need to calculate MTTF$_D$ values with calculating formulas. Parts such as switches and relays function and wear out only when operation requests are made. Thus, the number of operations is related to the time to a dangerous failure. For such parts, data called B$_{10D}$ is provided, which indicates the number of operations after which 10% of the parts cause a dangerous failure. MTTF$_D$ can be calculated based on the value and the number of operations.

The calculating formula for calculating MTTF$_D$ from B$_{10D}$ is:

$$\mathrm{MTTF_D} = \frac{B_{10\mathrm{D}}}{0.1 \times n_{\mathrm{op}}} \quad \text{(Formula 1)}$$

B$_{10D}$: Number of operations after which 10% of the parts cause a dangerous failure (unit: number of times)
n$_{op}$: Total number of operations per year for the target application (units: cycles/year)

In (Formula 1), the parameter n$_{op}$ is used to indicate the number of times the part is operated per year. Calculating this parameter requires that you know how frequent the target safety function is operated.
n$_{op}$ can be calculated with the following formula:

$$n_{\mathrm{op}} = \frac{d_{\mathrm{op}} \times h_{\mathrm{op}} \times 3600}{t_{\mathrm{cycle}}} \quad \text{(Formula 2)}$$

t$_{cycle}$: Average time interval per operation cycle (units: seconds/cycle)
h$_{op}$: Operation time per day (units: hours/day)
d$_{op}$: Operation days per year (units: days/year)

Typical MTTF_D and B_{10D} values for parts in Annex C of ISO 13849-1:2015 and relevant standards

(Excerpt from Table C.1 in Annex C of ISO 13849-1:2015)

	Basic and "well-tried" safety principles in ISO 13849-2:2012	Relevant standard See Note 1.	Typical values MTTF_D (years) B_{10D} (cycles)
Mechanical components	Tables A.1 and A.2	–	MTTF_D = 150
Hydraulic components ($n_{op} \geq$ 1,000,000)	Tables C.1 and C.2	ISO 4413	MTTF_D = 150
Hydraulic components (1,000,000 > $n_{op} \geq$ 500,000)	Tables C.1 and C.2	ISO 4413	MTTF_D = 300
Hydraulic components (500,000 > $n_{op} \geq$ 250,000)	Tables C.1 and C.2	ISO 4413	MTTF_D = 600
Hydraulic components (250,000 > n_{op})	Tables C.1 and C.2	ISO 4413	MTTF_D = 1,200
Pneumatic components	Tables B.1 and B.2	ISO 4414	B_{10D} = 20,000,000
Relays and contactor relays with small load	Tables D.1 and D.2	EN 50205 IEC 61810 all parts IEC 60947 all parts	B_{10D} = 20,000,000
Relays and contactor relays with nominal load	Tables D.1 and D.2	EN 50205 IEC 61810 all parts IEC 60947 all parts	B_{10D} = 400,000
Proximity switches with small load	Tables D.1 and D.2	IEC 60947 all parts ISO 14119	B_{10D} = 20,000,000
Proximity switches with nominal load	Tables D.1 and D.2	IEC 60947 all parts ISO 14119	B_{10D} = 400,000
Contactors with small load	Tables D.1 and D.2	IEC 60947 all parts	B_{10D} = 20,000,000 See Note 2.
Contactors with nominal load	Tables D.1 and D.2	IEC 60947 all parts	B_{10D} = 1,300,000 See Note 2.
Position switches*	Tables D.1 and D.2	IEC 60947 all parts ISO 14119	B_{10D} = 20,000,000
Position switches (with separate actuator or guard locking)*	Tables D.1 and D.2	IEC 60947 all parts ISO 14119	B_{10D} = 2,000,000
Emergency stop devices* See Note 3.	Tables D.1 and D.2	IEC 60947 all parts ISO 13850	B_{10D} = 100,000
Push buttons (for example, enabling switches)* See Note 3.	Tables D.1 and D.2	IEC 60947 all parts	B_{10D} = 100,000

For information about the definition and use of B_{10D}, see ISO 13849-1:2015 C.4.

Note:1. B_{10D} is estimated to be twice B_{10} (dangerous failure rate of 50%) if no other information (such as product standards) is available.

Note:2. For "nominal load" or "small load", the safety principles described in ISO 13849-2, such as multiplying the rated current value by the safety factor, must be taken into account. "Small load" means 20% of the rating, for example.

Note:3. Emergency stop devices based on IEC 60947-5-5 and ISO 13850 and enabling switches based on IEC 60947-5-8 can be regarded as a category 1 or category 3/4 subsystem according to the number of output contacts and on failure detection in the SRP/CS connected to them. Each contact element (including a mechanical actuator) can be regarded as a single channel with a B_{10D} value. For enabling switches conforming to IEC 60947-5-8, it is estimated that the contact is opened when the switch is pushed in or released. In some cases, the machine manufacturer can apply fault exclusion based on Table D.8 in ISO 13849-2 after considering the environmental factors for specific applications and devices.

* If fault exclusion with a direct opening action is possible.

$MTTF_D$ of channels

Upon completion of the assignment of $MTTF_D$ to all blocks, calculate $MTTF_D$ for each channel based on the assignment. The harmonic means is taken by applying the $MTTF_D$ values in all blocks on the same channel to the following formula.

$$MTTF_D = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTF_D i}}$$

(Formula 3)

Category 3 and category 4 have two channels each, and calculation is required for each of the channels.

$MTTF_D$ of subsystems

To calculate $MTTF_D$ for a subsystem, you need to average two channels.
If the $MTTF_D$ value is the same for channels 1 and 2, the result of calculation with (Formula 3) can be used as $MTTF_D$ directly for the subsystem.
If the $MTTF_D$ values for channels 1 and 2 differ, use the following formula to average the subsystem levels.

$$MTTF_D\mathrm{SB} = \frac{2}{3}\left[MTTF_D\mathrm{CH1} + MTTF_D\mathrm{CH2} - \frac{1}{\frac{1}{MTTF_D\mathrm{CH1}} + \frac{1}{MTTF_D\mathrm{CH2}}} \right]$$

(Formula 4)

<Reference> Mission time and T_{10D}
A part has an inherent failure probability. For a mechanical part, the probability starts to increase rapidly at a certain time due to fatigue or aging. The same is true with the dangerous failure occurrence probability. The characteristics during a period of such rapid changes cannot be used for the evaluation of $MTTF_D$. In PL evaluation, the dangerous failure occurrence probability is considered to be constant on the assumption that the part is replaced with an identical one after the usage period intended for design-related reasons in order to calculate $MTTF_D$ of the part. The intended usage period is called mission time.
The machine designer must bear the following in mind about mission time.

① The machine designer must define the mission time of the machine control system or the entire machine (intended number of operation years of the machine).
② If T_{10D} for each part used in the control system is shorter than the mission time of the machine, notify the user in writing that the part must be replaced at the interval of T_{10D}.

T_{10D} is the time required for 10% of the samples to cause a dangerous failure, and can be calculated with the following formula.

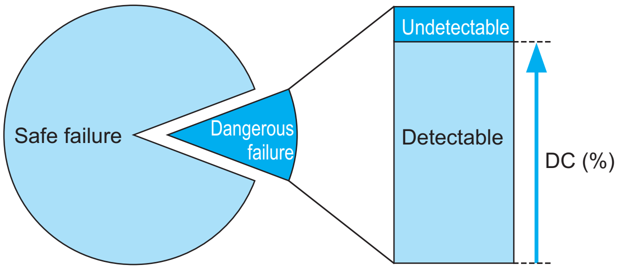
$$T_{\mathrm{10D}} = \frac{B_{\mathrm{10D}}}{n_{\mathrm{op}}}$$

(Formula 5)

(3) DC (Diagnostic Coverage) and DC_{avg}

Concept of DC

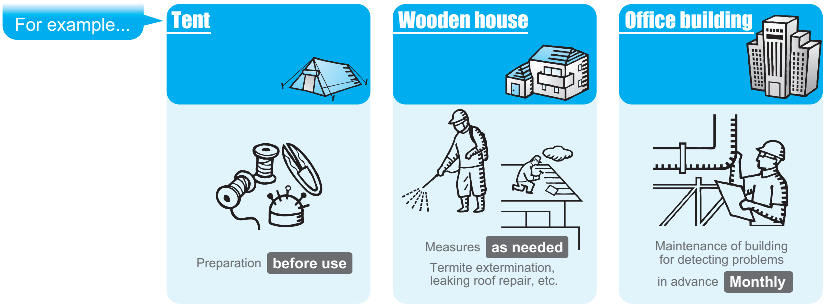
DC stands for "diagnostic coverage", which is a parameter representing the validity of detecting a dangerous failure of SRP/CS. DC_{avg} is an average value of DCs through entire SRP/CS or subsystems.
There are two types of SRP/CS failure: safe failure and dangerous failure. For a safe failure, the SRP/CS fulfill their functions. As long as the usage is appropriate when a safe failure occurs, this is not a problem. For a dangerous failure, what is important is to determine whether there is a function to detect it (diagnosis function) and "whether effective measures can be taken" for the dangerous failure or "not". DC is a parameter indicating the feasibility (%) of detecting such a dangerous failure and taking effective measures.



Are SRP/CS failures safe or dangerous?

Are dangerous failures detectable (effective measures can be taken) or undetectable?

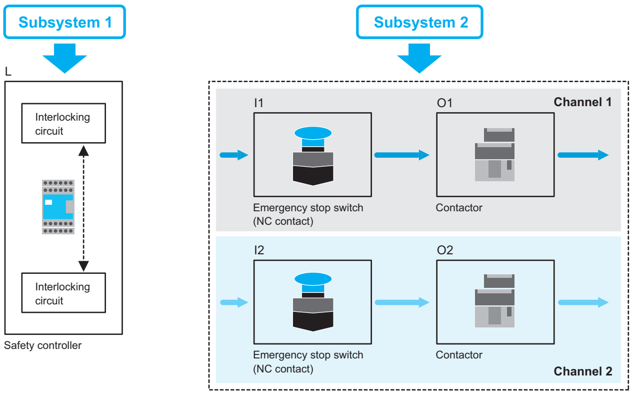
The DC value required for safety-related parts also differs depending on the safety category indicating the structure of the SRP/CS. In the case of buildings for preventing rain and wind, as far as a tent is concerned, repairing it once a year before use would be quite OK. For a wooden housing for daily life, immediate actions are required for termites or leaky roofs if they are found. When it comes to office buildings, unless advance actions are taken in anticipation of possible troubles through the periodic maintenance, a large disaster may result. As described above, the required level of diagnosis must be suitable for the structure.



Layers of DC

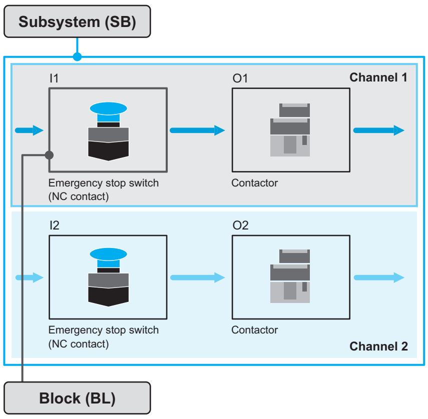
As with $MTTF_D$, you need to determine each DC value for each box in the block diagram that indicates a part. The average of DC values in all blocks at the subsystem level is called DC_{avg} (DC Average). In the figure below, DC_{avg} for subsystem 2 is the average of the DC values of discrete parts (blocks), emergency stop switch and contactor.

Note that DC and DC_{avg} are evaluated in the case of a designated architecture in safety category 2 or higher that has a failure detection function. For category B or 1, which does not have a failure detection function, DC and DC_{avg} are not defined.



DC for a discrete part (block)

The "Layers of DC" section states that DC is determined for each part, but in reality, discrete parts (such as switches and contactors) themselves are not provided with diagnosis functions such as failure detection. In almost all cases, the states of these devices are monitored by the failure diagnosis functions of other devices such as safety controllers. Because of this, it is necessary for the machine designers to determine what failure diagnosis is performed in discrete parts by checking with the diagnosis function on the controller side.


Subsystem (SB)
I1
O1
Channel 1
Emergency stop switch (NC contact)
Contactor
I2
O2
Emergency stop switch (NC contact)
Contactor
Channel 2
Block (BL)

Select the DC of a discrete part (block) from Table E.1 in Annex E of ISO 13849-1 by considering what function is used to achieve failure diagnosis for the part.

Estimating diagnostic coverage (DC) in Annex E of ISO 13849-1:2015

(Excerpt from Table E.1 in Annex E of ISO 13849-1:2015)

Input device		
Measures		DC
1	Cyclic test stimulus by dynamic change of the input signals	90%
2	Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99%
3	Cross monitoring of input devices without dynamic test	0% to 99%, depending on how often a signal change is done by the application
4	Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90%
5	Cross monitoring of input signals and intermediate results within the logic (L), temporary and logical software monitor of the program flow, and detection of static faults and short circuits (for multiple I/O)	99%
6	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application
7	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
8	Fault detection by the process	0% to 99%, depending on the application; this measure alone is not sufficient for the required performance level "e".
9	Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60%

Logic		
Measures		DC
1	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application
2	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%
3	Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60%
4	Temporal and logical monitoring by the watchdog, where the test equipment does plausibility checks of the behavior of the logic	90%
5	Start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90% (depending on the testing technique)
6	Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90%
7	Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99%
8	Invariable memory: signature of one word (8-bit)	90%
9	Invariable memory: signature of double word (16-bit)	99%
10	Variable memory: RAM-test by use of redundant data, e.g. flags, markers, constants, timers and cross comparison of these data	60%
11	Variable memory: check for readability and write ability of data memory cells to use	60%
12	Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. "galpat" or "Abraham")	99%
13	Processing unit: self-test by software	60% to 90%
14	Processing unit: coded processing	90% to 99%
15	Fault detection by the process	0% to 99%, depending on the application; this measure alone is not sufficient for the required performance level "e".

(Excerpt from Table E.1 in Annex E of ISO 13849-1:2015)

Output device		
Measures		DC
1	Monitoring of outputs by one channel without dynamic test	0% to 99%, depending on how often a signal change is done by the application
2	Cross monitoring of outputs without dynamic test	0% to 99%, depending on how often a signal change is done by the application
3	Cross monitoring of outputs without detection of short circuits (for multiple I/O)	90%
4	Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
5	Redundant shut-off path with monitoring of the actuators by logic and test equipment	99%
6	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application
7	Fault detection by the process	0% to 99%, depending on the application; this measure alone is not sufficient for the required performance level "e".
8	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%

Note:1. For information about additional diagnostic coverage (DC) estimation, see Tables A.2 to A.15 of IEC 61508-2:2000.
Note:2. If a "Medium" or "High" DC is requested for logic, at least one measure for ensuring that the DC of each of variable memory, invariable memory, and processing unit is at least 60% must be applied. Failure diagnosis methods may also use measures other than those listed in this table.
Note:3. For methods in which the DC is defined, such as a process-based failure detection method, the correct DC value can be established by considering all dangerous failures and deciding which of them are detected with the failure diagnosis method. If any questions arise, FMEA is regarded as the basis for DC estimation.

Examples of applying a DC to discrete parts

The following table lists the discrete parts (blocks) of typical SRP/CS to which Table E.1 in Annex E is applied.

Part	DC (%)	Relevant item in Annex E	Typical circuit configuration method example
Combination of two switches	99	Plausibility check (input device)	• At least one of the switches is provided with a direct opening action. • The two switches are mechanically connected (via a guard). • Inter-channel cross-monitoring is performed with a safety controller.* • They separately conform to the requirements of ISO 14119 (guard-linked interlocking device).
Relay	99	Direct monitoring (logic) - Monitoring of electromechanical device with mechanically linked contact elements	• Provided with forced guide contact mechanism. • Monitored by providing feedback to the safety controller.
Contactor	99	Direct monitoring (output device) - Monitoring of electromechanical device with mechanically linked contact elements	• Provided with a mirror contact. • Monitored by providing feedback to the safety controller.

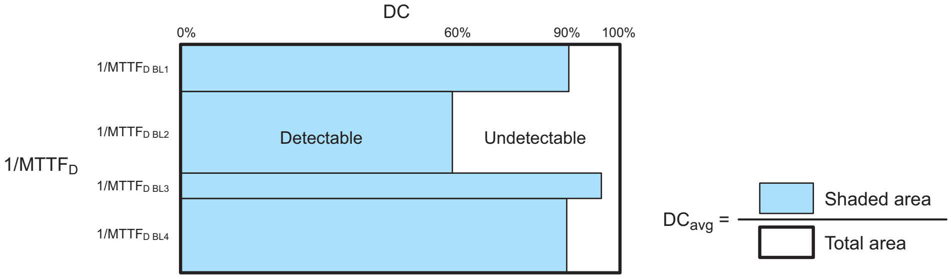
* Because the diagnosis function differs depending on the controller, the DC given may also differ. For details, contact the control device manufacturer.

DC_{avg} for a subsystem

DC_{avg} for a subsystem is obtained by averaging the DC values for all the discrete parts (blocks) composing the subsystem with the following formula.

$$DC_{avg} = \frac{\displaystyle\sum_{i=1}^{n} \frac{DC_{BLi}}{MTTF_{D_{BLi}}}}{\displaystyle\sum_{i=1}^{n} \frac{1}{MTTF_{D_{BLi}}}} \quad \text{(Formula 6)}$$

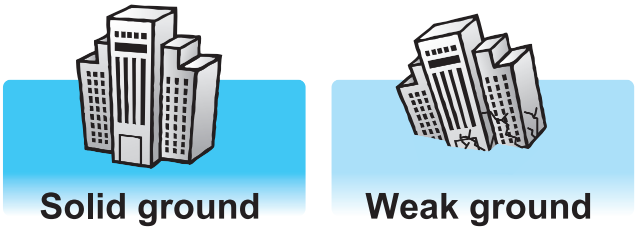
To obtain DC_{avg}, $MTTF_D$ values for the respective blocks are used. In other words, it is weighted with $MTTF_D$. This is illustrated in the figure below. This means that in a subsystem, a block with a smaller $MTTF_D$ value (lower reliability) has a larger impact on DC_{avg}.



(4) CCF (Common Cause Failure)

Concept of CCF

In general, the term common cause failure (CCF) refers to a failure mode in which multiple systems are all impaired with a common cause. As a PL parameter, a CCF is used to represent the level of tolerance to simultaneous failures of channels. A CCF is, as it were, a reliability index in terms of the engineering management of the design and construction of SRP/CS. This is similar to the ground on which a building is established; even a strong building is susceptible to collapse if erected on a weak ground.



A CCF is not to be evaluated on a block diagram, but is to be evaluated using scores based on the margins in the design specifications, the status of parts mounting on actual devices, the wiring status, and other factors, and is an item to be evaluated by the machine designers. Evaluation scores may vary depending on how much the safety principles effective to eliminating common causes are used.
Check sheets of items to consider for design reasons are supplied in Table F.1 in Annex F of ISO 13849-1. Select check boxes for the relevant items and add together the scores to obtain the CCF for the machine.
It is not necessary to consider the CCF in category B or 1. In the designated architecture of a redundant system in category 2 or higher, a CCF score of 65 points or higher is an essential requirement.

CCF scores in Annex F of ISO 13849-1

(Excerpt from Table F.1 in Annex F of ISO 13849-1:2015)

No.	CCF	Score
1	**Separation/segregation**	
	Physical separation between signal paths, for example: - separation in wiring/piping - detection of short circuits and open circuits in cables by dynamic test - separate shielding for the signal path of each channel - sufficient clearances and creepage distances on printed-circuit boards	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: - first channel electronic or programmable electronic, and second channel hardwired - different initiation of safety function for each channel (e.g. position, pressure, temperature) and/or digital and analog measurement of variables (e.g. distance, pressure, temperature) and/or components of different manufacturers	20
3	**Design/application/experience**	
3.1	Protection against overvoltage, overpressure, overcurrent, over-temperature, etc.	15
3.2	Components used are "well-tried".	5
4	**Assessment/analysis**	
	For each part of safety-related parts of control system, a failure mode and effect analysis (FMEA) has been carried out and its results taken into account to avoid common cause failures in the design.	5
5	**Competence/training**	
	Training of designers to understand the causes and consequences of common cause failures.	5
6	**Environmental**	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic compatibility (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Note: For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
	Total	**Maximum 100**

Total score	Measures for avoiding CCF
65 or more	Meet the requirements
Less than 65	Process failed Choose additional measures

(5) PFH_D (Probability of Dangerous Failure per Hour)

What is PFH_D?

PFH_D is a parameter derived from the concept of functional safety. It means the number of dangerous failures that a device causes per hour, that is, a probability of dangerous failures. It is defined in functional safety standards such as IEC 62061.
The reliability of an SRP/CS can be obtained with the sum of PFH_D values of all the subsystems composing it. A PL evaluation method using PFH_D is stated in technical documents such as ISO/TR 23849, which is a guidance on the application of ISO 13849-1.

Conversion into PFH_D

PFH_D can be obtained from a combination of category, $MTTF_D$, and DC_{avg}. For conversion into PFH_D, you can use Table K.1 in Annex K of ISO 13849-1, which indicates the relation between category, $MTTF_D$, DC_{avg}, and PL. PFH_D is a very small value, and is represented with a combination of exponent and mantissa.

Relation between parameters, PFH_D, and PL in Table K.1 in Annex K of ISO 13849-1:2015 (excerpt)

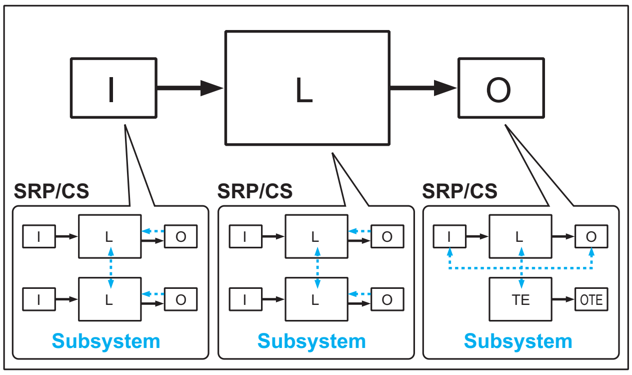
$MTTF_D$ for each channel (years)	PFH_D and corresponding PL													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high	
3	$3,80 \times 10^{-5}$	a			$2,58 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	a	$1,26 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b		
3,3	$3,46 \times 10^{-5}$	a			$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	a	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b		
3,6	$3,17 \times 10^{-5}$	a			$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b		
3,9	$2,93 \times 10^{-5}$	a			$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b		
4,3	$2,65 \times 10^{-5}$	a			$1,76 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b		
4,7	$2,43 \times 10^{-5}$	a			$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b		
5,1	$2,24 \times 10^{-5}$	a			$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b		
5,6	$2,04 \times 10^{-5}$	a			$1,33 \times 10^{-5}$	a	$9,87 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c		
6,2	$1,84 \times 10^{-5}$	a			$1,19 \times 10^{-5}$	a	$8,80 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c		
6,8	$1,68 \times 10^{-5}$	a			$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c		
7,5	$1,52 \times 10^{-5}$	a			$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c		
8,5	$1,39 \times 10^{-5}$	a			$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c		
9,1	$1,25 \times 10^{-5}$	a			$7,94 \times 10^{-6}$	b	$5,71 \times 10^{-6}$	b	$3,57 \times 10^{-6}$	b	$1,53 \times 10^{-6}$	c		
10	$1,14 \times 10^{-5}$	a			$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c		
11	$1,04 \times 10^{-5}$	a			$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c		
12	$9,51 \times 10^{-6}$	b			$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c		
13	$8,78 \times 10^{-6}$	b			$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d		
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b	$1,82 \times 10^{-6}$	c	$7,44 \times 10^{-7}$	d		
16	$7,13 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c	$1,67 \times 10^{-6}$	c	$6,76 \times 10^{-7}$	d		
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d		
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d		
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d		
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d		
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d		
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d	$1,78 \times 10^{-7}$	d	$7,11 \times 10^{-8}$	e
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d	$1,54 \times 10^{-7}$	d	$6,37 \times 10^{-8}$	e
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$		[illegible] $\times 10^{-7}$	d	$3,35 \times 10^{-7}$		[illegible] $\times 10^{-7}$	d	$5,76 \times 10^{-8}$	e
910													$2,51 \times 10^{-9}$	e
1 000													$2,28 \times 10^{-9}$	e
1 100													$2,07 \times 10^{-9}$	e
1 200													$1,90 \times 10^{-9}$	e
1 300													$1,75 \times 10^{-9}$	e
1 500													$1,51 \times 10^{-9}$	e
1 600													$1,42 \times 10^{-9}$	e
1 800													$1,26 \times 10^{-9}$	e
2 000													$1,13 \times 10^{-9}$	e
2 200													$1,03 \times 10^{-9}$	e
2 300													$9,85 \times 10^{-10}$	e
2 400													$9,44 \times 10^{-10}$	e
2 500													$9,06 \times 10^{-10}$	e

Note: For the entire contents of Table K.1, see Appendix (2).

5. Reliability Evaluation of Independent Subsystems

The term independent subsystem refers to a device that itself has a PL evaluation value as stated in "3. Procedure for Evaluating the PL for SRP/CS". Typical such devices include safety light curtains and safety controllers. Because their internal hardware structures are configured with a designated architecture and the reliability of the devices themselves is already evaluated, reliability data including PL and PFH_D is provided by control device manufacturers.

SRP/CS (entire system)



If such an independent subsystem is contained in an SRP/CS, PFH_D of the independent subsystem must be added to the PFH_D evaluation result in the subsystem consisting of discrete parts (blocks). If PFH_D is not provided, use the category, $MTTF_D$, and DC_{avg} for conversion into PFH_D, as previously described.
For some safety devices with complex electronic circuits, a value called the safety integrity level (SIL) is released. Devices that have an SIL evaluation value are devices that have been evaluated with functional safety standards IEC 62061 and/or IEC 61508, and are classified into different levels based on the PFH_D value. It can be said from this that even parts that have SIL evaluation values can be subject to PL evaluation by using PFH_D.
Note that PL and SIL are supported via PFH_D as shown below.

PL	PFH_D		SIL*
	Mantissa	Exponent	
a	10 > n ≥ 1	$\times 10^{-5}$	Not supported
b	10 > n ≥ 3	$\times 10^{-6}$	1
c	3 > n ≥ 1	$\times 10^{-6}$	1
d	10 > n ≥ 1	$\times 10^{-7}$	2
e	10 > n ≥ 1	$\times 10^{-8}$	3

IEC 61508-1, evaluation by high continuous mode of operation

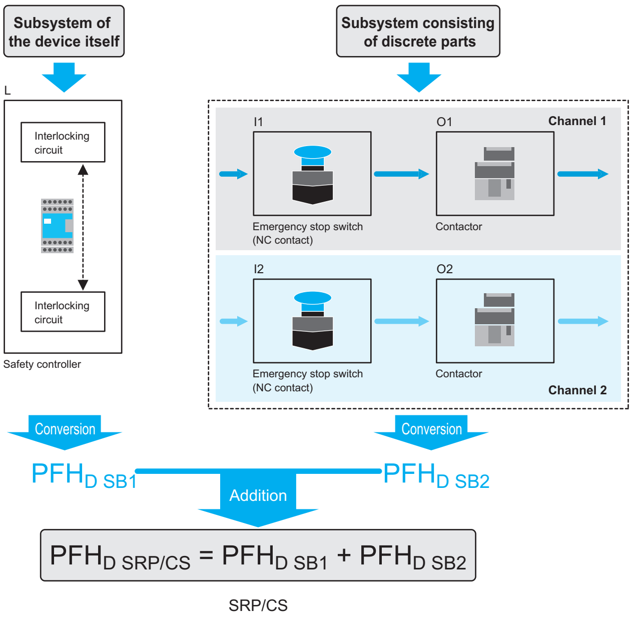
Note: In the PL evaluation of SRP/CS, you must make sure that the various requirements of ISO 13849-1 are satisfied, in addition to performing simple conversion from PFH_D and SIL based on the table above. Also, there are cases where SIL is not always linked with the magnitude of PFH_D depending on the hardware structure, because of the restriction called an SIL claim limit.

6. PL Determination

1) PL determination through PFH_D summation

The PL for SRP/CS is evaluated with the sum of the dangerous failure probabilities of all subsystem, that is, the sum of PFH_D values. Add together all the PFH_D values of the subsystems composing the SRP/CS in order to determine the PL with the sum.

$$PFH_{D\ SRP/CS} = \sum_{i=1}^{n} PFH_{D\ SBn} \qquad \text{(Formula 7)}$$


Subsystem of the device itself
Subsystem consisting of discrete parts
L
Interlocking circuit
Interlocking circuit
Safety controller
I1
O1
Channel 1
Emergency stop switch (NC contact)
Contactor
I2
O2
Emergency stop switch (NC contact)
Contactor
Channel 2
Conversion
Conversion
PFHD SB1
PFHD SB2
Addition
PFHD SRP/CS = PFHD SB1 + PFHD SB2
SRP/CS

The PL for the SRP/CS can be easily determined from the sum of all the PFH_D values of the subsystems. This is because PL and PFH_D have the relation below.

PL	PFH_D	
	Mantissa	Exponent
a	$10 > n \geq 1$	$\times 10^{-5}$
b	$10 > n \geq 3$	$\times 10^{-6}$
c	$3 > n \geq 1$	$\times 10^{-6}$
d	$10 > n \geq 1$	$\times 10^{-7}$
e	$10 > n \geq 1$	$\times 10^{-8}$

IEC 61508-1, evaluation by high continuous mode of operation

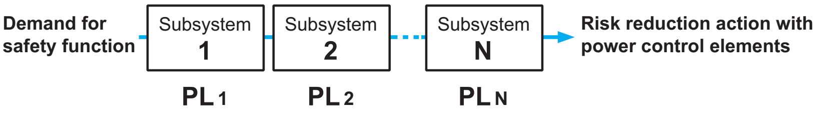
If, for example, the sum of PFH_D values is 1.50×10^{-7}, the exponent is the -7th power of 10, so that, from the table above, the PL for the SRP/CS can be determined to be d.

Regardless of the PFH_D values finally calculated, if the SRP/CS contain an independent subsystem, the result of evaluating the PL never exceeds the result of evaluating the PL for the independent subsystem. If, for example, the SRP/CS contain an independent subsystem that declares a PL of d, the result of evaluating the PL is d at the most.

2) Simplified determination method

For a product for which only the PL for a subsystem is declared by the control device manufacturer and for which PFH_D and other detailed data is not provided, you can evaluate the PL for the SRP/CS by using the PL for the subsystem in a simplified manner.

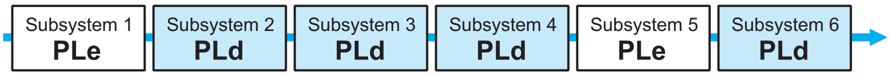
Simplified determination of the PL is performed based on the following.


Demand for safety function
Subsystem 1
Subsystem 2
Subsystem N
Risk reduction action with power control elements
PL 1
PL 2
PL N

1. Identify the lowest PL (PL_{low}) of the PL values for all subsystems.
2. Identify the number of subsystems that have the same PLlow (N_{low}) value.
3. Determine the PL for the SRP/CS according to the table below.

PL_{low}	N_{low}	PL
a	> 3	None
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

For a combination of the following subsystems, for example, the PL for the SRP/CS is c.



PL	Count (N)
e	2
d	4

Note: Neither of the methods used here, ① the method of determining the PL for the SRP/CS with the summation of the PFH_D values for the subsystems and ② the method of determining the PL for the SRP/CS with the number of PL_{low} values for the subsystems, means compatibility between ISO 13849-1 and IEC 62061.
The PFH_D values alone do not testify conformity with ISO 13849-1, and the achieved PL does not testify conformity with IEC 62061 or IEC 61508 SIL.
In addition to PFH_D and $MTTF_D$ values, confirmation and/or certification that the parts meet the ISO 13849-1 requirements such as category and CCF is necessary.

7. Basic Safety Functions for Risk Reduction in the Event of Failures

If electric device failures or disturbances may cause hazardous situations, threatening to impair the machine or works being processed, appropriate actions must be taken to minimize the probability of the occurrence of hazards. This section describes the main actions for minimizing the risks in the event of failures based on IEC 60204-1.

1) Use of tried-and-true circuit technologies and parts

1. The basic circuit configuration must consider earth faults.

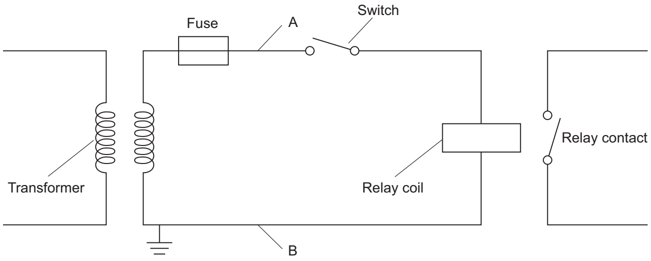
Typical action examples are listed below.

• Basic circuit configuration

The main considerations about the configuration when designing the safety circuit for a control system are listed below.

(1) The relay contact in the safety circuit must be opened when the coil is not excited.
(2) Connect one line of the safety circuit on the secondary winding of the isolation transformer to the earth.
(3) Place all the coils in the safety circuit as close to the earth line as possible and directly connect them.
(4) Be sure to attach a fuse to the safety circuit.

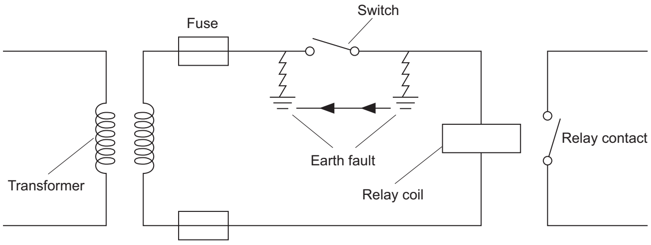
Shown below is the basic configuration of the safety circuit into which items (1) to (4) are incorporated.



If an earth fault occurs on switch line A, the fuse is blown to shut off the electric path. Because coil line B is earthed, there is no earth fault.

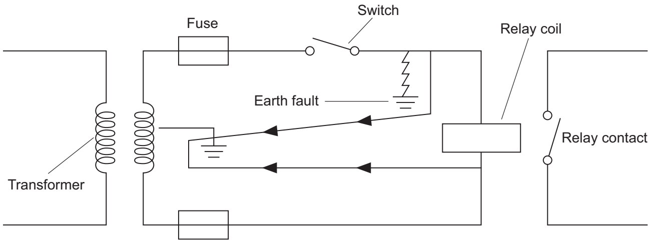
• Earth fault example

If the safety circuit is not earthed



Two earth faults may bypass the switch, possibly causing the machine to suddenly start or to be unable to stop.

If the safety circuit is earthed in the middle of the secondary winding of the transformer



A single earth fault may cause 50% of the voltage to be kept applied to the relay coil, possibly causing the machine to be unable to stop.

2. Means for enabling the shutoff or stop of the hazard must be provided with the stoppage principle.

It is requested to select appropriate stop methods and stop categories according to the risk reduction measures and configure a circuit suitable for the selected ones.

3. Safety standard-certified parts must be used.

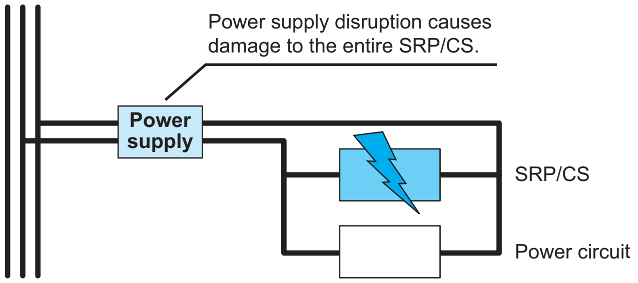
It is requested that the parts to use conform to the related standards.

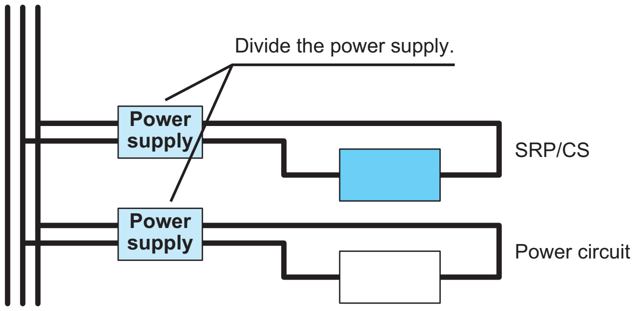
4. A safety switch that performs reliable opening operation must be used.

Standard-certified products above are labeled with the ⊖ mark.

5. The functions of the SRP/CS must not be impaired with a single power failure.

Isolate the power supplies of the SRP/CS from those of the power systems.





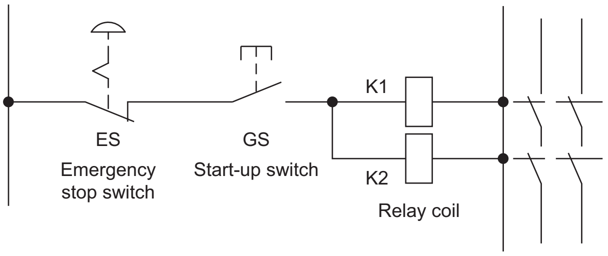
2) Conducting a periodic function test

Perform the function test particularly related to safety either automatically or manually with a control system.
Conduct the test at the beginning of the business hours and after a certain period of time. If a failure is detected, it is necessary to make sure that the machine is not restarted until the cause is clarified.

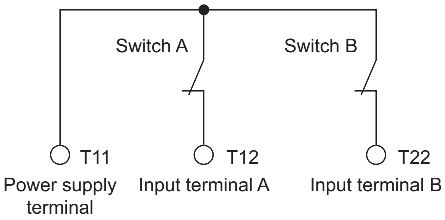
3) Redundant circuit configuration

Providing a partial or overall redundancy can minimize the probability of a single failure in the electric circuit causing a hazard.
For example, by combining two or more relays and switches, the occurrence of a hazardous situation can be avoided even if one of them causes a failure.

• Redundant output circuit configuration example with two relays



• Redundant input circuit configuration example with two switches

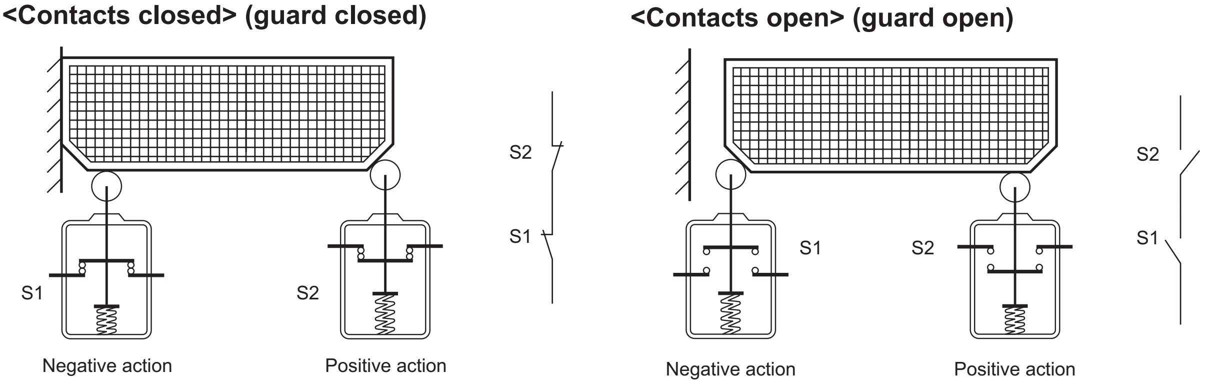


4) Use of diversity

Even if exactly the same parts are used in a redundant circuit configuration, the parts may fail at the same time under the same conditions. For this reason, using control circuits of diversified principles of operation or various types of devices or parts can reduce the probability of failures due to common causes.
Examples of methods using diversity are given below.

1. Combination of NC contact and NO contact

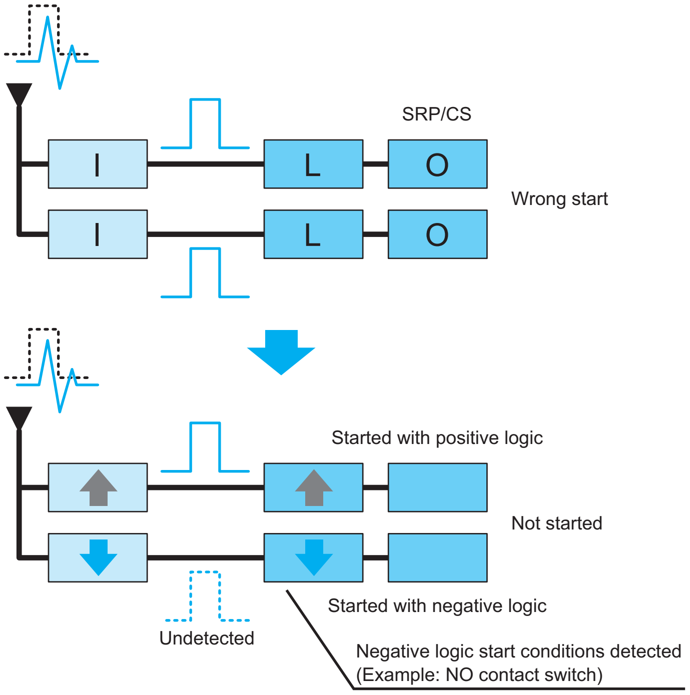
• Example of operating a protective door by combining negative and positive operation switches



2. Using different types of control parts

• Example of combining positive and negative logic operation sensors

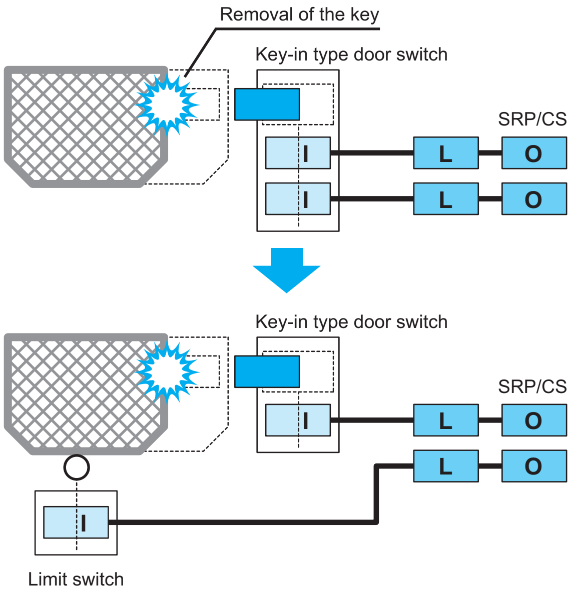
If a wrong signal is input to channels 1 and 2 due to a surge, for example, the noise of the same phase is eliminated by reversing the logic of the signals between the two channels to have reverse phases.


SRP/CS
I
L
O
I
L
O
Wrong start
Started with positive logic
Not started
Undetected
Started with negative logic
Negative logic start conditions detected
(Example: NO contact switch)

3. Redundant circuit configuration combining electromechanical circuits and electronic circuits

• Example of using different types of switches together

Two different types of detection means detect the opening/closing of the guard. A single key-in type switch may cause common cause failures such as the removal of the key. If this risk cannot be eliminated, a different type of means such as a limit switch must be used together.



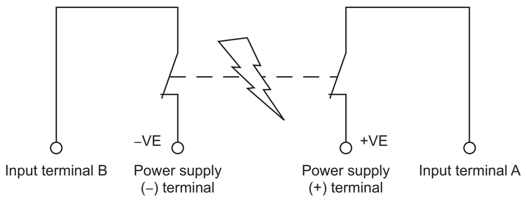
Note: It is necessary to determine the types of switches and their usage based on the risk assessment results and Type C standard requirements.

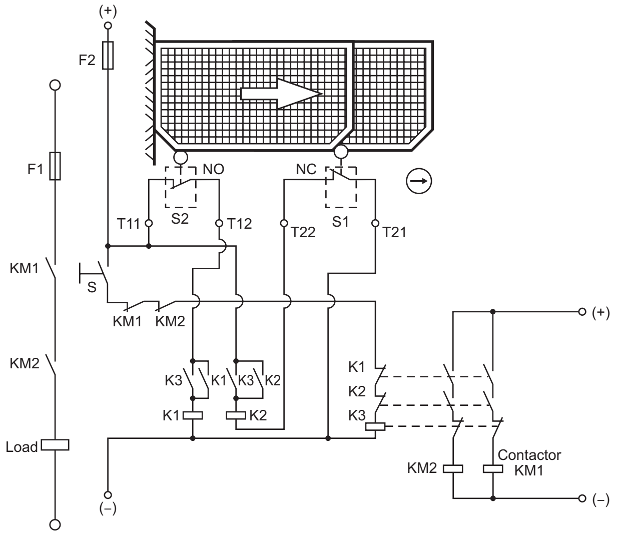
5) Short circuit protection or short circuit detection

Damages to wiring due to the impacts of squashing, high temperature, hitting, or chemical substances may cause a shunt or short circuit to the wiring. These impacts can be eliminated by providing short circuit protection on the safety control circuit.
To provide a short circuit protection, the following conditions must be met:

(1) The safety control circuit must be provided with two-channel inputs each having NC contacts.
(2) There must be a potential difference between channels.

• Circuit example in which 2-channel switch inputs are provided with a short circuit detection function





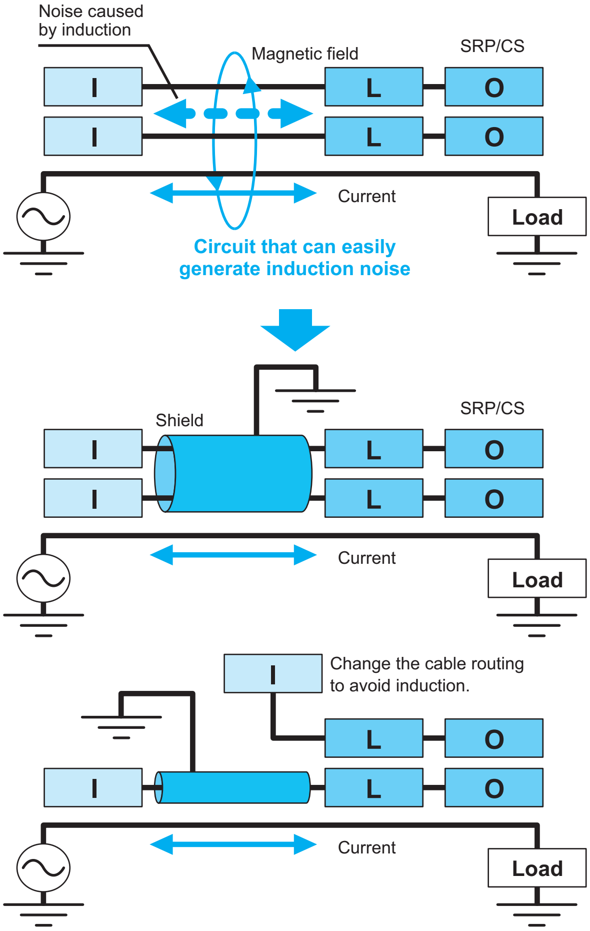
Note: Operation verification is not performed in the circuit example. For actual circuit construction, confirmation is required including the confirmation of conformity with safety standards.

6) Electromagnetic compatibility (EMC)

The circuitry must have an appropriate immunity to electromagnetic interference for proper operation in an intended environment of use.

• Examples of enhancing EMC

- Install an appropriate shield to a path where the impedance is likely to increase (for example, a cable connecting together an external sensor and the controller in the control panel).
- Change the cable routing to avoid induction (change the routing of two channels to avoid the interference from the same noise source on them both).
- Check the electromagnetic immunity with an EMC test.


Noise caused by induction
Magnetic field
SRP/CS
I
I
L
L
O
O
Current
Load
Circuit that can easily generate induction noise
Shield
SRP/CS
I
I
L
L
O
O
Current
Load
I
Change the cable routing to avoid induction.
L
O
I
L
O
Current
Load

7) Operation in other intended environments

• Considerations about the installation location

If input parts such as switches are to be installed close to a processing part, considerations are necessary to ensure that the parts are not impaired or do not malfunction, resulting in dangerous failures, due to heat (high or low temperature), installation in an environment exceeding the ratings of the parts, and chemical substances.

• Considerations about vibration

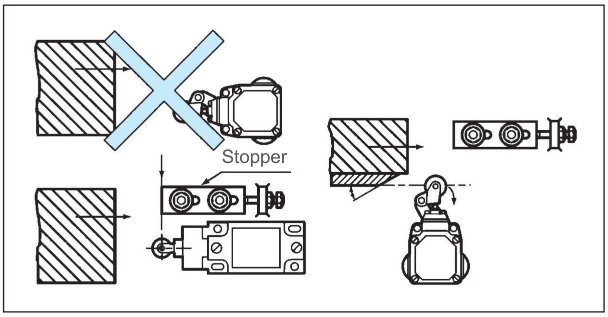
Make sure that mechanical contact parts such as relays are not installed where there is large vibration.

• Considerations about mechanical stress

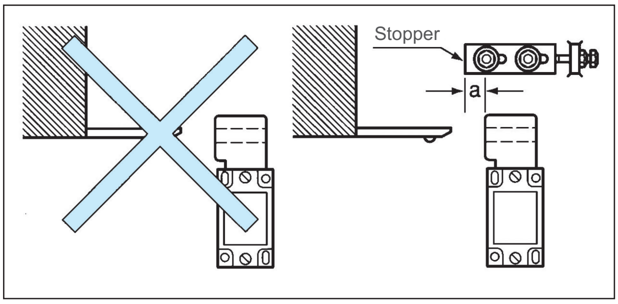
Be careful about mechanical stress so that the devices can exhibit their expected effects.

Consider the following, for example.

- Design and mount the limit switch dogs so that overtravel may not occur.



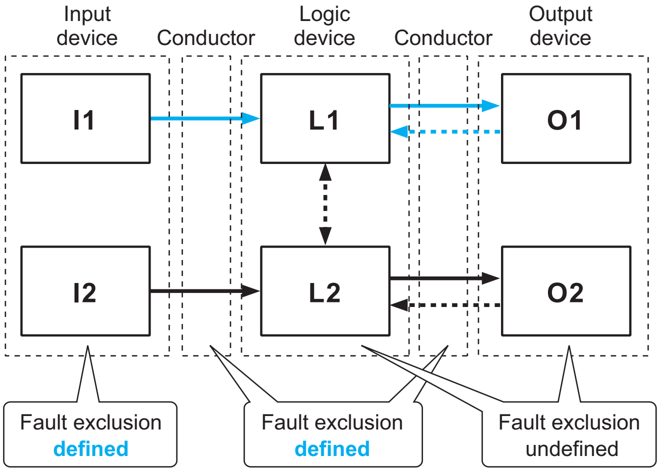
- Install a stopper to prevent the head of the key-in type door switch from being impacted by the guard.



- Observe the design value of the key insertion radius for the key-in type door switch.

8. Concept of Fault Exclusion

Fault exclusion refers to a rule whereby, because under a certain condition, the parts are not broken dangerously or are broken in a predefined way, there are no dangerous faults within the range of the condition. Conditions for fault exclusion are defined in the series standard, ISO 13849-2. Applying fault exclusion in ISO 13849-1 means that the $\mathrm{MTTF_D}$ and/or $\mathrm{DC_{avg}}$ of the relevant SRP/CS need not be considered.



Take a circuit comprised of typical electromechanical parts as an example. Of the input devices (I), logic devices (L), output devices (O), and the conductors as interfaces in the designated architecture, ISO 13849-2 defines fault exclusion for switches and conductors alone.

For example, for a switch conforming to Annex K of IEC 60947-5-1, that is, a switch provided with a direct opening action, fault exclusion is applicable to the fault mode, "contact does not open". For short circuits between terminals inside a switch, fault exclusion is applicable if the switch conforms to IEC 60947-5-1. For conductors such as cables, fault exclusion is applicable if appropriate cable protection is provided and the structure conforms to IEC 60204-1.

It is not that parts are not broken dangerously under any conditions. Depending on the use, fault exclusion cannot be applied. For example, fault exclusion is not defined for the fault, "switch does not close". That is, fault exclusion cannot be applied if the safety function is made to work with the "closing of the switch". Even for devices to which fault exclusion is applicable, it is important to design them with appropriate specifications by recognizing that depending on the conditions, devices "may be broken in a dangerous way". It should also be noted that fault exclusion cannot be applied to all safety components.

For details of faults that can be excluded in a system using electromechanical parts and the conditions for applying fault exclusion, see Annex D of ISO 13849-2.

- **Switches**

For interlocking switches such as door switches and limit switches, mechanical impairment cannot be ignored because the switches are operated with the opening/closing of the guard. If, in particular, the two NC contacts provided with a direct opening action that are built into a single switch (contacts conforming to Annex K of IEC 60947-5-1) are used as the redundant input for SRP/CS, this may cause common cause faults such as the removal and damage of actuators such as keys. Thus, especially if PL_r is e, the application of fault exclusion is not permitted.
For emergency stop switches and enabling switches, the application of fault exclusion is permitted. The reason for this is that they are manually operable switches and the number of operations in the usable life of the machine is sufficiently small as compared with the B_{10D} of the switches and the mechanical damage to the switches can be ignored.

- **Examples of fault exclusion for switches**

Fault considered	Fault exclusion	Remarks
Contact will close	Pressure-sensitive devices in accordance with ISO 13856	–
Contact will open	Contacts in accordance with Annex K of IEC 60947-5-1 are expected to open.	Fault exclusion is only applicable to the opening defects of the electric contacts and the opening defects due to the mechanical factors in the overall switch components cannot be excluded.
Short circuit between adjacent contacts insulated from each other	Short circuit of the contacts conforming to IEC 60947-5-1 can be excluded.	Conductive parts which become loose should not be able to bridge the insulation between contacts.
Simultaneous short circuit between three terminals of change-over contacts	Simultaneous short circuit of the contacts conforming to IEC 60947-5-1 can be excluded.	Conductive parts which become loose should not be able to bridge the insulation between contacts.

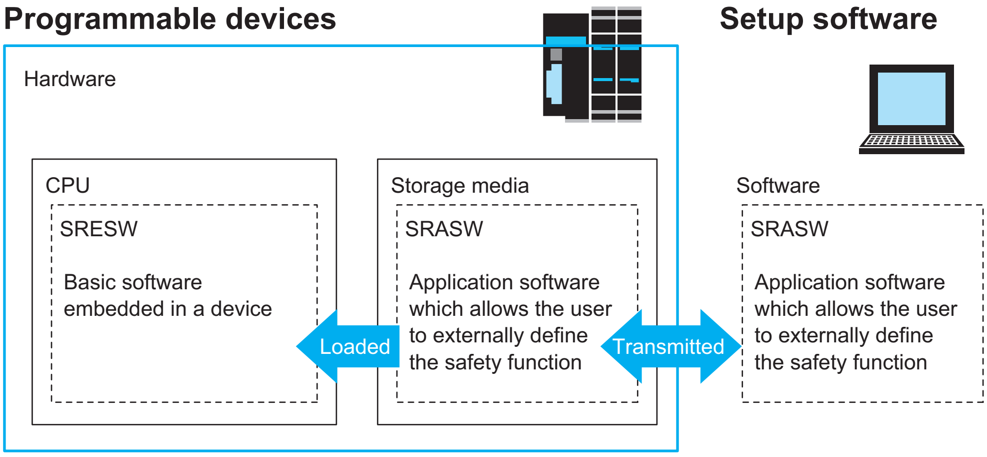
- **Example of fault exclusion for cables**

Fault considered	Fault exclusion	Remarks
Short circuit of conductors/ cables	A short circuit between conductors/cables can be excluded in the following cases: • The cables are secured so that they cannot be removed and are protected from external damage with cable ducts, etc. • They are laid inside the enclosure. (See Remarks.)	Appropriate protection of cables and enclosures conforming to IEC 60204-1

9. Validation for Programmable Devices

Before designing SRP/CS using programmable safety devices, you need to make sure that not only hardware but also software are designed safely.

There are two types of software: application software (SRASW) created by machine designers and firmware (SRESW) embedded in programmable devices. This section mainly describes application software.

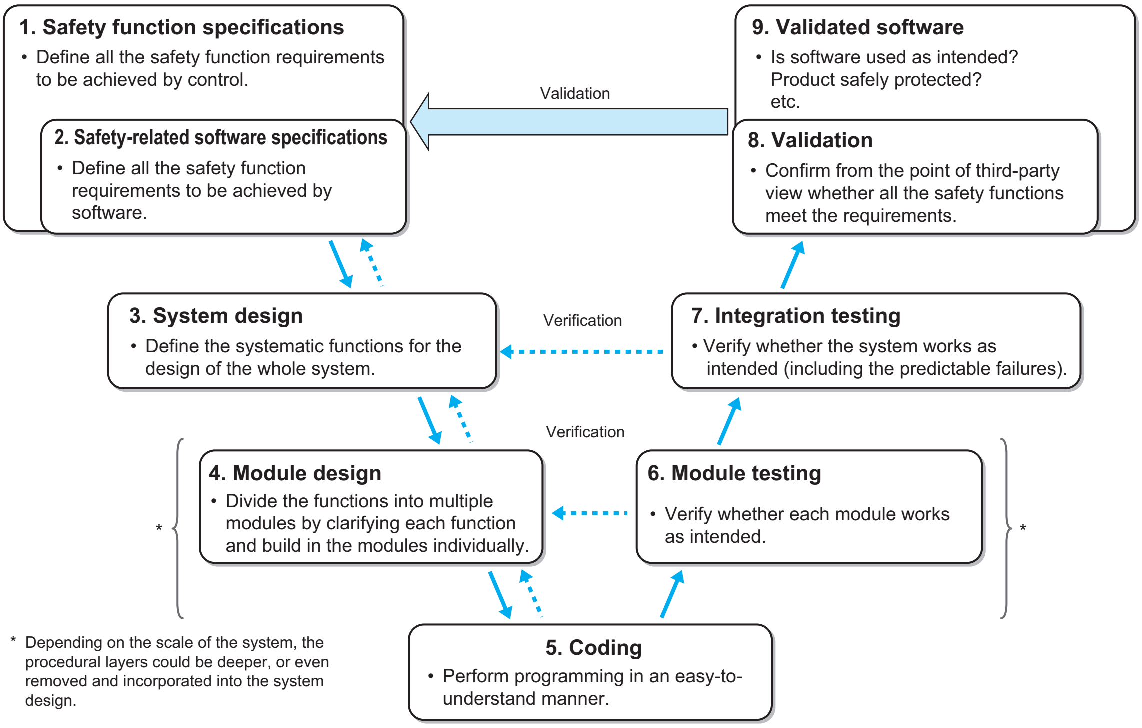

Programmable devices
Hardware
CPU
SRESW
Basic software embedded in a device
Storage media
SRASW
Application software which allows the user to externally define the safety function
Loaded
Transmitted
Setup software
Software
SRASW
Application software which allows the user to externally define the safety function

Design processes for the software of SRP/CS

ISO 13849-1 introduces the V model as a method for indicating the design processes for the software (SRASW) of SRP/CS.

This method is based on the concept of the quality management system ISO 9000 series, and is generally used in the development of not only SRP/CS but also generic software development process.

The design procedure to follow if using software for SRP/CS must be such that, as with the Plan-Do-Check-Action flow in quality control management, the documents necessary in each design phase are prepared first and it is then indicated to third parties that safety functions are appropriately configured with software. For details of respective design processes, see the appendix of this chapter, "(3) Design processes for the software of SRP/CS".

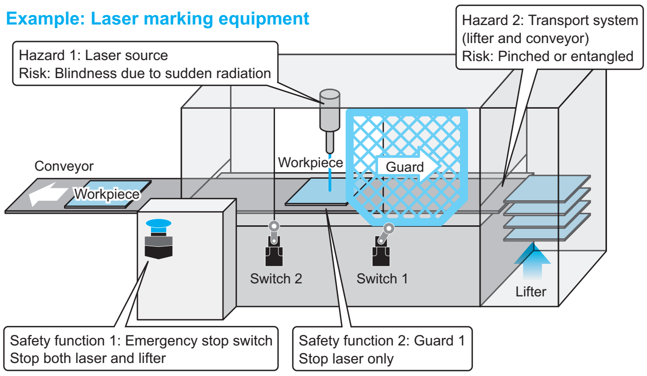

1. Safety function specifications
• Define all the safety function requirements to be achieved by control.
2. Safety-related software specifications
• Define all the safety function requirements to be achieved by software.
Validation
9. Validated software
• Is software used as intended? Product safely protected? etc.
8. Validation
• Confirm from the point of third-party view whether all the safety functions meet the requirements.
3. System design
• Define the systematic functions for the design of the whole system.
Verification
7. Integration testing
• Verify whether the system works as intended (including the predictable failures).
Verification
4. Module design
• Divide the functions into multiple modules by clarifying each function and build in the modules individually.
6. Module testing
• Verify whether each module works as intended.
*
*
5. Coding
• Perform programming in an easy-to-understand manner.

* Depending on the scale of the system, the procedural layers could be deeper, or even removed and incorporated into the system design.

10. Deployment of SRP/CS in Machines into a Block Diagram

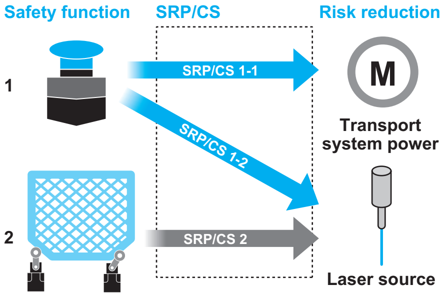
(1) Division according to safety function

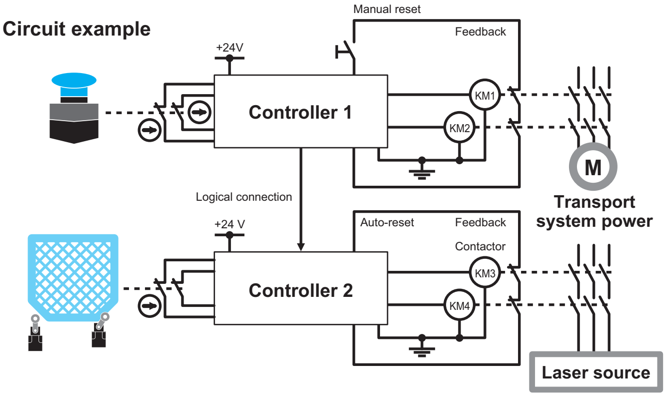
In many cases, the actual machine control system does not have only one safety function. There are some cases in which the machine is provided with more than one safety function for the risks derived from one hazard. There are still other cases in which the machine has multiple hazards and different safety functions are provided for the respective risks. Even in such cases, the PL must basically be calculated for each safety function.
It is not that all safety functions have their respective independent control circuits; they often share the same control circuit.
Suppose a machine shown below as an example that has such multiple safety functions.


Example: Laser marking equipment
Hazard 1: Laser source
Risk: Blindness due to sudden radiation
Hazard 2: Transport system (lifter and conveyor)
Risk: Pinched or entangled
Conveyor
Workpiece
Workpiece
Guard
Switch 2
Switch 1
Lifter
Safety function 1: Emergency stop switch
Stop both laser and lifter
Safety function 2: Guard 1
Stop laser only

This machine has two hazards. One is the laser source. It will cause the loss of eyesight in the worst-case scenario if the laser beam gets into an eye, and it has a PL_r equivalent of d. The other is the transport system (lifter and conveyor), which will cause relatively light dangers such as scraping and bruises due to hands and other body parts being pinched and entangled, and it has a PL_r equivalent of b.
For the laser source, a movable guard is installed so that the laser is shut off when the guard is opened by the interlock. If, for example, a workpiece is stuck in the machine, the operator manually handles it. At this time, he or she stops only the laser because stopping the transport system as well would cause inconvenience in work. In an emergency, the operator presses the emergency stop switch to shut off both the laser source and the transport system power.

Relationship between safety function and risk reduction action is as shown below, as well as a circuit example in which these safety functions are achieved. This machine has three safety functional chains, and the PL for each must be calculated.



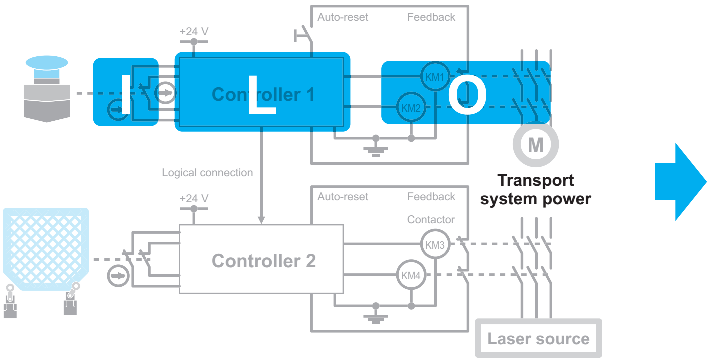


As logic devices, controller 1 shuts off the transport system power and controller 2 shuts off the laser source.
Controllers 1 and 2 are logically connected together with a redundant interface, and the logical input of controller 2 is ANDed together with the physical input system (safety functions 1 and 2). With this, if an operation request for the emergency stop switch is made, both the transport system power and the laser source are shut off, and if an operation request for guard 1 is made, only the laser source is shut off.
It is assumed that for controllers 1 and 2, PFH_D is evaluated individually.

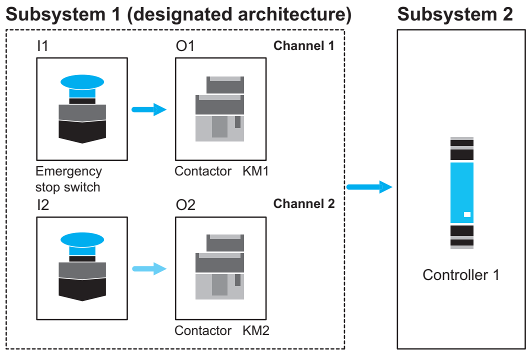
(2) Deploying into a block diagram

SRP/CS 1-1 consists of the designated architecture (subsystem 1), consisting of NC contacts 1 and 2 of the emergency stop switch and contactors KM1 and KM2, as well as controller 1 (subsystem 2), where the PL and PFH_D are evaluated independently.
For subsystem 1, parameters (category, $MTTF_D$, DC_{avg}, CCF) are used to calculate PFH_D.

SRP/CS 1-1

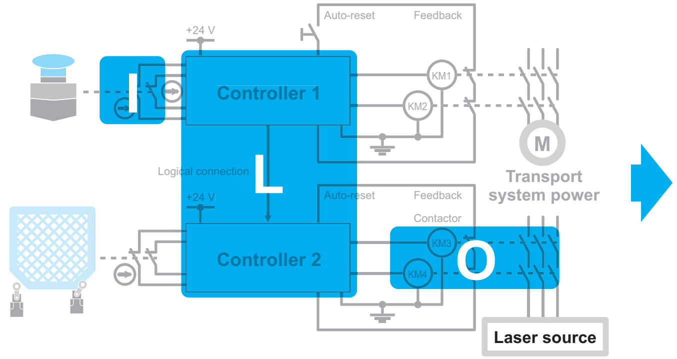


Block diagram

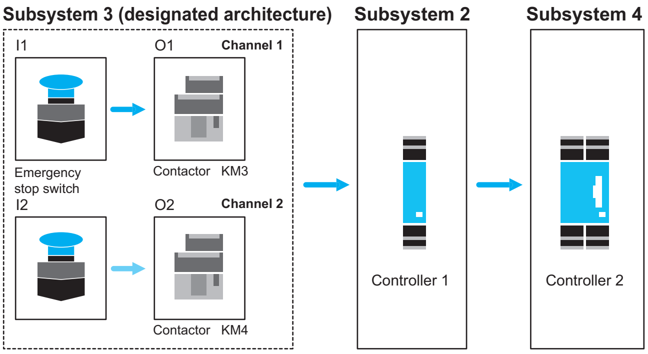


SRP/CS 1-2 consists of the designated architecture (subsystem 3), consisting of NC contacts 1 and 2 of the emergency stop switch and contactors KM3 and KM4, as well as controllers 1 and 2 (subsystems 2 and 4), where the PL and PFH_D are evaluated independently.
For subsystem 3, parameters (category, $MTTF_D$, DC_{avg}, and CCF) are used to calculate PFH_D.

SRP/CS 1-2



Block diagram



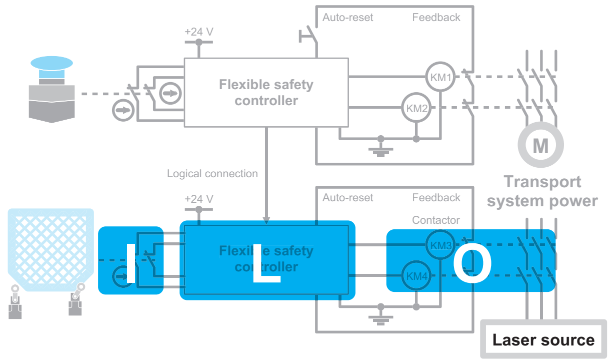
Note: Because contactors KM3 and KM4 are parts shared with SRP/CS 2, $MTTF_D$ is calculated with the sum of n_{op} values for the respective safety functions.
If, however, the operation frequency of one function is so low that it has hardly any impact on the other, this can be regarded as a margin of error and this calculation is not applied. (Example: The guard is operated many times a day, but the emergency stop is operated about once a year.)

Performance Level

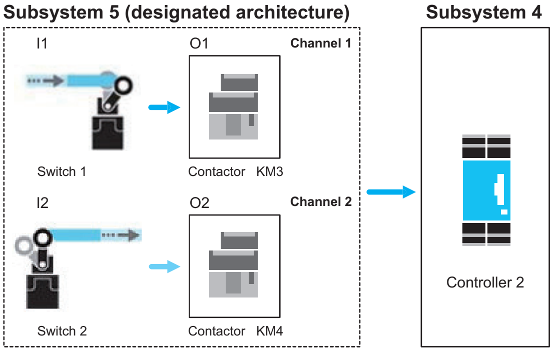
SRP/CS 2 consists of the designated architecture (subsystem 5), consisting of switches 1 and 2 and contactors KM3 and KM4, as well as controller 2 (subsystem 4), where the PL and PFH_D are evaluated independently.

For subsystem 5, parameters (category, $MTTF_D$, DC_{avg}, and CCF) are used to calculate PFH_D.

SRP/CS 2



Block diagram



Note: Because contactors KM3 and KM4 are parts shared with SRP/CS 1-2, $MTTF_D$ is calculated with the sum of n_{op} values for the respective safety functions. If, however, the operation frequency of one function is so low that it has hardly any impact on the other, this can be regarded as a margin of error and this calculation is not applied. (Example: The guard is operated many times a day, but the emergency stop is operated about once a year.)

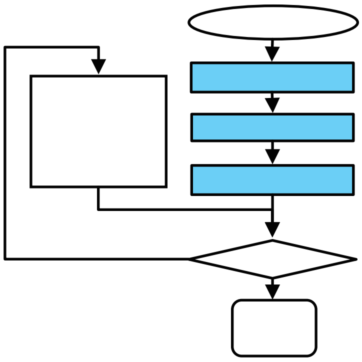
MEMO

11. Appendix

(1) PL evaluation procedure

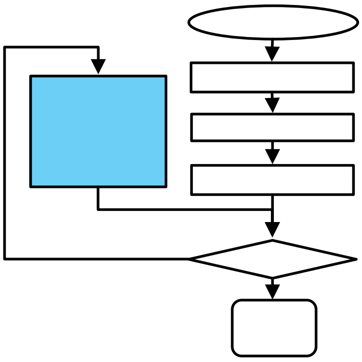
The flows shown below represent the procedure for evaluating the performance level indicated in ISO 13849-1 and ISO/TR 23849. Proceed to safety design and PL evaluation, by referring also the description of the related items.

A

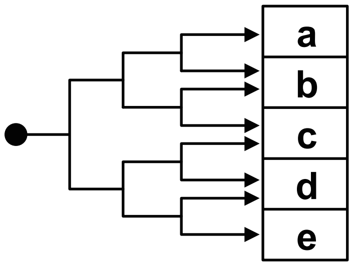


Enumerate the risks with a risk assessment.

B

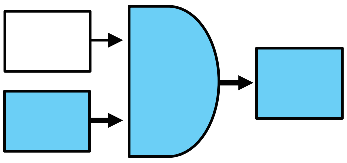


If the risk level is not acceptable, take measures for reducing the risk.

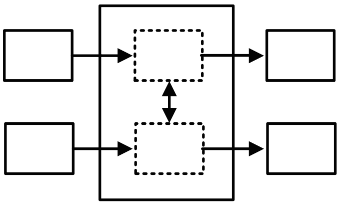


If the measure is control-based, determine the required performance level (PL_r) to be met by the measure (safety function).

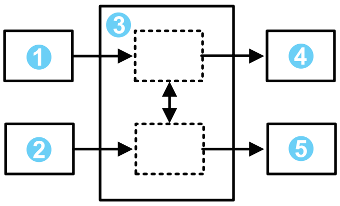
C



Design a control circuit to implement the requested safety function. To achieve the PL_r for the SRP/CS, it is necessary to select the parts having the circuit of designated architecture (category) and reliability to meet the requirements.



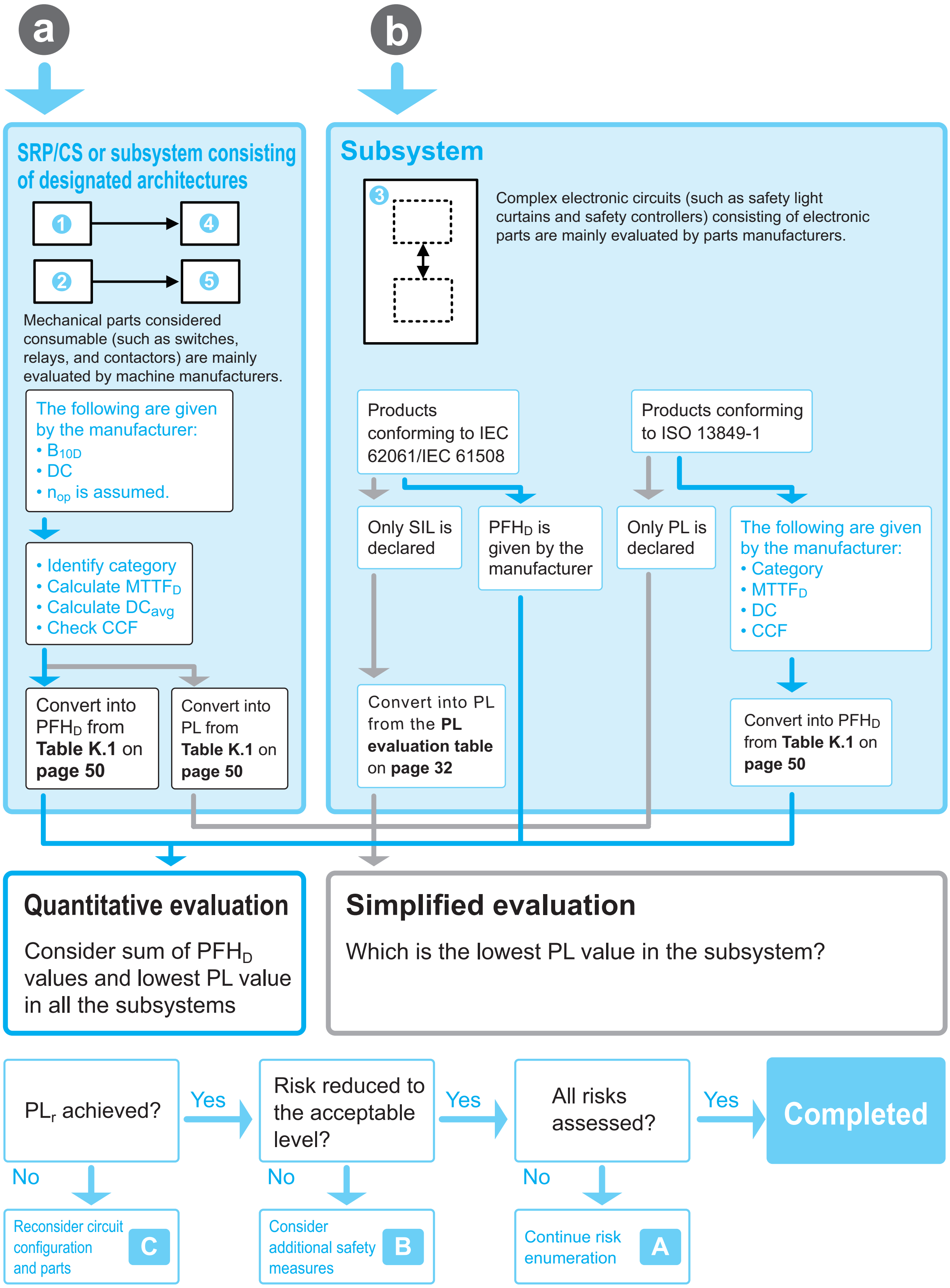
From the control circuit diagram, extract the safety-related parts for transmitting the operating requests for the safety functions and deploy them into a logical block diagram.



Of the safety-related parts, isolate the discrete parts from the parts whose PL is already evaluated and the ones for which the safety integrity level (SIL) is released.

a

b



a

SRP/CS or subsystem consisting of designated architectures

Mechanical parts considered consumable (such as switches, relays, and contactors) are mainly evaluated by machine manufacturers.

The following are given by the manufacturer:

- B_{10D}
- DC
- n_{op} is assumed.

- Identify category
- Calculate $MTTF_D$
- Calculate DC_{avg}
- Check CCF

Convert into PFH_D from **Table K.1** on **page 50**

Convert into PL from **Table K.1** on **page 50**

b

Subsystem

Complex electronic circuits (such as safety light curtains and safety controllers) consisting of electronic parts are mainly evaluated by parts manufacturers.

Products conforming to IEC 62061/IEC 61508

Only SIL is declared

Convert into PL from the **PL evaluation table** on **page 32**

PFH_D is given by the manufacturer

Products conforming to ISO 13849-1

Only PL is declared

The following are given by the manufacturer:

- Category
- $MTTF_D$
- DC
- CCF

Convert into PFH_D from **Table K.1** on **page 50**

Quantitative evaluation

Consider sum of PFH_D values and lowest PL value in all the subsystems

Simplified evaluation

Which is the lowest PL value in the subsystem?

PL_r achieved?

No

Reconsider circuit configuration and parts C

Yes

Risk reduced to the acceptable level?

No

Consider additional safety measures B

Yes

All risks assessed?

No

Continue risk enumeration A

Yes

Completed

(2) Relation between parameters, PFH_D, and PL in Table K.1 in Annex K of ISO 13849-1:2015

$MTTF_D$ for each channel (years)	PFH_D and corresponding PL													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high	
3	3,80 x 10^{-5}	a			2,58 x 10^{-5}	a	1,99 x 10^{-5}	a	1,26 x 10^{-5}	a	6,09 x 10^{-6}	b		
3,3	3,46 x 10^{-5}	a			2,33 x 10^{-5}	a	1,79 x 10^{-5}	a	1,13 x 10^{-5}	a	5,41 x 10^{-6}	b		
3,6	3,17 x 10^{-5}	a			2,13 x 10^{-5}	a	1,62 x 10^{-5}	a	1,03 x 10^{-5}	a	4,86 x 10^{-6}	b		
3,9	2,93 x 10^{-5}	a			1,95 x 10^{-5}	a	1,48 x 10^{-5}	a	9,37 x 10^{-6}	b	4,40 x 10^{-6}	b		
4,3	2,65 x 10^{-5}	a			1,76 x 10^{-5}	a	1,33 x 10^{-5}	a	8,39 x 10^{-6}	b	3,89 x 10^{-6}	b		
4,7	2,43 x 10^{-5}	a			1,60 x 10^{-5}	a	1,20 x 10^{-5}	a	7,58 x 10^{-6}	b	3,48 x 10^{-6}	b		
5,1	2,24 x 10^{-5}	a			1,47 x 10^{-5}	a	1,10 x 10^{-5}	a	6,91 x 10^{-6}	b	3,15 x 10^{-6}	b		
5,6	2,04 x 10^{-5}	a			1,33 x 10^{-5}	a	9,87 x 10^{-6}	b	6,21 x 10^{-6}	b	2,80 x 10^{-6}	c		
6,2	1,84 x 10^{-5}	a			1,19 x 10^{-5}	a	8,80 x 10^{-6}	b	5,53 x 10^{-6}	b	2,47 x 10^{-6}	c		
6,8	1,68 x 10^{-5}	a			1,08 x 10^{-5}	a	7,93 x 10^{-6}	b	4,98 x 10^{-6}	b	2,20 x 10^{-6}	c		
7,5	1,52 x 10^{-5}	a			9,75 x 10^{-6}	b	7,10 x 10^{-6}	b	4,45 x 10^{-6}	b	1,95 x 10^{-6}	c		
8,5	1,39 x 10^{-5}	a			8,87 x 10^{-6}	b	6,43 x 10^{-6}	b	4,02 x 10^{-6}	b	1,74 x 10^{-6}	c		
9,1	1,25 x 10^{-5}	a			7,94 x 10^{-6}	b	5,71 x 10^{-6}	b	3,57 x 10^{-6}	b	1,53 x 10^{-6}	c		
10	1,14 x 10^{-5}	a			7,18 x 10^{-6}	b	5,14 x 10^{-6}	b	3,21 x 10^{-6}	b	1,36 x 10^{-6}	c		
11	1,04 x 10^{-5}	a			6,44 x 10^{-6}	b	4,53 x 10^{-6}	b	2,81 x 10^{-6}	c	1,18 x 10^{-6}	c		
12	9,51 x 10^{-6}	b			5,84 x 10^{-6}	b	4,04 x 10^{-6}	b	2,49 x 10^{-6}	c	1,04 x 10^{-6}	c		
13	8,78 x 10^{-6}	b			5,33 x 10^{-6}	b	3,64 x 10^{-6}	b	2,23 x 10^{-6}	c	9,21 x 10^{-7}	d		
15	7,61 x 10^{-6}	b			4,53 x 10^{-6}	b	3,01 x 10^{-6}	b	1,82 x 10^{-6}	c	7,44 x 10^{-7}	d		
16	7,13 x 10^{-6}	b			4,21 x 10^{-6}	b	2,77 x 10^{-6}	c	1,67 x 10^{-6}	c	6,76 x 10^{-7}	d		
18	6,34 x 10^{-6}	b			3,68 x 10^{-6}	b	2,37 x 10^{-6}	c	1,41 x 10^{-6}	c	5,67 x 10^{-7}	d		
20	5,71 x 10^{-6}	b			3,26 x 10^{-6}	b	2,06 x 10^{-6}	c	1,22 x 10^{-6}	c	4,85 x 10^{-7}	d		
22	5,19 x 10^{-6}	b			2,93 x 10^{-6}	c	1,82 x 10^{-6}	c	1,07 x 10^{-6}	c	4,21 x 10^{-7}	d		
24	4,76 x 10^{-6}	b			2,65 x 10^{-6}	c	1,62 x 10^{-6}	c	9,47 x 10^{-7}	d	3,70 x 10^{-7}	d		
27	4,23 x 10^{-6}	b			2,32 x 10^{-6}	c	1,39 x 10^{-6}	c	8,04 x 10^{-7}	d	3,10 x 10^{-7}	d		
30			3,80 x 10^{-6}	b	2,06 x 10^{-6}	c	1,21 x 10^{-6}	c	6,94 x 10^{-7}	d	2,65 x 10^{-7}	d	9,54 x 10^{-8}	e
33			3,46 x 10^{-6}	b	1,85 x 10^{-6}	c	1,06 x 10^{-6}	c	5,94 x 10^{-7}	d	2,30 x 10^{-7}	d	8,57 x 10^{-8}	e
36			3,17 x 10^{-6}	b	1,67 x 10^{-6}	c	9,39 x 10^{-7}	d	5,16 x 10^{-7}	d	2,01 x 10^{-7}	d	7,77 x 10^{-8}	e
39			2,93 x 10^{-6}	c	1,53 x 10^{-6}	c	8,40 x 10^{-7}	d	4,53 x 10^{-7}	d	1,78 x 10^{-7}	d	7,11 x 10^{-8}	e
43			2,65 x 10^{-6}	c	1,37 x 10^{-6}	c	7,34 x 10^{-7}	d	3,87 x 10^{-7}	d	1,54 x 10^{-7}	d	6,37 x 10^{-8}	e
47			2,43 x 10^{-6}	c	1,24 x 10^{-6}	c	6,49 x 10^{-7}	d	3,35 x 10^{-7}	d	1,34 x 10^{-7}	d	5,76 x 10^{-8}	e
51			2,24 x 10^{-6}	c	1,13 x 10^{-6}	c	5,80 x 10^{-7}	d	2,93 x 10^{-7}	d	1,19 x 10^{-7}	d	5,26 x 10^{-8}	e
56			2,04 x 10^{-6}	c	1,02 x 10^{-6}	c	5,10 x 10^{-7}	d	2,52 x 10^{-7}	d	1,03 x 10^{-7}	d	4,73 x 10^{-8}	e
62			1,84 x 10^{-6}	c	9,06 x 10^{-7}	d	4,43 x 10^{-7}	d	2,13 x 10^{-7}	d	8,84 x 10^{-8}	e	4,22 x 10^{-8}	e
68			1,68 x 10^{-6}	c	8,17 x 10^{-7}	d	3,90 x 10^{-7}	d	1,84 x 10^{-7}	d	7,68 x 10^{-8}	e	3,80 x 10^{-8}	e
75			1,52 x 10^{-6}	c	7,31 x 10^{-7}	d	3,40 x 10^{-7}	d	1,57 x 10^{-7}	d	6,62 x 10^{-8}	e	3,41 x 10^{-8}	e
82			1,39 x 10^{-6}	c	6,61 x 10^{-7}	d	3,01 x 10^{-7}	d	1,35 x 10^{-7}	d	5,79 x 10^{-8}	e	3,08 x 10^{-8}	e
91			1,25 x 10^{-6}	c	5,88 x 10^{-7}	d	2,61 x 10^{-7}	d	1,14 x 10^{-7}	d	4,94 x 10^{-8}	e	2,74 x 10^{-8}	e
100			1,14 x 10^{-6}	c	5,28 x 10^{-7}	d	2,29 x 10^{-7}	d	1,01 x 10^{-7}	d	4,29 x 10^{-8}	e	2,47 x 10^{-8}	e
110													2,23 x 10^{-8}	e
120													2,03 x 10^{-8}	e
130													1,87 x 10^{-8}	e
150													1,61 x 10^{-8}	e
160													1,50 x 10^{-8}	e
180													1,33 x 10^{-8}	e
200													1,19 x 10^{-8}	e
220													1,08 x 10^{-8}	e
240													9,81 x 10^{-9}	e
270													8,67 x 10^{-9}	e
300													7,76 x 10^{-9}	e
330													7,04 x 10^{-9}	e
360													6,44 x 10^{-9}	e
390													5,94 x 10^{-9}	e
430													5,38 x 10^{-9}	e
470													4,91 x 10^{-9}	e
510													4,52 x 10^{-9}	e
560													4,11 x 10^{-9}	e
620													3,70 x 10^{-9}	e
680													3,37 x 10^{-9}	e
750													3,05 x 10^{-9}	e
820													2,79 x 10^{-9}	e
910													2,51 x 10^{-9}	e
1 000													2,28 x 10^{-9}	e
1 100													2,07 x 10^{-9}	e
1 200													1,90 x 10^{-9}	e
1 300													1,75 x 10^{-9}	e
1 500													1,51 x 10^{-9}	e
1 600													1,42 x 10^{-9}	e
1 800													1,26 x 10^{-9}	e
2 000													1,13 x 10^{-9}	e
2 200													1,03 x 10^{-9}	e
2 300													9,85 x 10^{-10}	e
2 400													9,44 x 10^{-10}	e
2 500													9,06 x 10^{-10}	e

Note 1: If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 4.5.4 of ISO 13849-1:2015), then the PFH_D values stated in the Table K.1 for category 2 multiplied by a factor of 1.1 can be used as a worst case estimate.

Note 2: PFH_D values are calculated based on the following DC_{avg} values:
- DC_{avg} = low, calculated with 60%;
- DC_{avg} = medium, calculated with 90%;
- DC_{avg} = high, calculated with 99%.

MEMO

(3) Design processes for the software of SRP/CS

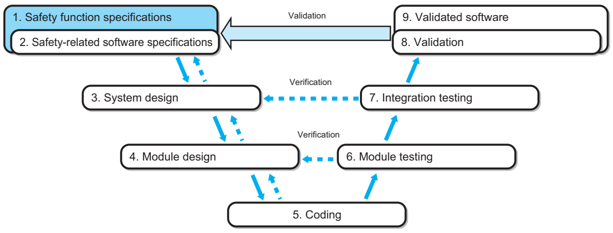
1. Safety function specifications

From the risk assessment sheet, extract all safety functions (safety functions described in ISO 13849-1) achievable with control, and define their operations, performance levels (PL_r), operation frequencies (n_{op}), and so on as requirements in safety function specifications.

Based on the safety function specifications, create a control circuit diagram and a list of parts composing the safety functions. Obtain parts specifications, mechanical safety reliability data for dangerous failures, and so on from device manufacturers. Perform analyses (such as FMEA) on the control circuits and define predictable failures and abuses of parts.

<Document examples>

- Safety function specifications
- Control circuit diagram
- Operation list
- Parts list
- Parts specifications
- Mechanical safety reliability data for dangerous failures



2. Safety-related software specifications

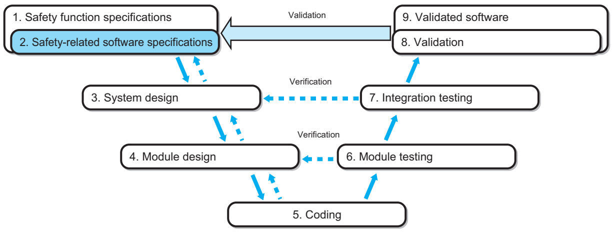
Of the safety functions, define the requirements for the ones to be achieved with software.

From the operation list created on the basis of "1. Safety function specifications", extract only the safety functions related to the programmable safety controller. Create a list of assignment of the I/O devices of safety functions to the I/O of the programmable safety controller in order to determine interface specifications.

From the operation list, determine the logic of the safety functions and operation specifications.

<Document examples>

- Interface specifications
- Operating specifications

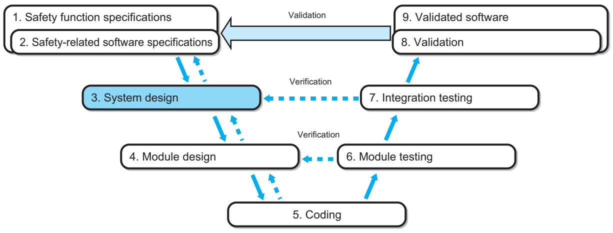


3. System design

Based on the interface specifications, define the variables that are subsequently used in the software design phase. Design the safety functions defined in the external requirement specifications determined on the basis of "1. Safety function specifications". Create a system test procedure in advance to facilitate the verification of all operation systems in the integration testing in the subsequent processes.

<Document example>

- System test procedure



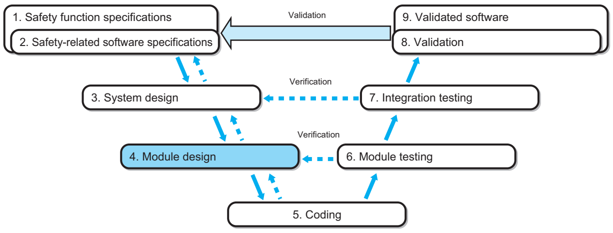
4. Module design

Depending on the scale of the system, combine multiple hardware modules, that is, multiple programmable safety controllers to achieve safety functions. In this case, divide each software program into function blocks for design. Function blocks may include function blocks to be created by designers independently.

Create a test procedure for each module to facilitate verification in the module tests in the subsequent processes.

<Document example>

- Test procedure for each module

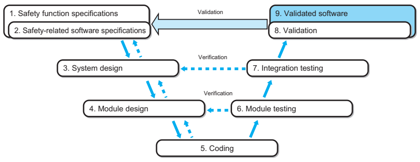


9. Validated software

Upon completion of software validation, integrate it with the hardware of the SRP/CS for validation. Next, with the software embedded in the machine, proceed to confirm risk reduction by integrating the software with mechanism parts and so on.
Once validated, a program is treated as a part integral with hardware. Manage the following and other items in an easy-to-understand manner. If a program needs to be modified in the life cycle of the machine, provide security so that only authorized personnel can modify the program.

<Management item examples>

- Machine type and revision
- Machine user (customer)
- Control circuit design version
- Target module
- Type and revision of the device to which to transfer a program
- Version of a program itself

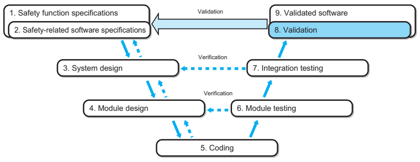


8. Validation

Confirm whether the program is designed according to the safety function specifications, based on the external specifications, by creating input conditions with the program being implemented in the SRP/CS. Confirm also the changes in output including the response performance. Because the confirmation method focuses on external specifications, you need not go into the detailed structure of the software.
Record the results in a validation test confirmation document. If any troubles are found, they may be attributable to the software specifications themselves. Return the specifications to the safety-related software specification process and correct them.

<Document example>

- Validation record

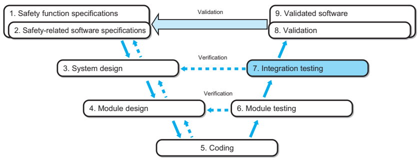


7. Integration testing

Verify whether the operation of the entire software, into which modules are integrated, is as intended, based on the system test procedure. On the development tool simulator, execute all operations of the program at least once, with the program implemented in the SRP/CS in some cases, in order to verify the response performance from the time an input is given until the output reacts, as well as the operations for predictable part failures and abuses defined in the safety function specifications. Record the results in an integration testing result document. Troubles may be attributable to design. Return them to the system design process and correct them. Reverify whether there are any new troubles due to the correction.

<Document example>

- Integration testing result document

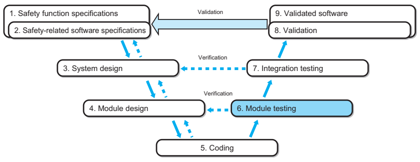


6. Module testing

Verify whether each module operates as intended based on the test procedure for that module. On the development tool simulator, perform verification on the actual device by feeding simulated input in some cases.
Record the results in a module test result document. Troubles may be attributable to design. Return them to the module design process and correct them. Reverify whether there are any new troubles due to the correction.

<Document examples>

- Module test result document
- Software correction procedure

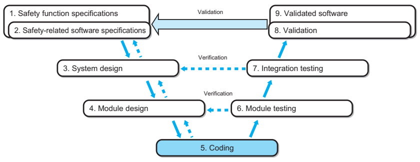


5. Coding

Achieve the system built in with module design, using a program. At this time, create the program by adding comment statements understandable by third parties.
If any troubles are found in the module test or integration test in the subsequent processes, regression is repeated several times in coding for correction. Program versions are managed to notify the subsequent processes what types of troubles are corrected and reflected.

<Document example>

- Program version management



MEMO

Chapter 2

Safety Circuit Examples & PLE Evaluation Cases

1. Introduction 56

Precautions 56

Conditions for PL Evaluation 57

Reliability Data for Safety of Machinery for OMRON Products 57

2. Safety Circuit Examples & PL Evaluation Cases 58

Circuit Example 1: Emergency Stop Switches Connected to Safety Relays 58

Circuit Example 2: Safety Limit Switches Connected to Safety Relay Units 60

Circuit Example 3: Safety Light Curtain (Stand Alone) with Contactors 62

Circuit Example 4: Emergency Stop Switch and Safety Limit Switch Connected to Safety Controllers 64

Circuit Example 5: Emergency Stop Switch and Non-contact Door Switch Connected to Safety Controller 66

Circuit Example 6: Mode switching and STO Functions 68

1. Introduction

This chapter describes circuit examples, as well as PL evaluation cases, using interlock devices. For referring to the cases, keep the followings in mind.

The description is subject to changes due to update of safety standards, products' specifications, improvement of accessories, or other reasons.

Precautions

1. Circuit Configurations for SRP/CS

A variety of circuit examples in this chapter are only intended to show one type of configuration for securing the safety of control systems for machinery. In actual circuit configurations, it is necessary to use protective grounding, wiring protection, and other methods to prevent problems like open circuits and short circuits. With respect to specific measures, it is recommended that you comply with the related standards. Also recommended is to receive verification by a third-party certification body for the safety of the overall system.

2. Determining PL_r

PL_r, which is a performance indicator of safety measures, is determined as a result of a risk assessment. You must determine proper PL_r through risk assessment taking into account the machine specifications as well as working environment including installation, usage, and disposal of the machine.

3. About 2-channel Input

For applications in which the open/closed status of a guard is detected by the contact signals of position detection equipment such as Safety Door Switches, the circuit configuration must be carefully designed. In some cases, a circuit configuration is adopted that has 2-channel input to the control unit (e.g. safety controller) from 2 contacts inside a position detector having multiple contacts, to check open/closed status of a guard. In such a configuration, however, common cause failures may occur in both two contacts due to improper insertion of an operation key and/or broken head unit of the position detector by excessive impact. Depends on the risk assessment, please consider safety measures such as using 2 independent position detection switches to check open/closed status of a guard. ISO/TR 23849:2010 7.2.2.5 and in ISO 14119:2013 8.2 suggest that it is normally not achievable PL=e by using 2 contacts inside a position detector. Therefore it is recommended to consider carefully configurations of components as well as the PLr.

4. The Role of Safety Components

SRP/CS must be designed to minimize the possibility of danger occurring even when there is a failure in an interlocking device. As stipulated by standards, OMRON safety components are equipped with functions such as direct opening action for switches, and forced guide contact mechanisms. These functions are designed to operate effectively within the SRP/CS in which they are contained.

5. How to use Safety Components

Refer to the precautions listed in this catalog and manual for the use of safety components.

Especially the guards fitted with guard lock safety-door switches, please use appropriate fixings together to keep closing conditions. If the guard lock safety-door switch itself have been used as fixing parts for guards, it is capable to cause malfunction of the switches due to the weight of the guard itself, vibration from machinery, misoperation under the locking condition, or impacts during closing.

6. Trip and presence sensing function

The basic feature of the Safety Light Curtain is to detect fingers, hands or bodies of persons. When it is possible that entire human body keep staying hazardous area through detection zone of the Safety Light Curtain, it is recommended to use together with safety devices with presence sensing function such as Safety Mat, Safety Laser Scanner, etc..

7. Reset function

These circuit examples use basically manual resetting. The standards especially stipulate that an emergency stop circuit shall reset manually. When applying manual reset function for interlocking circuit configured with protective equipments, please confirm by risk assessment that the function is not cause to arise hazardous situations, and refer to ISO 12100 6.3.2.5.3 and 6.3.3.2.5. How to configure reset functions are shown in catalogs and manuals of each components.

8. Magnetic Contactors

It is recommended to use contactors with mirror contact, it is mechanism to prevent close of auxiliary contact on welding of the mechanically linked main contact.

Conditions for PL Evaluation

In the circuit examples described in this document, PL is evaluated based on the following usage conditions.
However, these are only examples and you should evaluate PL based on the actual usage conditions in actual applications.

Device	Safety function (Safety component)	Number of operation demanded per year (n_{op})	Reliability Data for Safety of Machinery
Input device	Emergency stop switch	500	Refer to Reliability Data for Safety of Machinery for each product or ISO 13849-1:2015 Annex C.
	Safety limit switch (when used for guard interlocking)	27,500	
	Safety door switch without guard lock function (including non-contact type door switches)	22,000	
	Guard lock safety-door switch	11,000	
	Safety light curtain/single-beam sensor	27,500	
	Two-hand control device	27,500	
	Safety laser scanner/safety mat	11,000	
	Enabling switch/enabling grip switch	500	
Control device	Safety relay	By the total of operation requests of the related input devices	
	Safety controller		
Output device	Power shut off by servo/inverter (STO) * Assumes that this device has the EDM function.	By the total of operation requests of the related input devices	
	Power shut off by contactor (stop category 0) * Assumes that this device has the mirror contactor.		

Reliability Data for Safety of Machinery for OMRON Products

OMRON provides reliability data for safety of machinery for each product category by means of the parameter list (PDF file) and SISTEMA dedicated library to help customers to calculate PL of their devices.
Refer to our web site (www.ia.omron.com).

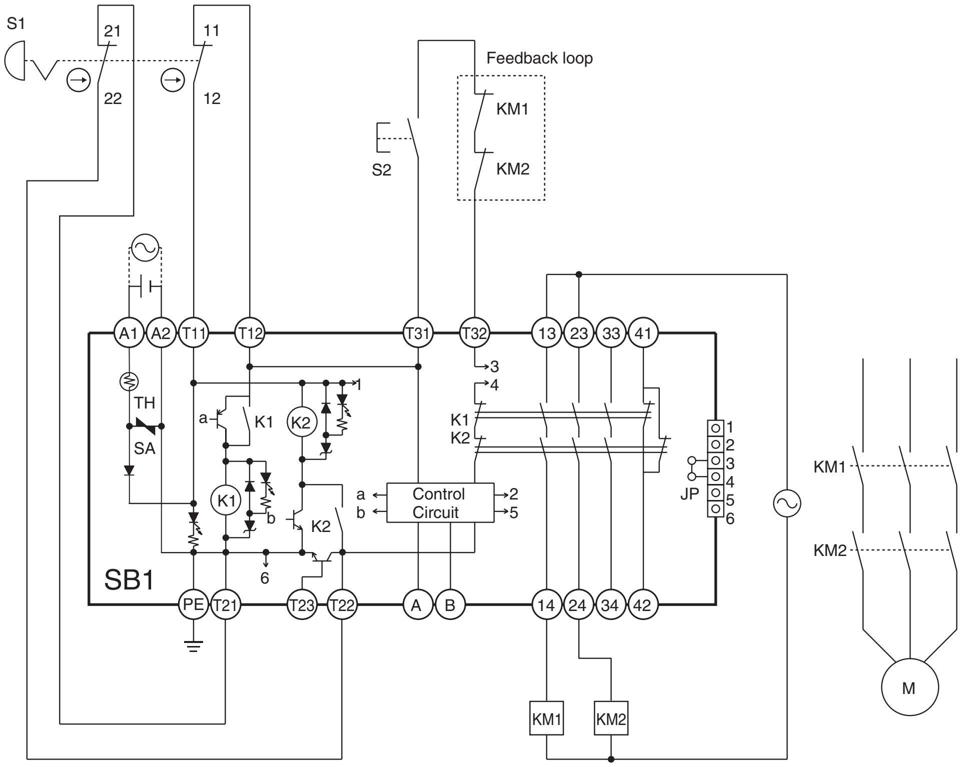
PL evaluation examples in this chapter are based on calculation by SISTEMA v2.0 and the libraries. Evaluation results of safety functions are rounded up to the third decimal place.

2. Safety Circuit Examples & PL Evaluation Cases

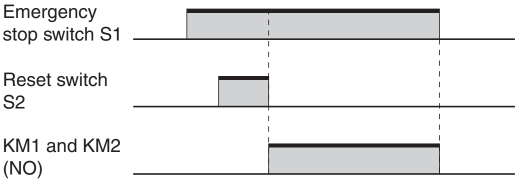
Circuit Example 1: Emergency Stop Switches Connected to Safety Relays

• Safety Functions

Safety function	Operation	Stop function	Reset function
1	• Immediately removes power to Motor M when Emergency Stop Switch S1 is pressed. • The power to Motor M is kept removed until the Emergency Stop Switch is released and Reset Switch S2 is pressed.	Stop category 0	Manual



• Timing Chart



• Model used and machinery safety reliability data

Symbol	Model used	Machinery safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B_{10D}: 100,000
S2	Reset Switch: General push button switch (NO contact, momentary)	-
SB1	Safety Relay Unit G9SA-301 (PLe certified on ISO 13849-1)	Category 4, $MTTF_D$: 100 years, DC_{avg}: 99%
KM1/KM2	Contactor with nominal load	B_{10D}: 1,300,000 [*1]

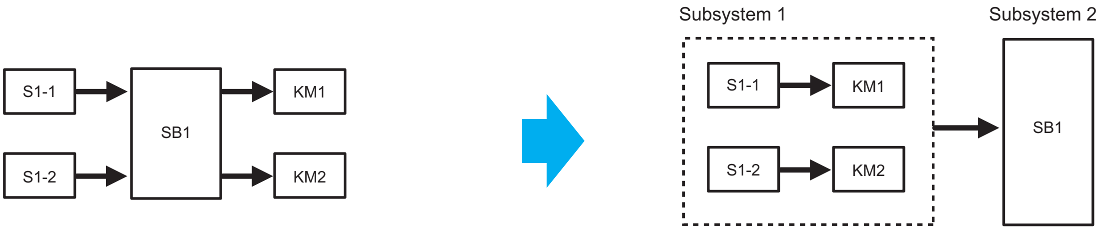
*1. Source: ISO 13849-1: 2015 Annex C

• Developed block diagram

Electrical block diagram of SRP/CS

Developed logical block diagram

Safety function 1



• PL of SRP/CS

Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	S1-1	Faults excluded				4	2,500 [*1]	99	9.06 x 10^{-10} [*2]	e
		KM1	1,300,000	500	26,000	99					
		S1-2	Faults excluded								
		KM2	1,300,000	500	26,000	99					
	2	SB1	PLe certified on ISO 13849-1				4	100	99	2.47 x 10^{-8} [*2]	e
	PFH_D and PL for the SRP/CS									2.56 x 10^{-8}	e

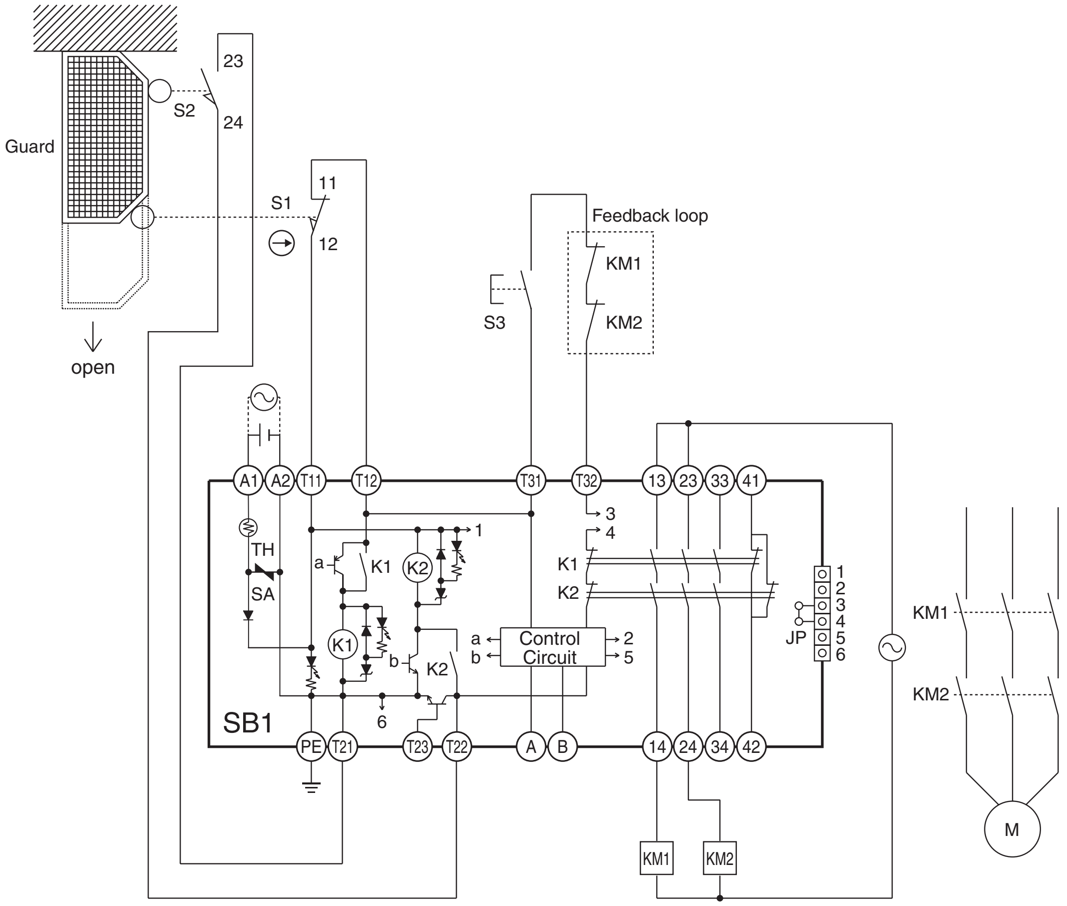
*1. Applied the upper limit of Category 4 $MTTF_D$ or 2,500 years.
*2. Converted to PFH_D based on Table K.1 of Annex K of ISO 13849-1.

Note: The point of CCF shall be at least 65.

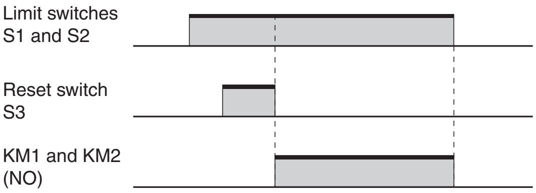
Circuit Example 2: Safety Limit Switches Connected to Safety Relay Units

• Safety Functions

Safety function	Operation	Stop function	Reset function
1	• Immediately removes power to Motor M when limit Switch S1 and S2 detect the opening of the Guard. • The power supply to the motor M is kept OFF until the guard is closed and the reset switch S3 is pressed.	Stop category 0	Manual



• Timing Chart

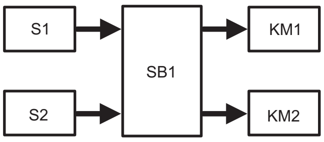


• Model used and machine safety reliability data

Symbol	Model used	Reliability data for safety of machinery
S1	Safety Limit Switch: D4N-□□20 (NC contact direct mechanical action)	B_{10D}: 20,000,000
S2	General limit switch (NO contact)	B_{10D}: 10,000,000
S3	Reset Switch: General push button switch (NO contact, momentary)	-
SB1	Safety Relay Unit G9SA-301 (PLe certified on ISO 13849-1)	Category 4, $MTTF_D$: 100 years, DC_{avg}: 99%
KM1/KM2	Contactor with nominal load	B_{10D}: 1,300,000 *1

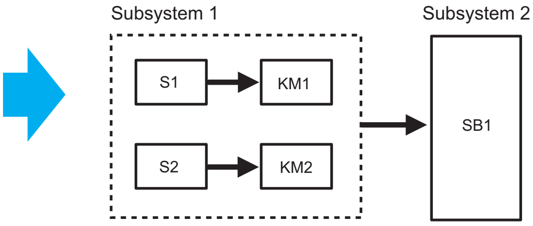
• Developed block diagram

Electrical block diagram of SRP/CS



Developed logical block diagram

Safety function 1



• PL of SRP/CS

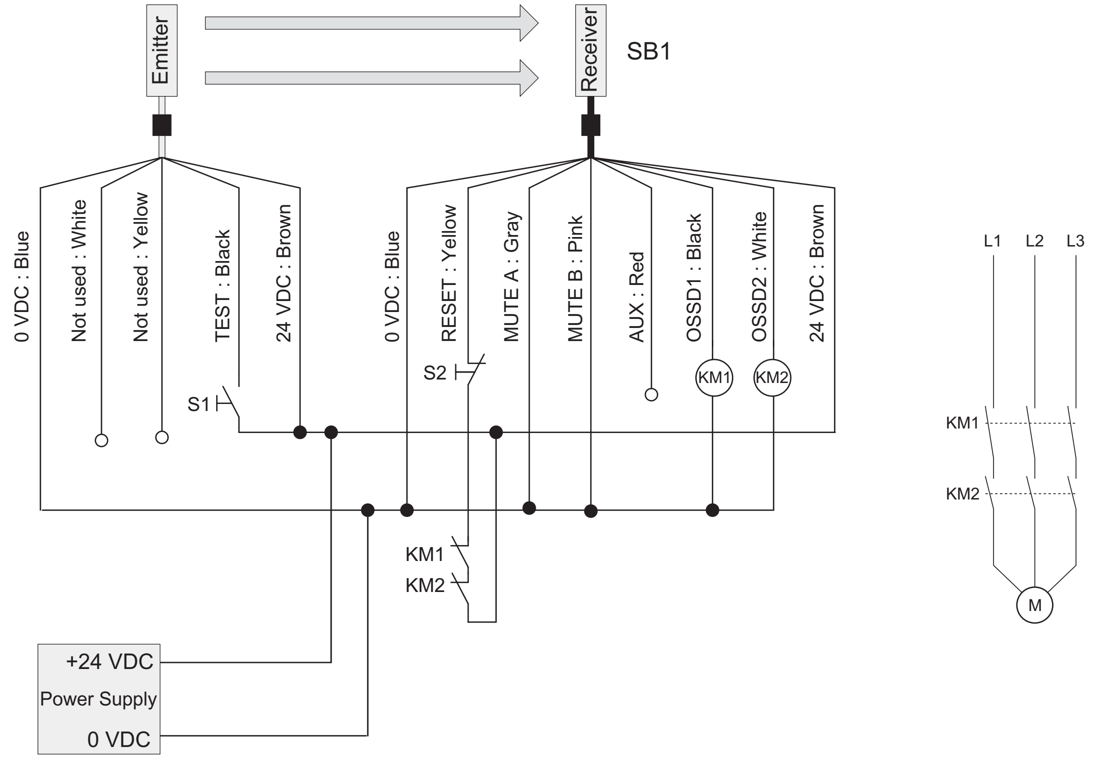
Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	S1	20,000,000	27,500	7,273	99	4	339	99	6.85×10^{-9}	e
		KM1	1,300,000	27,500	473	99					
		S2	1,000,000	27,500	363	99					
		KM2	1,300,000	27,500	473	99					
	2	SB1	PLe certified on ISO 13849-1				4	100	99	2.47×10^{-8}	e
	PFH_D and PL for the SRP/CS									3.16×10^{-8}	e

Note: The point of CCF shall be at least 65.

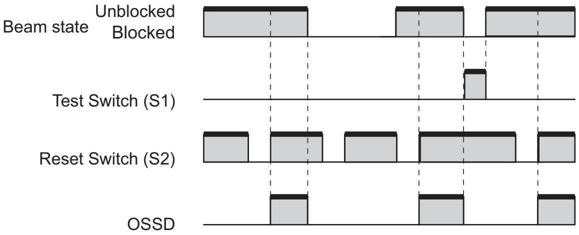
Circuit Example 3: Safety Light Curtain (Stand Alone) with Contactors

• Safety Functions

Safety function	Operation	Stop function	Reset function
1	• Immediately removes power to Motor M when the Safety Light Curtain detects a person entering the area. • The power to Motor M is kept removed until Reset Switch S2 is pressed.	Stop category 0	Manual



• Timing Chart



- Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
S1	Test Switch: General push button switch (NO contact, momentary)	-
S2	Reset Switch: General push button switch (NC contact, momentary)	-
KM1/KM2	Contactor with nominal load	B_{10D}: 1,300,000 [*1]
SB1	Safety Light Curtain: F3SG-4RA (IEC 61496-1 TYPE 4, IEC61508 SIL 3 certified)	Category 4, PFH_D: 1.10 x 10^{-8}

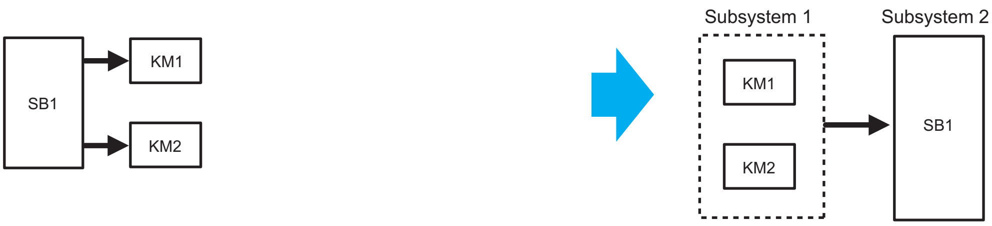
[*1] Source: ISO 13849-1: 2015 Annex C

- Developed block diagram

Electrical block diagram of SRP/CS

Developed logical block diagram

Safety function 1



- PL of SRP/CS

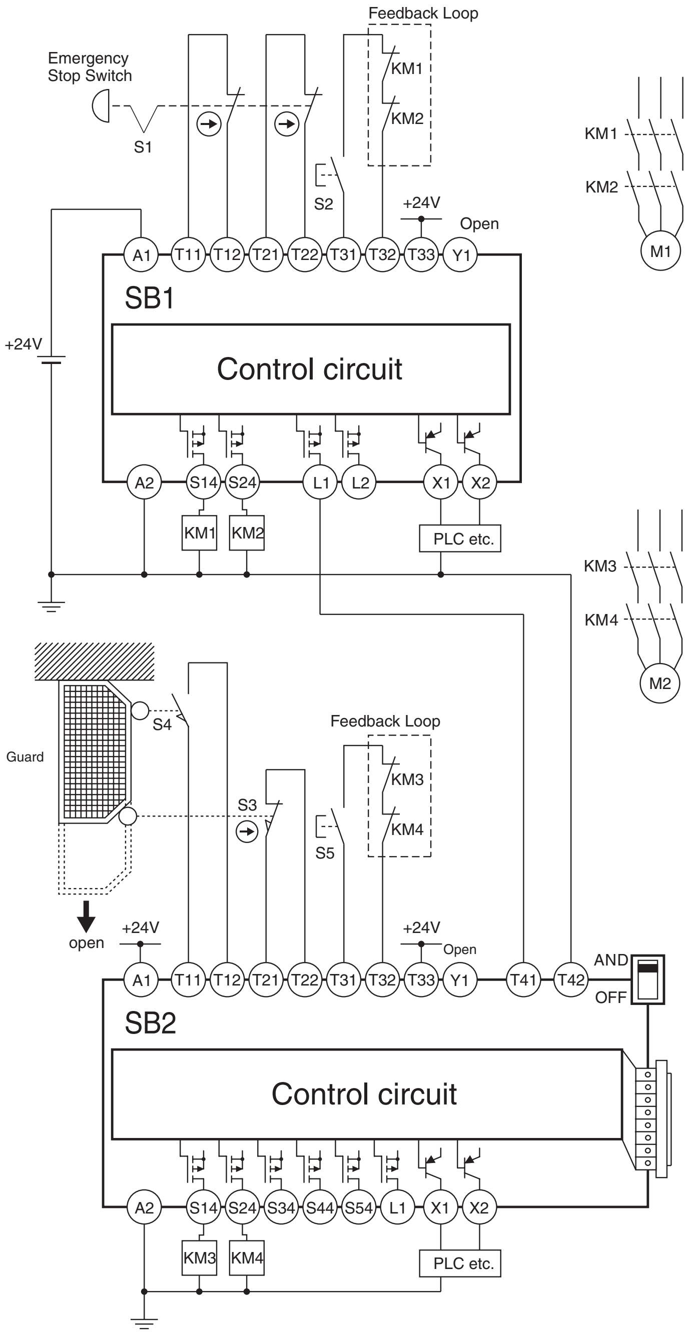
Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	KM1	1,300,000	27,500	473	99	4	473	99	4.89 x 10^{-9}	e
		KM2	1,300,000	27,500	473	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10 x 10^{-8}	e
	PFH_D and PL for the SRP/CS									1.59 x 10^{-8}	e

Note: The point of CCF shall be at least 65.

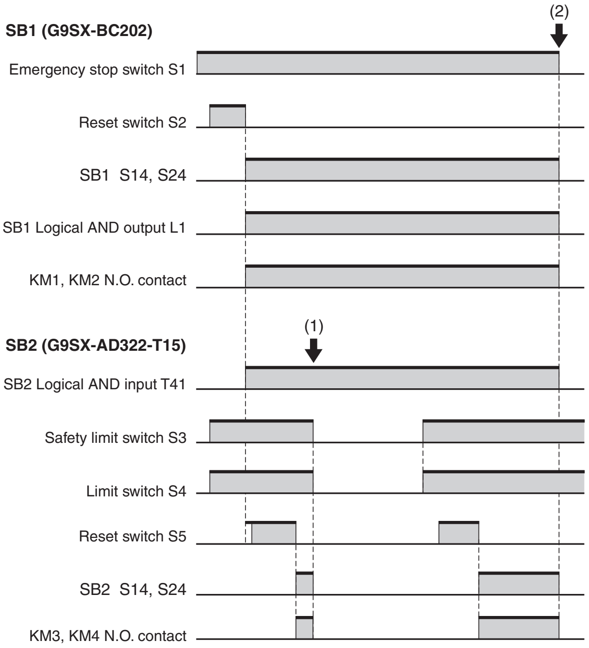
Circuit Example 4: Emergency Stop Switch and Safety Limit Switch Connected to Safety Controllers

• Safety Functions

Safety function	Operation	Stop function	Reset function
1	• The power supply to the motor M1 is turned OFF immediately when the emergency stop switch S1 is pressed. • The power supply to the motor M1 is kept OFF until the emergency stop switch S1 is released and the reset switch S2 is pressed.	Stop category 0	Manual
2	• The power supply to the motor M2 is turned OFF immediately when the emergency stop switch S1 is pressed. • The power supply to the motor M2 is kept OFF until the guard is closed and the reset switch S2 and S5 are pressed while the emergency stop switch is released.	Stop category 0	Manual
3	• During emergency stop switch S1 is not pressed, the power supply to the motor M2 is turned OFF immediately when the limit switch S3 and S4 detect that the guard is opened. • The power supply to the motor M is kept OFF until the reset switch S5 is pressed.	Stop category 0	Manual



• Timing Chart



(1) Guard opened: Only the SB2 stops.

(2) Emergency stop switch pressed: Both the SB1 and SB2 stop.

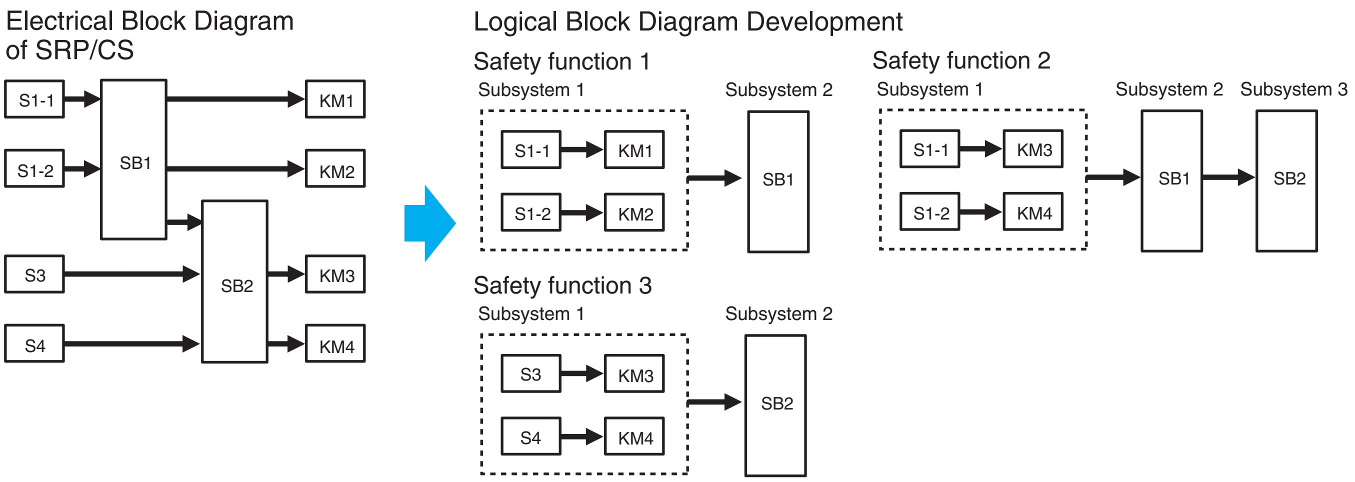
Note: In this example, press reset switch S2, confirm that SB1 has started operating, and then press reset switch S5.

• Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B_{10D}: 100,000
S2/S5	Restart Switch: General push button switch (NO contact, momentary)	-
S3	Safety Limit Switch: D4N-□□20 (NC contact direct mechanical action)	B_{10D}: 20,000,000
S4	General limit switch (NO contact)	B_{10D}: 1,000,000
SB1	Flexible Safety Unit G9SX-BC202 (IEC 61508 SIL3 certified)	Category 4, PFH_D: 4.10×10^{-9}
SB2	Flexible Safety Unit G9SX-AD322-T15 (IEC 61508 SIL3 certified)	Category 4, PFH_D: 5.70×10^{-9}
KM1/KM2 KM3/KM4	Contactor with nominal load	B_{10D}: 1,300,000 [*1]

[*1] Source: ISO 13849-1: 2015 Annex C

• Developed block diagram


Electrical Block Diagram of SRP/CS

Logical Block Diagram Development

• PL of SRP/CS

Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	S1-1	Faults excluded				4	2,500[*1]	99	9.06×10^{-10}[*2]	e
		KM1	1,300,000	500	26,000	99					
		S1-2	Faults excluded								
		KM2	1,300,000	500	26,000	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	4.10×10^{-9}	e
	PFH_D and PL of the SRP/CS									5.01×10^{-9}	e
2	1	S1-1	Faults excluded				4	464	99	4.98×10^{-9}	e
		KM3	1,300,000	28,000[*3]	464	99					
		S1-2	Faults excluded								
		KM4	1,300,000	28,000[*3]	464	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	4.10×10^{-9}	e
	3	SB2	IEC 61508 SIL3 certified				4	-	-	5.70×10^{-9}	e
	PFH_D and PL of the SRP/CS									1.48×10^{-8}	e
3	1	S3	20,000,000	27,500	7,273	99	4	334	99	6.96×10^{-9}	e
		KM3	1,300,000	28,000[*3]	464	99					
		S4	20,000,000	27,500	363	99					
		KM4	1,300,000	28,000[*3]	464	99					
	2	SB2	IEC 61508 SIL3 certified				4	-	-	5.70×10^{-9}	e
	PFH_D and PL of the SRP/CS									1.27×10^{-8}	e

[*1] Applied the upper limit of Category 4 MTTFD or 2,500 years.

[*2] Applied the upper limit of Category 4 DCavg of 99%.

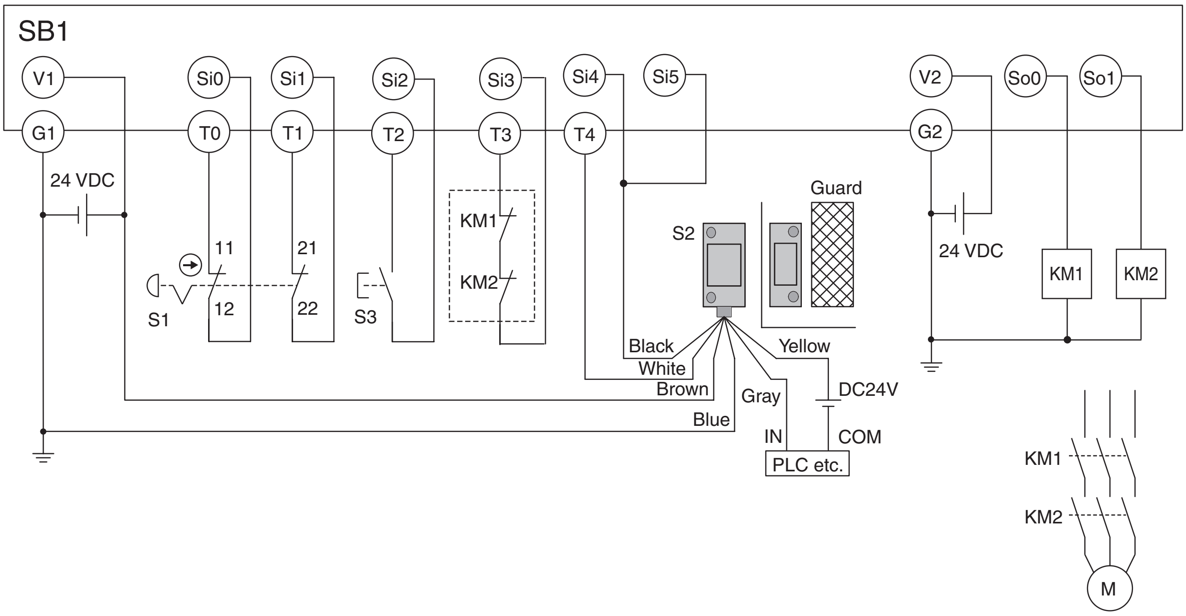
[*3] Overall demands of entire SRP/CS are considered (The total operational demand of the component during operation by the subjected safety function and other safety functions)

Note: The point of CCF shall be at least 65.

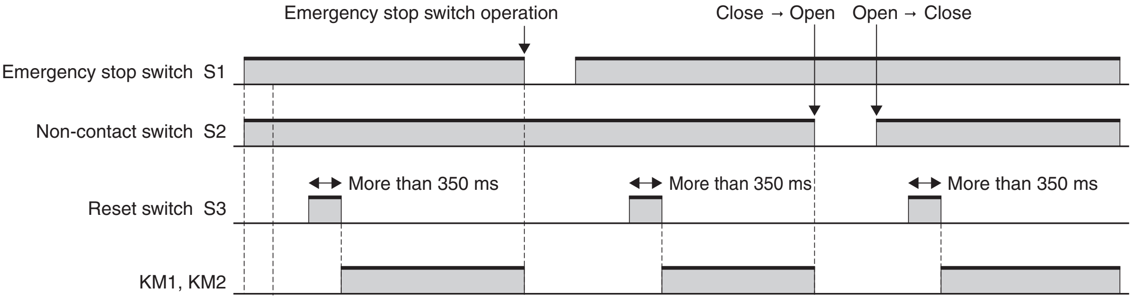
Circuit Example 5: Emergency Stop Switch and Non-contact Door Switch Connected to Safety Controller

- Safety Functions

Safety function	Operation	Stop function	Reset function
1	• The power supply to the motor M is turned OFF immediately when the emergency stop switch S1 is pressed. • The power supply to the motor M is kept OFF until the reset switch S3 is pressed while the guard is closed and the emergency stop switch is released.	Stop category 0	Manual
2	• During emergency stop switch S1 is not pressed, the power supply to the motor M is turned OFF immediately when the non-contact door switch S2 detect that the guard is opened. • The power supply to the motor M is kept OFF until the reset switch S3 is pressed while the guard is closed.	Stop category 0	Manual



- Timing chart



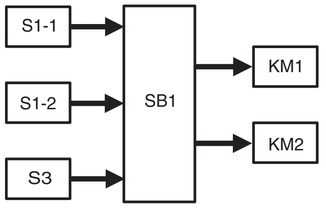
• Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B_{10D}: 100,000
S2	Compact Non-contact Door Switch: D40Z (IEC 61508 SIL3 certified)	Category 4, PFH_D: 1.50×10^{-10}
S3	Restart Switch: General push button switch (NO contact, momentary)	-
SB1	Safety Controller: G9SP-N20S (IEC 61508 SIL3 certified)	Category 4, PFH_D: 1.10×10^{-10}
KM1/KM2	Contactor with nominal load	B_{10D}: 1,300,000 [*1]

[*1] Source: ISO 13849-1: 2015 Annex C

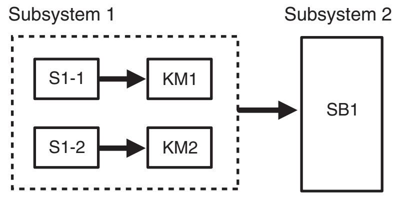
• Developed block diagram

Electrical Block Diagram of SRP/CS

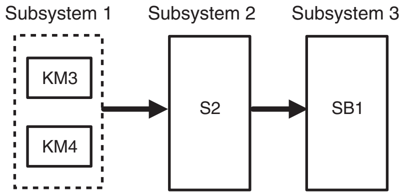


Logical Block Diagram Development

Safety function 1



Safety function 2



• PL of SRP/CS

Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	S1-1	Faults excluded				4	464	99	4.98×10^{-9}	e
		KM1	1,300,000	28,000[*1]	464	99					
		S1-2	Faults excluded								
		KM2	1,300,000	28,000[*1]	464	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	IEC 61508 SIL3 certified									5.09×10^{-9}	e
2	1	KM1	1,300,000	28,000[*1]	464	99	4	464	99	4.98×10^{-9}	e
		KM2	1,300,000	28,000[*1]	464	99					
	2	S2	IEC 61508 SIL3 certified				4	-	-	1.50×10^{-10}	e
	3	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	PFH_D and PL of the SRP/CS									5.24×10^{-9}	e

[*1] Overall demands of entire SRP/CS are considered (The total operational demand of the component during operation by the subjected safety function and other safety functions)

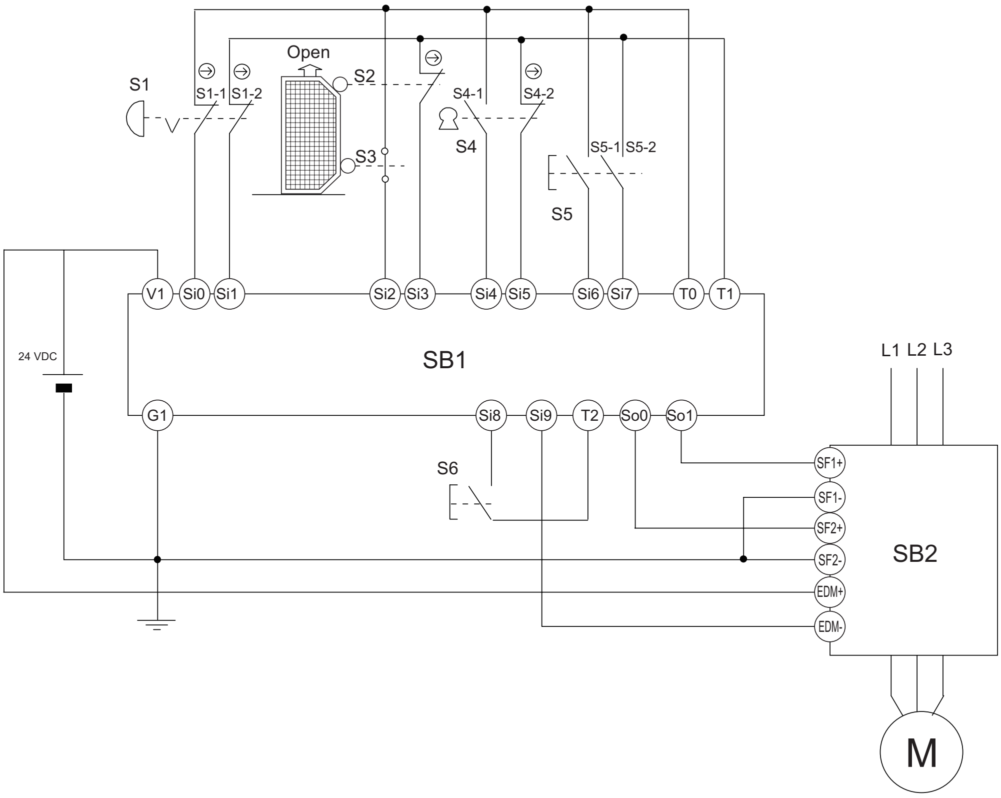
Note: The point of CCF shall be at least 65.

Circuit Example 6: Mode switching and STO Functions

• Safety Functions

Safety function	Operation	Stop function	Reset function
1	• Immediately removes power to Motor M when Emergency Stop Switch S1 is pressed regardless of operation mode. • The power to Motor M is kept removed until the Emergency Stop Switch is released and Reset Switch S6 is pressed.	Stop category 0 (STO*)	Manual
2	• When the Guard is open during scheduled operation, Limit Switch S2 and S3 detects it and the circuit immediately remove power to Motor M. • The power to Motor M is kept removed until the Guard is closed and Reset Switch S6 is pressed.	Stop category 0 (STO*)	Manual
3	• Immediately removes power to Motor M when Enabling Grip S5 is gripped or released during maintenance mode. • The power to Motor M is kept removed until the Enabling Grip is held and Reset Switch S6 is pressed.	Stop category 0 (STO*)	Manual
4	• Mode Selector S4 switches between scheduled operation mode and maintenance mode. • During scheduled operation mode, enable grip switch S4 is disabled. • During maintenance mode, limit switches for guard open/close detection are disabled.	-	-

* Based on the definition of IEC 61800-5-2.

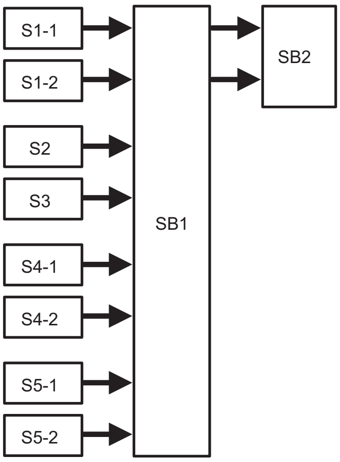


• Model used and machine safety reliability data

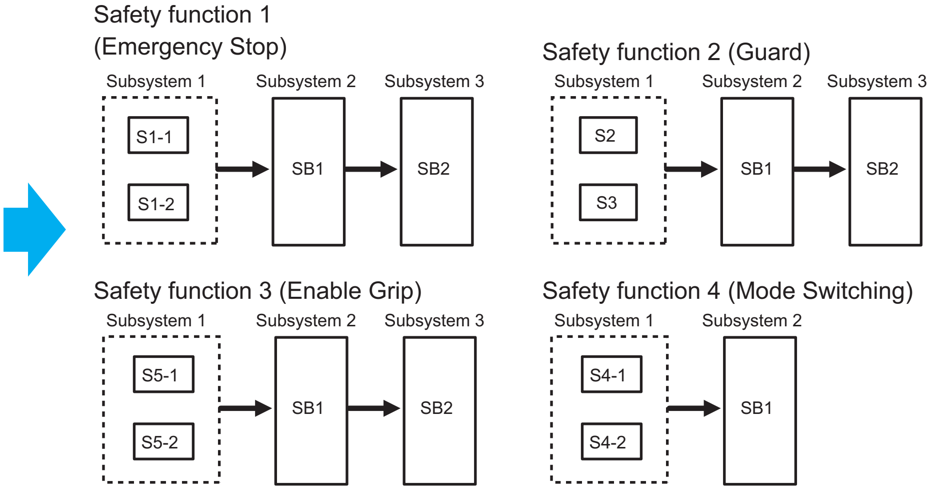
Symbol	Model used	Machinery safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B_{10D}: 100,000
S2	Safety Limit Switch: D4N-□□20 (NC contact direct mechanical action)	B_{10D}: 20,000,000
S3	General limit switch (NO contact)	B_{10D}: 10,000,000
S4-1/S4-2	Mode Selector: A22TK-2□□-11 (1NC/1NO contact)	B_{10D}: 100,000
S5-1/S5-2	Enable Grip Switch: A4EG-C000041 (2NO contact)	B_{10D}: 100,000
S6	Reset Switch: General push button switch (NO contact, momentary)	-
SB1	Safety Controller: G9SP-N20S (IEC 61508 SIL3 certified)	Category 4, PFH_D: 1.10×10^{-10}
SB2	AC Servo Driver G5 Series: R88D-KT/KN (IEC 61508 SIL2 certified)	Category 3, PFH_D: 2.80×10^{-8}

• Developed block diagram

Electrical block diagram of SRP/CS



Developed logical block diagram



• PL of SRP/CS

Safety function	Sub-system	Subsystem parts					Category	$MTTF_D$ (year)	DC_{avg} (%)	PFH_D	PL
			B_{10D} (times)	n_{op} (times/year)	$MTTF_D$ (year)	DC (%)					
1	1	S1-1	Faults excluded				-	-	-	-	-
		S1-2									
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	3	SB2	IEC 61508 SIL2 certified (PLd due to SIL Claim Limit)				3	-	-	2.80×10^{-8}	d
	PFH$_D$ and PL for the SRP/CS									2.82×10^{-8}	d [*2]
2	1	S2	20,000,000	27,500	7,273	99	4	1,698	99	1.34×10^{-9}	e
		S3	1,000,000	27,500	364	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	3	SB2	IEC 61508 SIL2 certified (PLd due to SIL Claim Limit)				3	-	-	2.80×10^{-8}	d
	PFH$_D$ and PL for the SRP/CS									2.95×10^{-8}	d [*2]
3	1	S5-1	100,000	500	2,000	99	4	2,000	99	1.13×10^{-9} [*1]	e
		S5-2	100,000	500	2,000	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	3	SB2	IEC 61508 SIL2 certified (PLd due to SIL Claim Limit)				3	-	-	2.80×10^{-8}	d
	PFH$_D$ and PL for the SRP/CS									2.93×10^{-8}	d [*2]
4	1	S4-1	100,000	500	2,000	99	4	2,000	99	1.13×10^{-9} [*1]	e
		S4-2	100,000	500	2,000	99					
	2	SB1	IEC 61508 SIL3 certified				4	-	-	1.10×10^{-10}	e
	PFH$_D$ and PL for the SRP/CS									1.24×10^{-9}	e

*1. Converted to PFH$_D$ based on Table K.1 of Annex K of ISO 13849-1.
*2. Applied the limit due to PL$_{low}$.

Note: The point of CCF shall be at least 65.

MEMO

ADVANCED GUIDE
Chap. 1
Chap. 2
Chap. 3

3

Chapter 3

Regulations and Standards

1. **Regulations and Standards by Country 72**

(1) Europe 72

(2) The United States of America 76

(3) Canada 78

(4) Japan 79

(5) China 81

(6) South Korea 83

(7) Australia 84

(8) Industry Standards 85

2. **Description of Safety Component-related Standards 86**

(1) Description of Standard 86

(2) Safety component terminology 94

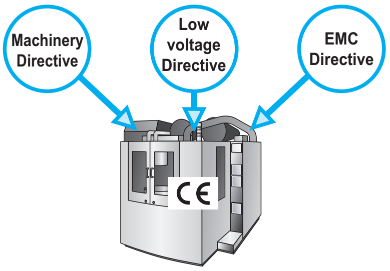
(3) Markings 97

1. Regulations and Standards by Country

(1) Europe

• CE Marking and EU Directives/Regulations

In Europe, there are the rule named CE marking as one of the schemes to achieve free trading among European Economic Area (EEA). CE mark indicates that products meet requirements of Directives/Regulations which are EU legal acts. Manufacturers have to affix CE marking to their products such as electrical devices, industrial machines etc. Products labeled with the CE Marking may be imported and exported to Europe without restriction. The CE Marking is a so-called "passport" to Europe. First of all, manufacturers have to identify the corresponding Directives/Regulations to affix the CE Marking to products. A majority of industrial machines should comply with Low voltage Directive, EMC Directive, and Machinery Directive.



• Low-voltage Directive (LVD)

Low voltage electrical equipment subject to Low Voltage Directive (2014/35/EU) are those that operate at 50 to 1,000 VAC or 75 to 1,500 VDC. The LVD applies to almost all electrical devices from electrical household appliances and office equipment to industrial electrical machinery. The LVD pertains to electrical safety in the Machinery Directive, along with the EMC Directive.

• EMC Directive (EMCD)

The EMC Directive (2014/30/EU) is for products that may generate electromagnetic disturbance or that can be affected by external electromagnetic disturbance. EMC stands for "electromagnetic compatibility." When measures have been taken for both electromagnetic interference (EMI) and electromagnetic susceptibility/immunity (EMS), the device is called electromagnetically compatible, which means that EMC measures have been successfully applied.

• Machinery Directive (MD)

This Directive was issued as the new Machinery Directive 2006/42/EC in 2006, and has been implemented in place of 98/37/EC since 2009.

• Essential Health and Safety Requirements of the Machinery Directive

These basic requirements are listed in Machinery Directive Annex I. The Preliminary Observations of the Machinery Directive explicitly state that the manufacturers can ensure the safety of the products by complying to the essential health and safety requirements.
The Preliminary Observations of the Machinery Directive introduce some aspects of the essential health and safety requirements which can be summarized as shown below.

- The obligations laid down by the essential health and safety requirements apply only when the corresponding hazard exists for the machinery in question when it is used under the conditions foreseen by the manufacturer.
- The essential health and safety requirements laid down in this Directive are mandatory. However, taking into account the state of the art, it may not be possible to meet the objectives set by them. in this case, the machinery must as far as possible be designed and constructed with the purpose of approaching those objectives.

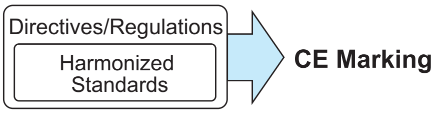
The essential health and safety requirements is consistent with ISO 12100. This standard is good reference for evaluation of machine hazards and safe design based on the evaluation.

• Directives/Regulations and Harmonized Standards

Standards for countries in the European region are unified by CEN and CENELEC. The unified standards are called European Norm (EN) and “EN” is added to the front of the standard numbers. When new EN Standards are established, each country in the region must replace its relevant domestic standard with the EN Standard. In addition to official EN Standards, Drafts of European Standards (prEN), Harmonization Documents (HD), European Pre-standards (ENV), and CEN Reports (CR) are also published. The ISO/IEC standards are used as an EN standard under the WTO/TBT Agreement.

Measures conformed with the Harmonized standard are used for many machines as "presumption of conformity" to the Directives/Regulations. Applicable standards for products intended are not indicated in the individual Directives/Regulations. The list of EN Standards that can apply for each directives/regulations are published separately in the Official Journal of the European Union (OJEU). The EN standards listed in this Official Journal are called "Harmonized standard." Manufacturers are able to comply with directives/regulations by designing based on the EN Standards announced in the OJEU.

• Relation between the Directives/Regulations, EN Standards, and CE Marking



As explained above, all relevant directives/regulations have to be satisfied for a product to be labeled with the CE Marking. While EN Standards as the harmonized standards complement the directives/regulations, satisfying the EN Standards alone, however, does not result in the directives/regulations being satisfied. In addition to product designing and manufacturing based on the requirements by the standards, countermeasures for product liability is mainly required in instructions and catalogs.

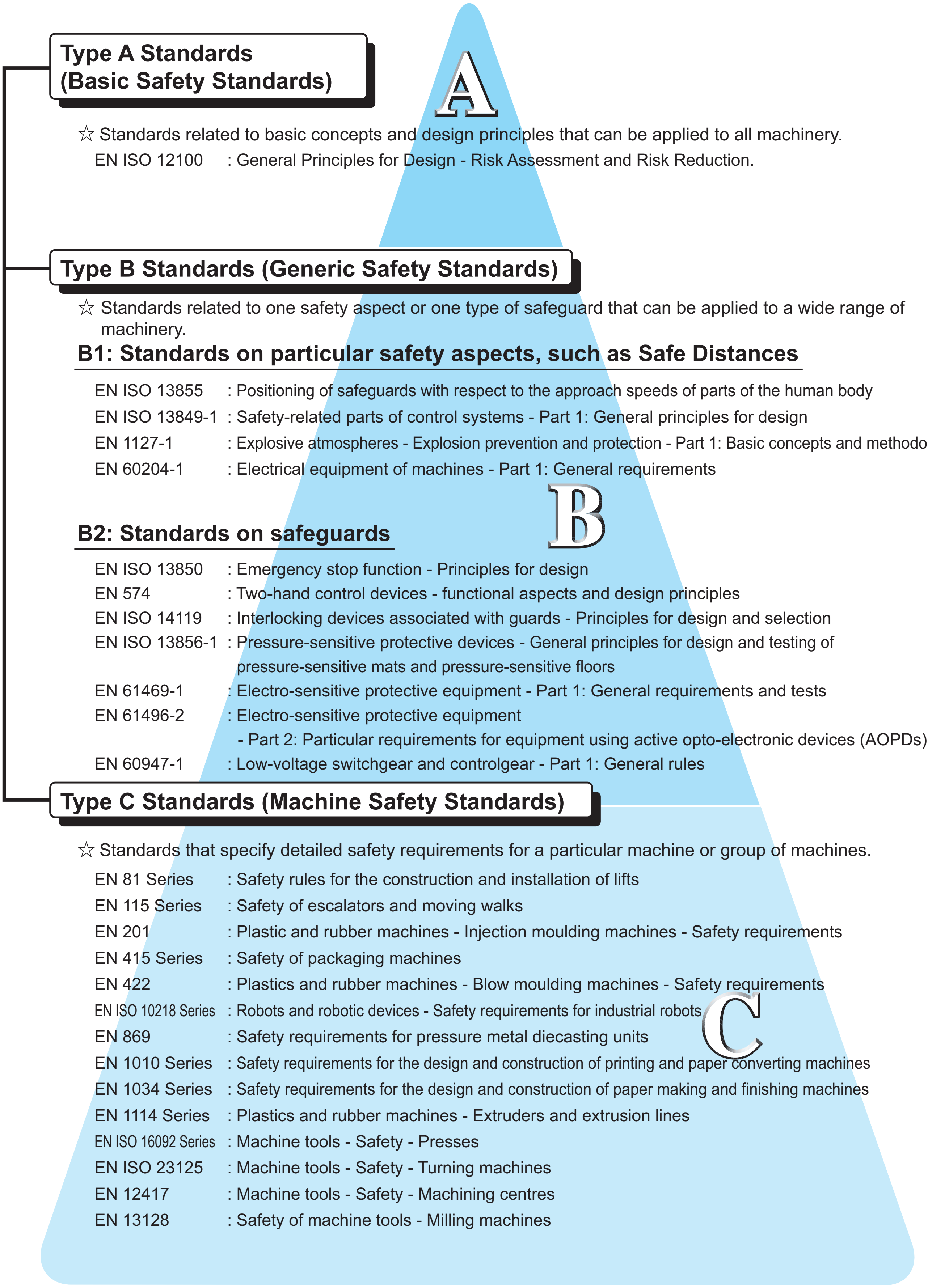
• Product Liability

The General Product Safety Directive (GPSD) and Liability for Defective Products Directive are complementary regulations but their scope is not identical.

The Liability for Defective Products Directive applies to virtually all products, while the GPSD applies only to new, used, and reconditioned products intended for or used by consumers.

Both regulations, however, include areas of uncertainty. Therefore, to be especially careful, a manufacturer must compare the individual provisions of all directives that apply to its product.

- Structure of Major Standards Related to Machinery Safety



Type A Standards (Basic Safety Standards)

☆ Standards related to basic concepts and design principles that can be applied to all machinery.

EN ISO 12100	: General Principles for Design - Risk Assessment and Risk Reduction.

Type B Standards (Generic Safety Standards)

☆ Standards related to one safety aspect or one type of safeguard that can be applied to a wide range of machinery.

B1: Standards on particular safety aspects, such as Safe Distances

EN ISO 13855	: Positioning of safeguards with respect to the approach speeds of parts of the human body
EN ISO 13849-1	: Safety-related parts of control systems - Part 1: General principles for design
EN 1127-1	: Explosive atmospheres - Explosion prevention and protection - Part 1: Basic concepts and methodology
EN 60204-1	: Electrical equipment of machines - Part 1: General requirements

B2: Standards on safeguards

EN ISO 13850	: Emergency stop function - Principles for design
EN 574	: Two-hand control devices - functional aspects and design principles
EN ISO 14119	: Interlocking devices associated with guards - Principles for design and selection
EN ISO 13856-1	: Pressure-sensitive protective devices - General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors
EN 61469-1	: Electro-sensitive protective equipment - Part 1: General requirements and tests
EN 61496-2	: Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic devices (AOPDs)
EN 60947-1	: Low-voltage switchgear and controlgear - Part 1: General rules

Type C Standards (Machine Safety Standards)

☆ Standards that specify detailed safety requirements for a particular machine or group of machines.

EN 81 Series	: Safety rules for the construction and installation of lifts
EN 115 Series	: Safety of escalators and moving walks
EN 201	: Plastic and rubber machines - Injection moulding machines - Safety requirements
EN 415 Series	: Safety of packaging machines
EN 422	: Plastics and rubber machines - Blow moulding machines - Safety requirements
EN ISO 10218 Series	: Robots and robotic devices - Safety requirements for industrial robots
EN 869	: Safety requirements for pressure metal diecasting units
EN 1010 Series	: Safety requirements for the design and construction of printing and paper converting machines
EN 1034 Series	: Safety requirements for the design and construction of paper making and finishing machines
EN 1114 Series	: Plastics and rubber machines - Extruders and extrusion lines
EN ISO 16092 Series	: Machine tools - Safety - Presses
EN ISO 23125	: Machine tools - Safety - Turning machines
EN 12417	: Machine tools - Safety - Machining centres
EN 13128	: Safety of machine tools - Milling machines

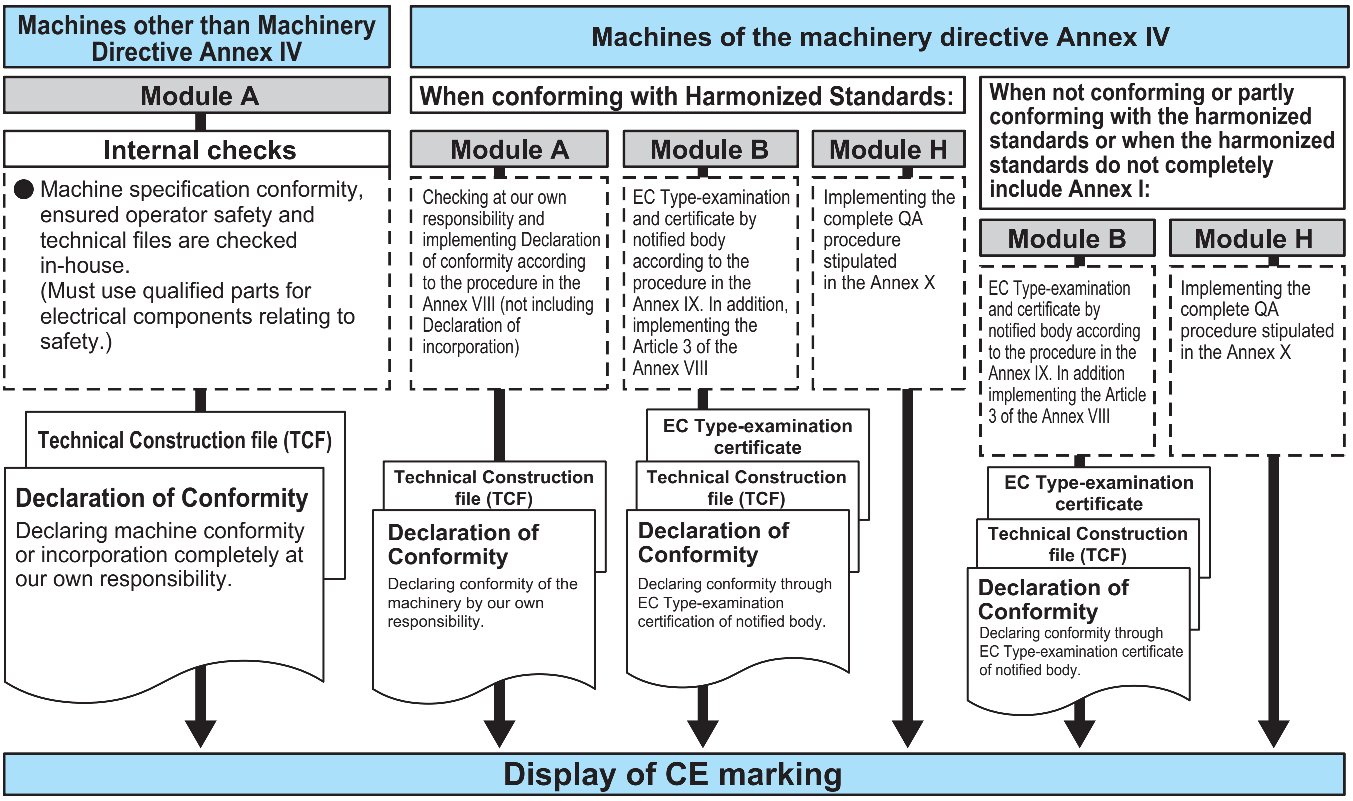
(As of July 2018)

• Main EC Directives for which the CE Marking is mandatory (as of November, 2016)

Directive No.	Directive Name
2006/42/EC	Machinery (MD)
2014/35/EU	Low Voltage (LVD)
2014/30/EU	Electromagnetic compatibility (EMCD)
2014/29/EU	Simple pressure vessels (SPVD)
2014/34/EU	Equipment and protective systems intended for use in Potentially Explosive Atmospheres (ATEX)
2014/68/EU	Pressure Equipment (PED)
2016/425	Personal Protective Equipment (PPER)
2014/33/EU	Lifts (LD)
2014/53/EU	Radio equipment (RED)
2014/32/EU	Measuring instruments (MID)
2009/48/EC	Safety of toys

Directive No.	Directive Name
2016/426	Appliances burning gaseous fuels (GAR)
2016/424	Cableway installations designed to carry persons
2011/65/EU	Restriction of Hazardous Substances in electrical and electronic equipment (RoHS2)
2014/28/EU	Explosive for Civil uses
90/385/EEC	Active implantable medical devices (AIMD)
93/42/EEC	Medical devices (MDD)
98/79/EC	In vitro diagnostic medical devices (IVDMDD)
92/42/EEC	Hot-water boilers
2014/31/EU	Non-automatic weighing instruments (NAWID)
2009/125/EC	Ecodesign of energy related products
2013/53/EU	Recreational craft and personal watercraft

• Example of conformity assessment based on machinery directive



Machines other than Machinery Directive Annex IV

Module A

Internal checks

● Machine specification conformity, ensured operator safety and technical files are checked in-house.
(Must use qualified parts for electrical components relating to safety.)

Technical Construction file (TCF)

Declaration of Conformity
Declaring machine conformity or incorporation completely at our own responsibility.

Machines of the machinery directive Annex IV

When conforming with Harmonized Standards:

Module A

Checking at our own responsibility and implementing Declaration of conformity according to the procedure in the Annex VIII (not including Declaration of incorporation)

Technical Construction file (TCF)

Declaration of Conformity
Declaring conformity of the machinery by our own responsibility.

Module B

EC Type-examination and certificate by notified body according to the procedure in the Annex IX. In addition, implementing the Article 3 of the Annex VIII

EC Type-examination certificate

Technical Construction file (TCF)

Declaration of Conformity
Declaring conformity through EC Type-examination certification of notified body.

Module H

Implementing the complete QA procedure stipulated in the Annex X

When not conforming or partly conforming with the harmonized standards or when the harmonized standards do not completely include Annex I:

Module B

EC Type-examination and certificate by notified body according to the procedure in the Annex IX. In addition implementing the Article 3 of the Annex VIII

EC Type-examination certificate

Technical Construction file (TCF)

Declaration of Conformity
Declaring conformity through EC Type-examination certificate of notified body.

Module H

Implementing the complete QA procedure stipulated in the Annex X

Display of CE marking

• Machinery requiring EC Type-examination by a notified body (Machinery Directive Annex IV)

(1) Circular saw machines for cutting wood, meat and analogous material (Single blades/multi-blade)
(2) Hand-fed surface planing machines for woodworking
(3) Thicknessers for one-side dressing with manual loading and/or unloading for woodworking
(4) Band saw machines for cutting wood, meat and analogous material
(5) Combined machines of the types referred to in (1) to (4) and (7)
(6) Hand-fed Tenoning machines
(7) Hand-fed vertical spindle moulding machines for working with wood and analogous materials.
(8) Portable chainsaws for woodworking
(9) Presses (Have a travel exceeding 6 mm and a speed exceeding 30 mm/s)
(10) Injection or compression plastics-moulding machines
(11) Injection or compression rubber-moulding machines
(12) Machines for underground working
(13) Manually-loaded trucks for the collection of household refuse incorporating a compression mechanism
(14) Transmissions
(15) Guard for transmissions
(16) Vehicles servicing lifts
(17) Lifting device
(18) Portable impact machine
(19) Protective device for human body detection
(20) Power interlock guard used as a protective measure of the machines (9), (10), and (11)
(21) Logic units for safety functions
(22) Roll-over protection structures
(23) Falling-object protective structures

(2) The United States of America

• Occupational Safety and Health Administration (OSHA)

The Occupational Safety and Health Act (OSH Act) passed in 1970 to provide safe and healthy working conditions. Title 29 of Code of Federal Regulations (29CFR) gives specific standards.
Subpart O of Part 1910 sets standards for machinery and machine guarding, and divides into Part1910.211 to Part 1910.219.

Standard No.	Title
1910.211	Definition
1910.212	General requirements for all machines
1910.213	Woodworking machinery requirements
1910.214	Cooperage machinery
1910.215	Abrasive wheel machinery
1910.216	Mills and calendars in the rubber and plastic industries
1910.217	Mechanical power presses
1910.218	Forging machines
1910.219	Mechanical power-transmission apparatus

Part1910.212 covers general requirements for all machines. The main points in Part1910.212 are given below.

Paragraph (a)(1)

One or more methods of machine guarding shall be provided to protect the operator and other employees in the machine area from hazards such as those created by point of operation, ingoing nip points, rotating parts, flying chips, and sparks. Examples of guarding methods are barrier guards, two-hand tripping devices, electronic safety devices, etc.

Paragraph (a)(3)(ii)

The point of operation of machines whose operation exposes an employee to injury shall be guarded. The guarding device shall be in conformity with any appropriate standards, therefore, or, in the absence of applicable specific standards, shall be so designed and constructed as to prevent the operator from having any part of his body in the danger zone during the operating cycle.

• American National Standards Institute (ANSI)

ANSI is an independent standards organization in the USA. It does not create any standards by itself, but rather approves and registers US standards created in various fields.

UL (Underwriters Laboratories) which was established by the fire insurance industry have published various product standards as a Standards Developing Organization(SDO). ASME (American Society of Mechanical Engineers) is also one of the famous SDOs for many years.
For particular machinery, there are a lot of important ANSI standards, such as ANSI B11 series for machine tools, ANSI RIA standards for industrial robots and robot systems, etc.

1. Safety of Machine Tools

ANSI B11 series consists of over 20 documents dealing with mainly machine tool safety. They specify requirements for both the manufacturers and users of the machines.

Major ANSI B11 series

Standard No.	Title
ANSI B11.1	Mechanical power presses
ANSI B11.2	Hydraulic and pneumatic power presses
ANSI B11.3	Power press brakes
ANSI B11.4	Shears
ANSI B11.5	Ironworkers
ANSI B11.6	Manual turning machines with or without automatic control
ANSI B11.7	Cold headers and cold formers
ANSI B11.8	Manual milling, drilling and boring machines with or without automatic control
ANSI B11.9	Grinding machines
ANSI B11.10	Metal sawing machines
ANSI B11.11	Gear and spline cutting machines
ANSI B11.12	Roll forming and roll bending machines
ANSI B11.13	Single and multiple spindle automatic screw/bar and chucking machines

(As of July 2018)

Standard No.	Title
ANSI B11.15	Pipe tube and shape bending machines
ANSI B11.16	Powder/metal compacting presses
ANSI B11.17	Horizontal hydraulic extrusion presses
ANSI B11.18	Machines processing or slitting coiled or non-coiled metal
ANSI B11.19	Performance criteria for safeguarding
ANSI B11.20	Integrated manufacturing systems
ANSI B11.21	Machine tools using a laser for processing materials
ANSI B11.22	Turning centers and automatic, numerically controlled turning machines
ANSI B11.23	Machining centers and automatic, numerically controlled milling, drilling and boring machines
ANSI B11.24	Transfer machines

(As of July 2018)

ANSI B11.19 specify requirements of safeguards referred by the other B11 standards.

2. Safety of Industrial Robots

ANSI/RIA R15.06 as the standards for industrial robots is the base of ISO 10218 series, stipulating both ISO 10218-1 which defines requirements for industrial robots themselves and ISO 10218-2 which defines requirements for robot systems using industrial robots. The standard indicates the specific safe design guideline and provides lists of typical hazards and validity check after design to be checked on risk assessment of industrial robots and robot systems, allowing utilization in series of considerations for deployment of industrial robots.

• National Fire Protection Association (NFPA)

NFPA which was established for protection against and prevention from fire has published national codes and standards. Major standards related to electrical design of machinery are as follows;

Standard No.	Title
NFPA 70	National Electrical Code (NEC)
NFPA 79	Electrical standard for Industrial machinery

(3) Canada

• CSA

Safety standards created by Canadian Standards Association are called CSA standards, which are mainly for electrical equipment, medical devices, machines, and instruments.
Electrical equipment and appliances that are connected to power source to use in Canada must retain electrical safety based on the CSA standards regardless of the types and/or quantity.

Major standards applying to machinery

Standard No.	Title
CSA Z431	Basic and Safety Principles for Man-Machine Interface, Marking and Identification-Coding Principles for Indicators and Actuators.
CSA Z432	Safeguarding of Machinery
CSA Z434	Industrial Robots and Robot Systems

• Pre-Start Health And Safety Reviews (PSR)

Ontario has original provincial law for safety and health, "Occupational Health and Safety Act R.R.O.1990, REGULATION 851". It includes implementation provisions of PSR review by professional technicians for new machine installation.

(4) Japan

• Industrial Safety and Health Act

It is a law established for the purpose of securing the safety and health of workers in the workplace and forming a comfortable working environment. From the revision in 2006, it has required investigation of dangers and hazards as well as implementation of countermeasures. It is a framework to identify dangers and hazards in the workplace, evaluate respective risks, and implement measures to reduce these risks based on the evaluation, which is similar to implementation of risk assessment and risk reduction measures in ISO 12100 (JIS B 9700).

• Ordinance on Industrial Safety and Health

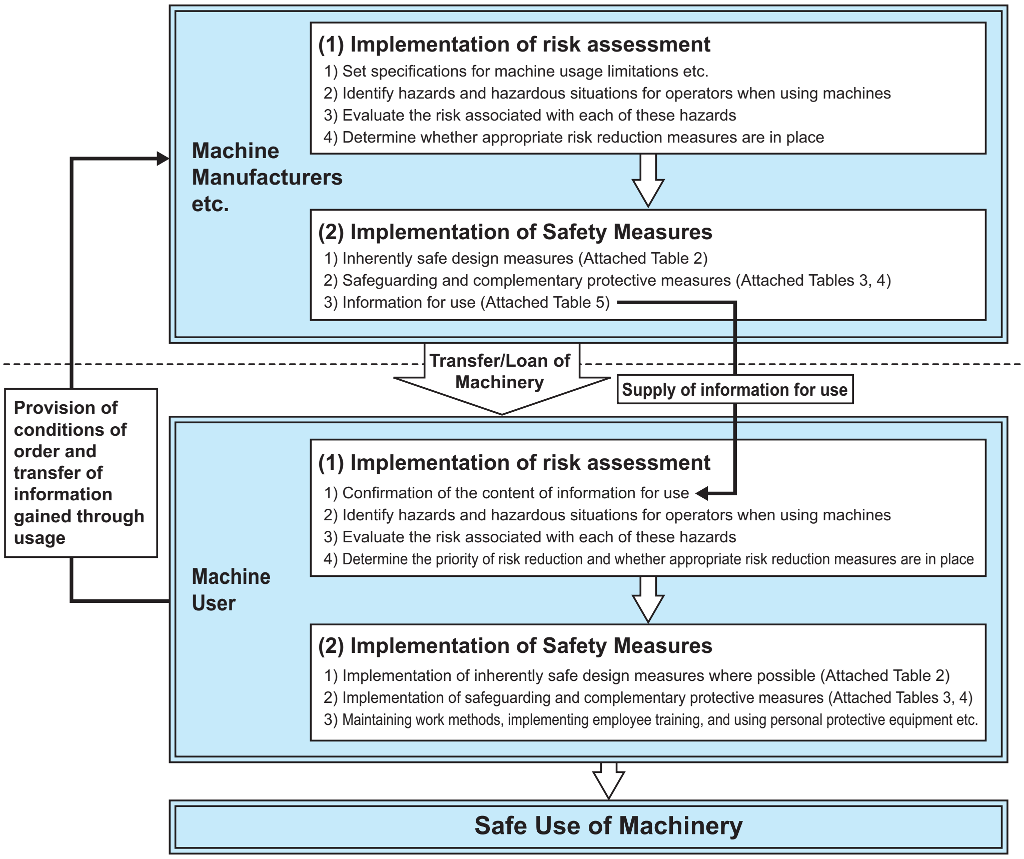
Individual hazard prevention standards are stipulated for machine tool, woodworking machine, food processing machine, press and shearing machine, centrifugal machine, crushing and mixing machine, rolling mills, high speed rotating body, and industrial robots. Also general standards are stipulated for all types of machines. One of the articles revised in October 2013, requires that all the machines should stop during adjustment works, for example when clogging occurs.

• Guidelines for Comprehensive Safety Standards of machinery

In July 2007, the Ministry of Health, Labor and Welfare in Japan amended its Guidelines for Comprehensive safety Standards of Machinery, which was originally issued in June 2001 in response to the basic safety standards provided in ISO 12100. These Guidelines stipulate the procedure for manufacturers about risk reduction and design that take safety into consideration in the manufacture of production equipment and machinery. It is also required operational safety measures of users when they introduce and use the equipment and machinery. In general, the measures that ensure safety in machinery include measures that manufacturers build-in at the design stage and measures that users must take when using the machinery. However, the Guidelines also clarify the fact that the measures that manufacturers build-in at the design stage must naturally precede the measures taken by the users.

The following diagram shows the flow of achieving machinery safety based on the Guidelines for Comprehensive Safety Standard of machinery.

Safety Procedure for Machinery


Machine Manufacturers etc.
(1) Implementation of risk assessment
1) Set specifications for machine usage limitations etc.
2) Identify hazards and hazardous situations for operators when using machines
3) Evaluate the risk associated with each of these hazards
4) Determine whether appropriate risk reduction measures are in place
(2) Implementation of Safety Measures
1) Inherently safe design measures (Attached Table 2)
2) Safeguarding and complementary protective measures (Attached Tables 3, 4)
3) Information for use (Attached Table 5)
Transfer/Loan of Machinery
Supply of information for use
Provision of conditions of order and transfer of information gained through usage
Machine User
(1) Implementation of risk assessment
1) Confirmation of the content of information for use
2) Identify hazards and hazardous situations for operators when using machines
3) Evaluate the risk associated with each of these hazards
4) Determine the priority of risk reduction and whether appropriate risk reduction measures are in place
(2) Implementation of Safety Measures
1) Implementation of inherently safe design measures where possible (Attached Table 2)
2) Implementation of safeguarding and complementary protective measures (Attached Tables 3, 4)
3) Maintaining work methods, implementing employee training, and using personal protective equipment etc.
Safe Use of Machinery

• JIS

The regulations and standards of individual countries should be brought in line with international standards to remove trade barriers and thus ensure free trade worldwide. To that end, Japan accepted the terms of the World Trade Organization (WTO), becoming a member and signatory to the WTO Agreement as well as the TBT Agreement (Technical Barrier Treatment). In 1995, Japan declared its commitment to a system of global cooperation. Due to mandatory adoption of international standards, Japanese Industrial Standards (JIS) were enacted under the Industrial Standardization Law, to bring them in line with the ISO and IEC standards.

JIS Standards		International Standards
B 9700: 2013	Safety of machinery - General principles for design - Risk assessment and risk reduction	ISO 12100: 2010
B 9703: 2011	Safety of machinery -- Emergency stop -- Principles for design	ISO 13850: 2006
B 9705-1: 2011	Safety of machinery -- Safety-related parts of control systems - Part 1: General principles for design	ISO 13849-1: 2006
B 9709-1: 2001	Safety of machinery -- Reduction of risks to health from hazardous substances emitted by machinery - Part 1: Principles and specifications for machinery manufacturers	ISO 14123-1: 1998
B 9709-2: 2001	Safety of machinery -- Reduction of risks to health from hazardous substances emitted by machinery - Part 2: Methodology leading to verification procedures	ISO 14123-2: 1998
B 9710: 2006	Safety of machinery -- Interlocking devices associated with guards -- Principles for design and selection	ISO 14119: 1998
B 9711: 2002	Safety of machinery -- Minimum gaps to avoid crushing of parts of the human body	ISO 13854: 1996
B 9712: 2006	Safety of machinery -- Two-hand control devices -- Functional aspects and design principles	ISO 13851: 2002
B 9713-1: 2004	Safety of machinery -- Permanent means of access to machinery - Part 1: Choice of a fixed means of access between two levels	ISO 14122-1: 2001
B 9713-2: 2004	Safety of machinery -- Permanent means of access to machinery - Part 2: Working platforms and walkways	ISO 14122-2: 2001
B 9713-3: 2004	Safety of machinery -- Permanent means of access to machinery - Part 3: Stairs, stepladders and guard-rails	ISO 14122-3: 2001
B 9713-4: 2004	Safety of machinery -- Permanent means of access to machinery - Part 4: Fixed ladders	ISO/FDIS 14122-4: 2000
B 9714: 2006	Safety of machinery -- Prevention of unexpected start-up	ISO 14118: 2000
B 9715: 2013	Safety of machinery -- Positioning of safeguards with respect to the approach speeds of parts of the human body	ISO 13855: 2010
B 9716: 2006	Safety of machinery -- Positioning of protective equipment with respect the approach of parts of the human body	ISO 14120: 2002
B 9718: 2013	Safety of machinery -- Safety distances to prevent hazard zones being reached by the upper and lower limbs	ISO 13857: 2008
B 9960-1: 2008 /A1: 2011	Safety of machinery -- Electrical equipment of machines - Part 1: General requirements	IEC 60204-1: 2005/A1: 2008
B 9961: 2015	Safety of machinery -- Functional safety of safety-related electrical, electronic and programmable electronic control systems	IEC 62061: 2005/A1: 2011/ A2: 2015
B 9704-1: 2015	Safety of machinery -- Electro-sensitive protective equipment - Part 1: General requirements and tests	IEC 61496-1: 2012
B 9704-2: 2017	Safety of machinery -- Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)	IEC61496-2: 2013
B 9704-3: 2011	Safety of Machinery -- Electro-Sensitive Protective Equipment - Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR).	IEC 61496-3: 2008
B 9706-1: 2009	Safety of machinery -- Indication, marking and actuation - Part 1: Requirements for visual, acoustic and tactile signals.	IEC 61310-1: 2007
B 9706-2: 2009	Safety of machinery -- Indication, marking and actuation - Part 2: Requirements for marking	IEC 61310-2: 2007
B 9706-3: 2009	Safety of machinery -- Indication, marking and actuation - Part 3: Requirements for the location and operation of actuators	IEC 61310-3: 2007
C 0508-1: 2012	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	IEC 61508-1: 2010
C 0508-2: 2014	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	IEC 61508-2: 2010
C 0508-3: 2014	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	IEC 61508-3: 2010
C 0508-4: 2012	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	IEC 61508-4: 2010
C 0508-5: 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels	IEC/FDIS 61508-5: 1998
C 0508-6: 2000	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of parts 2 and 3	IEC/CDV 61508-6: 1998
C 0508-7: 2017	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures	IEC 61508-7: 2010

(As of July 2018)

(5) China

- GB

Chinese national standards (GB: Guojia Biaozhun)

GB as the Chinese National Standards are defined based on the ISO and IEC standards. There are two standard types, GB and GB/T.

Structure of National Standards

	Standard	Administrator
GB	Mandatory National Standards	Standardization Administration of the People’s Republic of China
GB/T	Voluntary National Standards	Standardization Administration of the People’s Republic of China

Examples of GB standards related to safety of machinery

Mandatory National Standards (GB: Guojia Biaozhun)		International Standards
GB 5226.1	Safety of Machinery -- Electrical equipment of machines - Part 1: General requirements	IEC 60204-1
GB 28526	Safety of Machinery -- Functional safety of safety-related electrical, electronic and programmable electronic control systems	IEC 62061

Examples of GB/T standards related to safety of machinery

Voluntary National Standards (GB/T: Guojia Biaozhun/ Tuijian)		International Standards
GB/T 12265.3	Safety of machinery -- Minimum gaps to avoid crushing of parts of the human body	ISO 13854
GB/T 15706	Safety of machinery -- General principles for design - Risk assessment and risk Reduction	ISO 12100
GB/T 16754	Safety of machinery -- Emergency stop -- Principles for design	ISO 13850
GB/T 16855.1	Safety of machinery -- Safety-related parts of control systems - Part 1 : General principles for design	ISO 13849-1
GB/T 16855.2	Safety of machinery -- Safety-related parts of control systems - Part 2 : Validation	ISO 13849-2
GB/T 17888.1, 2, 3, 4	Safety of machinery -- Permanent means of access to machinery	ISO 14122-1, 2, 3, 4
GB/T 18209.1, 2, 3	Safety of machinery -- Indication, marking and actuation	IEC 61310-1, 2, 3
GB/T 18831	Safety of machinery -- Interlocking devices associated with guards - Principles for design and selection	ISO 14119
GB/T 19436.1	Safety of machinery -- Electro-sensitive protective equipment - Part 1 : General requirements and tests	IEC 61496-1
GB/T 19436.2	Safety of Machinery -- Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices	IEC 61496-2
GB/T 19876	Safety of machinery -- Positioning of safeguards with respect to the approach speeds of parts of the human body	ISO 13855
GB/T 20438. 1, 2, 3, 4, 5, 6, 7	Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC 61508-1, 2, 3, 4, 5, 6, 7
GB/T 23821	Safety of machinery -- Safety distances to prevent hazard zones being reached by the upper and lower limbs	ISO 13857

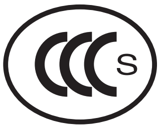
(As of July 2018)

• CCC

CCC: China Compulsory Certification mark system

Upon its entry into the WTO in 2001, China integrated its former Product Safety Certification System for Imported Items (CCIB mark) and Product Safety Certification System for Items Distributed within China (CCEE mark), and issued the China Compulsory Product Certification System (Abbreviated name: CCC mark) on December 3, 2001, which took effect on May 1, 2002.
On August 1, 2003 it became prohibited to sell, import, or use products of the items subject to the compulsory certification system that do not meet either of the following conditions: having a certificate from the specified verification organization and displaying China Compulsory Certification mark (CCC mark).
The number of products subject to the compulsory certification system is increased gradually after the first publication in 2003. You can view the detailed item list in the Certification and Accreditation Administration of the People's Republic of China web page (http://www.cnca.gov.cn/cnca/).
Products manufactured and certificated outside China must display the China Compulsory Certification mark (CCC mark) before being imported to China, while products manufactured and certificated within China must display it when being shipped from the factory.
For details of CCC-certificated models, refer to each catalog or contact an OMRON sales representative.

Examples of the standards for CCC certification related to electric wires and cables



CCC mark

Electric circuit switches, electronic equipment for protection or connection use

GB	International Standards
GB/T 14048.2	IEC 60947-2
GB/T 14048.3	IEC 60947-3
GB/T 14048.4	IEC 60947-4-1
GB/T 14048.5	IEC 60947-5-1
GB/T 14048.10	IEC 60947-5-2

Low-voltage electrical equipment

GB	International Standards
GB/T 14048.5	IEC 60947-5-1
GB/T 14048.6	IEC 60947-4-2

(6) South Korea

• KS

South Korea also bring Korean Industrial standards(KS) in line with ISO and IEC standards as a member country of the WTO/TBT Agreement.

• KCs Marking System

Occupational Safety and Health Act, Article 34 requires safety certification for harmful or hazardous machines, devices, and equipment.
Also the Article 35 in force since March 1, 2013 stipulates the Self-regulatory Safety Certification System. Manufacturers of products subject to this system are required to confirm conformity and submit conformed document. The items subject to the Self-regulatory Safety Certification System are as follows; high-risk machines, protective devices (including explosion-proof devices) and personal protective equipments (PPE).
Products that obtain a safety certification and products whose Self-regulatory Safety Certification System document is accepted must display a KCs mark.

• S-mark

The S-mark is a voluntary certification system established in November 1997 by the Korea Occupational Safety and Health Agency (KOSHA) to reduce the occurrence of work-related accidents. The S-mark is granted for products that have been examined by KOSHA and are deemed to satisfy standards based on the Occupational Safety and Health Act, Article 34, item 2, for product safety, product reliability, and the quality control capabilities of the manufacturer. The requirements are divided into Safety and EMC. Products that obtain an S-mark certification are not required to submit Self-regulatory Safety Certification System document, even if they are also subject to the Safety Certification System.
In the case of OMRON, safety components have been certified for both safety and EMC, and basic sensors have received EMC certification.
For details of certified models, refer to each catalog or contact an OMRON sales representative.

(7) Australia

• AS (Australian standard)

In Australia, Standards Australia has published AS standards. AS 4024.1 series is used as the safety standards applied to machinery. These standard series were revised by adopting ISO, IEC and EN standards in 2014. Most of them are identical with New Zealand standards and stipulated as AS/NZS.

Standards included in AS 4024.1-2014 series "Safety of machinery"

Classification	Standard No.	Title	Adopted standards
Application guide	AS/NZS 4024.1100	Application guide	—
General principles for design	AS/NZS 4024.1201	General principles for design - Risk assessment and risk reduction	ISO 12100
Risk assessment	AS/NZS 4024.1302	Risk assessment - Reduction of risks to health from hazardous substances emitted by machinery - Principles and specifications for machinery manufacturers	—
	AS/NZS 4024.1303	Risk assessment - Practical guidance and examples of methods	ISO/TR 14121-2
Ergonomic principles	AS/NZS 4024.1401	Ergonomic principles - Design principles - Terminology and general principles	—
Safety related parts of control systems	AS 4024.1501	Design of safety related parts of control systems - General principles for design	—
	AS 4024.1502	Design of safety related parts of control systems - Validation	—
	AS/NZS 4024.1503	Safety-related parts of control systems - General principles for design	ISO 13849-1
Interlocks/interlocking devices, guards	AS/NZS 4024.1601	Design of controls, interlocks and guarding - Guards - General requirements for the design and construction of fixed and movable guards	EN 953
	AS/NZS 4024.1602	Interlocking devices associated with guards - Principles for design and selection	ISO 14119
	AS 4024.1603	Design of controls, interlocks and guardings - Prevention of unexpected start-up	—
	AS/NZS 4024.1604	Design of controls, interlocks and guarding - Emergency stop - Principles for design	ISO 13850
Human body measurements	AS/NZS 4024.1701	Human body measurements - Basic human body measurements for technological design	ISO 7250-1
	AS/NZS 4024.1702	Human body measurements - Principles for determining the dimensions required for openings for whole body access into machinery	EN 547-1
	AS/NZS 4024.1703	Human body measurements - Principles for determining the dimensions required for openings for access openings	EN 547-2
	AS/NZS 4024.1704	Human body measurements - Anthropometric data	EN 547-3
Safety distances	AS/NZS 4024.1801	Safety distances to prevent danger zones being reached by upper and lower limbs	ISO 13857
	AS/NZS 4024.1803	Safety distances and safety gaps - Minimum gaps to prevent crushing of parts of the human body	ISO 13854
Displays, controls, actuators and signals	AS/NZS 4024.1901	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	EN 894-1
	AS/NZS 4024.1902	Displays, controls, actuators and signals - Ergonomic requirements for the design of displays and control actuators - Displays	—
	AS/NZS 4024.1903	Displays, controls, actuators and signals - Ergonomic requirements for the design of displays and control actuators - Control actuators	—
	AS/NZS 4024.1904	Displays, controls, actuators and signals - Indication, marking and actuation - Requirements for visual, auditory and tactile signals	IEC 61310-1
	AS/NZS 4024.1905	Displays, controls, actuators and signals - Indication, marking and actuation - Requirements for visual, auditory and tactile signals	IEC 61310-2
	AS/NZS 4024.1906	Displays, controls, actuators and signals - Indication, marking and actuation - Requirements for the location and operation of actuators	IEC 61310-3
	AS/NZS 4024.1907	Displays, controls, actuators and signals - System of auditory and visual danger and information signals	—

(As of July 2018)

(8) Industry Standards

• Semiconductor Manufacturing Equipment Guideline SEMI Standards

SEMI, which is an abbreviation of Semiconductor Equipment and Materials International, was established in 1970 as an international industry association for semiconductor manufacturing equipment and materials manufacturers. SEMI standards have been established as independent industry standards. There are separate standards for materials (M Series), Facilities (F Series), Flat Panel Displays (D Series), and Traceability (T Series), and the S Series governs environment, health and safety (EHS). These standards have been employed by many equipment users, primarily in the United States. Their headquarters are in California, and there are offices around the world, including in Tokyo.

Structure of SEMI S Series

Item	Content
SEMI S1	Safety Guideline for Equipment Safety Labels
SEMI S2	Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment
SEMI S3	Safety Guidelines for Process Liquid Heating System
SEMI S4	Safety Guideline for the Separation of Chemical Cylinders Contained in Dispensing Cabinets
SEMI S5	Safety Guideline for Sizing and Identifying Flow Limiting Devices for Gas Cylinder Valves
SEMI S6	EHS Guideline for Exhaust Ventilation of Semiconductor Manufacturing Equipment
SEMI S7	Safety Guidelines for Environmental, Safety, and Health (ESH) Evaluation of Semiconductor Manufacturing Equipment
SEMI S8	Safety Guidelines for Ergonomics Engineering of Semiconductor Manufacturing Equipment
SEMI S9 (revoked)	Guide to Electrical Design Verification Tests for Semiconductor Manufacturing Equipment
SEMI S10	Safety Guideline for Risk Assessment and Risk Evaluation Process
SEMI S11 (revoked)	Environmental, Safety, and Health Guidelines for Semiconductor manufacturing Equipment Mini-environments
SEMI S12	Guidelines for Equipment Decontamination
SEMI S13	Environmental, Health and Safety Guideline for Documents Provided to the Equipment User for Use with Semiconductor Manufacturing Equipment
SEMI S14	Safety Guidelines for Fire Risk Assessment and Mitigation for Semiconductor Manufacturing Equipment
SEMI S15 (revoked)	Safety Guideline for the Evaluation of Toxic and Flammable Gas Detection Systems
SEMI S16	Guide for Semiconductor Manufacturing Equipment Design for Reduction of Environmental Impact at End of Life
SEMI S17	Safety Guideline for Unmanned Transport Vehicle (UTV) Systems
SEMI S18	Environmental, Health and Safety Guideline for Silane Family Gases Handling
SEMI S19	Safety Guideline for Training of Semiconductor Manufacturing Equipment Installation, Maintenance and Service Personnel
SEMI S20 (revoked)	Safety Guideline for Identification and Documentation of Energy Isolation Devices for Hazardous Energy Control
SEMI S21	Safety Guideline for Worker Protection
SEMI S22	Safety Guideline for the Electrical Design of Semiconductor Manufacturing Equipment
SEMI S23	Safety Guideline for Conservation of Energy, Utilities and Materials used by Semiconductor Manufacturing Equipment
SEMI S24	Safety Guideline for Multi-Employer Work Areas
SEMI S25	Safety Guideline for Hydrogen Peroxide Storage & Handling Systems
SEMI S26	Environmental, Health, and Safety Guideline for FPD Manufacturing System
SEMI S27	Safety Guideline for the Contents of Environmental, Safety, and Health (ESH) Evaluation Reports
SEMI S28	Safety Guideline For Robots And Load Ports Intended For Use In Semiconductor Manufacturing Equipment
SEMI S29	Safety Guideline for Fluorinated Greenhouse Gas (F-GHG) Emission Characterization and Reduction

(As of July 2018)

2. Description of Safety Component-related Standards

(1) Description of Standard

This section describes the international standards in the order of the standard number, and lists corresponding EN standards and JIS standards. (As of July 2018)

ISO 12100

Safety of machinery - General principles for design - Risk assessment and risk Reduction
EN standards: EN ISO 12100
JIS standards: JIS B 9700

- **Description**

These standards define the basic concepts of machinery safety and stipulates safety design procedures.

- **Main Points**

(1) Machinery hazards are classified as follows:
Mechanical hazards, electrical hazards, thermal hazards, hazards generated by noise, hazards generated by vibrations, hazards generated by radiation, hazards generated by materials and substances, and hazards generated by neglecting ergonomic principles in machine design.
(2) Identify the preceding hazards and apply safety design procedures to reduce risks.
Step 1: Specify the operating range of the machine.
Step 2: Identify the hazardous events and assess the risks.
Step 3: Use inherently safe design to remove hazards and reduce risks as much as possible.
Step 4: Design guards, safety equipment, and other safeguards against any residual risks.
Step 5: Inform and warn users about any residual risks.

ISO 13849-1

Safety of machinery - Safety-related parts of control systems - Part 1 : General principles for design
EN standards: EN ISO 13849-1
JIS standards: JIS B 9705-1

- **Description**

These standards apply to control systems where safety is a concern.

- **Main Points**

(1) Manufactures need to consider the anticipated degree of injury (light to serious) and the probability of injury (rare to common) in determining the hazard level of machinery.
(2) These standards classify hazard levels in five required performance levels and stipulate requirements for Safety-related parts of control systems.

ISO 13849-2

Safety of machinery - Safety-related parts of control systems - Part 2 : Validation
EN standards: EN ISO 13849-2

- **Description**

Regarding the verification and validation of the conformity to the ISO 13849-1 requirements.

- **Main Points**

In order to verify conformity to the requirements, the following should be specified:
(1) Guidelines for validity testing and inspections
(2) General considerations at time of design
(3) List of failures and fault exclusion criteria
(4) Test and Test results or report

ISO 13850

Safety of machinery - Emergency stop - Principles for design
EN standards: EN ISO 138850
JIS standards: JIS B 9703

• Description

These standards stipulate principles used to design emergency stop functions.

• Main Points

(1) Electrical emergency stop devices should conform with IEC 60947-5-5.
(2) Stop category must be 0 or 1.
(3) The emergency stop devices must be placed where operators can access them easily and can operate them without exposure to hazards.

ISO 13851

Safety of machinery - Two-hand control devices, Functional aspects and design principles
EN standards: EN 574
JIS standards: JIS B 9712

• Description

These standards stipulate safety requirements related to the design and selection of two-hand control devices.

• Main Points

(1) Stipulates dimensions for prevention of defect.
(2) In case of type III C, output signal shall be designated only when both input signals are actuated within 0.5 s.
(3) Classify devices by type (type I, II, IIIA, IIIB and IIIC) and risk assessment results as the basis for selecting devices.

ISO 13855

Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body
EN standards: EN ISO 13855
JIS standards: JIS B 9715

• Description

These standards stipulate the minimum distance that should be provided between hazardous parts of machinery and protective equipment. Referred to as the safe distance, this distance is calculated from the operator approaching direction, protective equipment response time, machine response time, and minimum object size detectable by the protective equipment.

• Main Points

(1) These standards apply when individual machine standards do not prescribe the method used to calculate minimum distance.
(2) Protective equipment must be selected with a detection performance level capable of maintaining a minimum distance so machines can be stopped before they pose a hazard to operators.

ISO 13856-1

Safety of machinery - Pressure-sensitive protective devices - Part 1 : General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors
EN standards: EN ISO 13856-1
JIS standards: JIS B 9717-1

• Description

These standards stipulate requirements for mats and floors that detect a hazardous condition as a safety device protecting operators from hazardous machines when an operator steps on them.

• Main Points

(1) These mats must detect operators with a weight of 35 kg or more.
(2) The controller units' PL must be c or higher.
(3) Enclosure rating of mats must be IP54 or higher.
(4) The output signals must be turned OFF within 200ms after a vertical contact with the mat surface at a speed of 0.25m/s.

ISO 13856-2

Safety of machinery - Pressure-sensitive protective devices - Part 2 : General principles for the design and testing of pressure-sensitive edges and pressuresensitive bars
EN standards: EN ISO 13856-2

• Description

These standards stipulate requirements for edges and bars that detect a hazardous condition as a safety device protecting operators from hazardous machines when an operator presses them.

ISO 14119

Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
EN standards: EN ISO 14119
JIS standards: JIS B 9710

• Description

These standards stipulate general design and selection principles for equipment that uses interlocking devices for safety.

• Main Points

(1) There are four types of interlocking devices: type 1 (mechanical, without coding), type 2 (mechanical, with coding), type 3 (non-contact, without coding), and type 4 (non-contact, with coding).
(2) Interlocking devices with coding are classified into three levels based on the number of actuator IDs, low (1 - 9), medium (10 - 1000), and high (1001 -).
(3) Interlocking devices need to be designed so as to minimize the possibility that a user may disable them based on analysis at the design phase.
(4) The lock status of the guard lock must be monitored.
(5) In case of PL_r = d or e, the fault exclusion cannot be applied to mechanical part of interlocking devices. For example, two contacts in one interlocking device cannot be certified as being duplexed.

IEC 60204-1

Safety of machinery - Electrical equipment of machines - Part 1 : General requirements
EN standards: EN 60204-1
JIS standards: JIS B 9960-1

• Description

These standards apply to electrical equipment with a maximum rated power supply voltage of 1,000 VAC or 1,500 VDC between lines or a maximum rated frequency of 200 Hz.

• Main Points

These standards stipulate all elements required in electrical equipment for machines including the control circuits, functions, devices, safety measures, and technical documents related to the installation, operation, and maintenance of electrical and electronic equipment in machines.

IEC 60947-5-1

Low-voltage switchgear and controlgear - Part 5-1 : Control circuit devices and switching elements - Electromechanical control circuit devices
EN standards: EN 60947-5-1
JIS standards: JIS C 8201-5-1

• Description

These standards apply to control circuit devices and switching elements that are produced to control, signal, and interlock switching and control devices. It applies to control circuits with a maximum rated voltage of 600 VDC or 1,000 VAC (a maximum frequency of 1,000 Hz).

• Main Points

(1) These standards consist of General Requirements, Special Requirements for Indicators, and Special Requirements for direct opening action.
(2) It contains provisions such as switching capacity, temperature rise, terminal strength, protective structures, and direct opening action.

IEC 60947-5-5

Low-voltage switchgear and controlgear - Part 5-5 : Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function
EN standards: EN 60947-5-5
JIS standards: JIS C 8201-5-5

• Description

These standards stipulate electrical/mechanical structure of emergency stop switches with a latching mechanism.

• Main Points

(1) Switches must have a direct opening action.
(2) Switches must have a latching mechanism.
(3) The operative parts must be structured to allow easy access to the mushroom-shaped pushbuttons, wires, and ropes.
(4) The operative parts must be red on a yellow background.

IEC 60947-5-8

Low-voltage switchgear and controlgear - Part 5-8 : Control circuit devices and switching elements - Three-position enabling switches
EN standards: EN 60947-5-8
JIS standards: JIS C 8201-5-8

• Description

These standards stipulate 3-position enabling switches, for enable devices under the IEC60204-1.
This does not apply to devices that employ teaching pendants or grip switches etc., but only to those devices with built-in enable switches.

• Main Points

(1) Stipulates electrical properties such as withstand voltage and insulation, and operating characteristics for operating stroke and load etc.
(2) Stipulates the 3-position enabling switch mark.

IEC 61310-1

Safety of machinery - Indication, marking and actuation - Part 1 : Requirements for visual, acoustic and tactile signals
EN standards: EN 61310-1
JIS standards: JIS B 9706-1

• Description

These standards set out specific requirements regarding visual, audio and tactile methods for providing safety related information to operators and those that may be placed in dangerous situations.

• Main Points

(1) Separate signals into passive and active
(2) Visual spectrum, brightness, and contrast ratio
(3) Meaning of colors and the shape of markings, and examples of forms that can be discerned by touch alone
(4) Operating switch symbols
(5) Shape, color and dimensions of safety markings (Prohibitions, warnings, information etc.)

IEC 61310-2

Safety of machinery - Indication, marking and actuation - Part 2 : Requirements for marking
EN standards: EN 61310-2
JIS standards: JIS B 9706-2

• Description

These standards set out the identification of machines, and markings to ensure safe use and the reduction of danger from incorrect connections.

• Main Points

(1) Regulations regarding manufacturer information (manufacturer name, address etc.), and rating information (power supply range, maximum speed etc.)
(2) Regulations regarding necessary markings such as for AC, DC and earthing etc.

IEC 61310-3

Safety of machinery - Indication, marking and actuation - Part 3 : Requirements for the location and operation of actuators
EN standards: EN 61310-3
JIS standards: JIS B 9706-3

• Description

Specifies safety issues for actuators that are operated by hand or by human control.

• Main Points

(1) Set up away from dangers, and avoid ambiguous operations. Also, be sure that operation does not create alternative risks.
(2) Design to increase the clockwise rotation of handles and lifting action for levers, so that the operator is better aware of the resulting operation.
(3) Two-handed operating controls and enabling devices where necessary.

IEC 61496-1

Safety of machinery - Electro-sensitive protective equipment - Part 1 : General requirements and tests
EN standards: EN 61496-1
JIS standards: JIS B 9704-1

• Description

These standards apply to equipment, such as safety sensors safety light curtains, that detect the presence of operators electrically and output a control signal for their protection. They stipulate items like fault detection performance, software design policy, heat resistance performance, EMC performance, vibration and shock performance, indicator colors, labeling details, and the content of instructions.

• Main Points

(1) Electro-sensitive protective equipment (ESPE) is classified as type 2, type 3 or type 4.
(2) The provisions in these standards stipulate that equipment displays the fault mode for electronic components in the equipment and they demonstrate that safety characteristics for the type of equipment are maintained in all fault modes.

IEC 61496-2

Safety of machinery - Electro-sensitive protective equipment - Part 2 : Particular requirements for equipment using active opto-electronic protective devices (AOPDs)
EN standards: EN 61496-2
JIS standards: JIS B 9704-2

• Description

These standards apply to the type of ESPE that in principle detect emitted or received light. They stipulate items such as detection performance for the minimum size object detected, effective aperture angle, extraneous light resistance performance, and mutual interference resistance performance.

• Main Points

(1) Directional angles are stipulated separately for type 4 and type 2 according to the distance between the emitter and receiver.
(2) Conditions that maintain ordinary operation and conditions that permit incorrect operation safely are stipulated for all extraneous light sources.

IEC 61496-3

Safety of machinery - Electro-sensitive protective equipment - Part 3 : Particular requirements for Active Optoelectronic Protective Devices responsive to Diffuse Reflection (AOPDDR)
EN standards: EN 61496-3
JIS standards: JIS B 9704-3

• Description

These standards apply to electro-sensitive protective equipment that diffuse or reflect light. They stipulate items such as detection performance for the detection range, allowable errors, response time, detection capacity, resistance to extraneous light, and reflective detection capability as well as the influence of background interference.

• Main Points

(1) Only stipulated for Type 3. (not specified for types 1, 2 and 4)
(2) Conditions that maintain ordinary operation and conditions that permit incorrect operation safely are stipulated for all extraneous light sources.

IEC 61800-5-2

Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional
EN standards: EN 61800-5-2

• Description

These standards are applied to designing/developing of safety related power drive systems (PDS(SR)), and created based on the IEC 61508 Series Functional Safety Standards.

• Main Points

(1) More than 10 types of safety sub-functions, such as STO, are defined.
(2) The development procedure is the same as IEC 61508.
(3) SIL is used as the indicator of safety functions.
(4) General failures and falut exclusion are explicitly indicated.

IEC 62046

Safety of machinery - Application of protective equipment to detect the presence of persons
EN standards: EN IEC 62046

• Description

These standards stipulate requirements for selection/installation of protective equipment to detect persons such as light curtains, safety mats, etc.

• Main Points

(1) Description on types and characteristics of protective equipment and considerations for selection
(2) Description on considerations about added functions of light curtains and others, such as muting and overriding
(3) Regulations on inspection and testing

IEC 62061

Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN standards: EN 62061
JIS standards: JIS B 9961

• Description

These standards specify those matters applicable to the machinery portion of the industry as included in the IEC 61508 Series Functional Safety Standards.
These standards apply to the design and verification of safety related control systems that use electrical, electronic, and programmable electronic control systems.

• Main Points

Standards, including the following, for the allotment of SIL (Safety Integrity Level) and in order to achieve the allotted SIL, for safety functions performed by safety control systems.
(1) Functional safety management
(2) Create specifications for safety controls
(3) Control system design
(4) User information (Manual)
(5) Validation

IEC/TR 62061-1, ISO/TR 23849

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

• Description

Guidance on the application of ISO 13849-1 and IEC 62061 jointly created by ISO and IEC. Although the both standards are not the same, an equivalent level of risk reduction is possible by applying each standard correctly. Machine designers can decide which of those should be used depending on its application.

• Main Points

(1) Both PL and SIL are categorized by PFH (Probability of dangerous Failure per Hour).
(2) Integration by combining safety-related parts with subsystems
(3) Explicit indication of considerations for applying fault exclusion
(4) Calculation examples

IEC 61810-3

Electromechanical elementary relays - Part 3: Relays with forcibly guided (mechanically linked) contacts
EN standards: EN 61810-3

Relay with forcibly guided (mechanically linked) contacts

• Description

These standards apply to control circuit relays that are installed for safety and its provisions are for self-monitoring relays that have a forced guided mechanism that prevents normally open and closed contacts from closing simultaneously.

• Main Points

(1) If a normally open contact of a relay with forcibly guided (linked) contact is welded shut, the coil switches OFF and all normally closed contacts must maintain a gap of at least 0.5 mm. Even if a normally closed contact is welded shut, the coil switches ON and all normally open contacts must maintain a gap of at least 0.5 mm.
(2) Ideally, contact load switching must comply with the AC-15 (AC electromagnetic load) and DC-13 (DC electromagnetic load) utilization categories.
(3) The forced guide contact mark may be used on all class A relays (all relays with forcibly guided (linked) contacts).

GS-ET-15

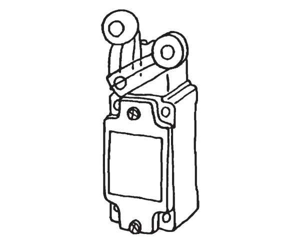
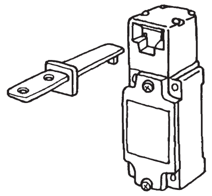
Principles of testing and certification for direct opening action switches

• Description

These are German labor safety standards that were enacted to prevent industrial accidents. They apply to testing on direct opening action detector switches that are installed for safety.

• Main Points

(1) Limit and door switches are classified in two categories according to function.

	B1 A safety switch falls under category 1 if the switch mechanism and actuator are of monoblock construction physically and functionally, and the safety function is activated by actuator operation.
	B2 A safety switch falls under category 2 if the switch mechanism and actuator are not of monoblock construction and the safety function is activated when the actuator is separated from the switch mechanism.

(2) The switches must have a direct opening action, a mechanical service life of 1,000,000 operations, Protective class of IP54, and must not operate with any tool except a special tongue.

GS-ET-19

Principles of testing and certification for interlocking devices with solenoid guard-locking

• Description

These are also German labor safety standards. They apply only to devices that have a lock monitoring mechanism in door switches that use a key lock for safety.

• Main Points

(1) The switches must use a mechanism like a solenoid for locking and unlocking.

(2) They must have a locking strength and direct opening action, a mechanical service life of 1,000,000 operations, and a protective class of IP54, and must not operate with a tool other than a special tongue.

(2) Safety component terminology

1) General Terminology

• Class 1 circuit (NFPA 70)

Class 1 remote-control, signaling, and power-limited circuits
Class 1 circuit is further divided into two circuits:
(A) Class 1 power-limited circuit
This circuit is supplied power from 30 V or less and 1000 VA or less power source.
(B) Class 1 remote-control and signaling circuit
This circuit must be 600 V or less. There is no regulation on current limitation.

• Class 2 circuit (NFPA 70)

Class 2 remote-control, signaling, and power-limited circuits
This circuit uses Class 2-certificated power supplies and/or transformers and utilizes Class 2 or Class 3-certificated conductors as wiring parts.

• Class 3 circuit (NFPA 70)

Class 3 remote-control, signaling, and power-limited circuits
This circuit uses Class 3-certificated power supplies and/or transformers and utilizes Class 3-certificated conductors as wiring parts. Class 2-certificated conductors cannot be used in Class 3 circuits.

• ELV (IEC 60364-4-41)

Extra-Low Voltage
A circuit that satisfies the following two criteria for protection from electrical shock caused by direct and indirect contacts: (1) AC 50 V or less or DC 120 V (the RMS of ripple voltage must be 10 % or less of DC components) and (2) isolation from hazardous voltage levels at least with basic insulation. ELV is categorized into FELV, PELV, and SELV.

• SELV (IEC 60364-4-41)

Safety Extra-Low Voltage
A circuit that meets all the following criteria for protection from electrical shock caused by direct and indirect contacts:
(1) AC 50 V or less or DC 120 V (the RMS of ripple voltage must be 10 % or less of DC components)
(2) Basic insulation from other SELV or PELV circuits
(3) Double insulation or reinforced insulation from other non-SELV or non-PELV circuits
(4) Basic insulation from ground (earthing is not allowed)
(5) When using plugs and sockets:
- Plugs cannot be inserted into other power voltage system sockets.
- Sockets cannot accept plugs from other power voltage systems.

Note: these criteria may be different for other standards.

• PELV (IEC 60204-1)

Protective Extra-Low Voltage
A circuit that meets all the following criteria for protection from electrical shock caused from indirect contact and limited area direct contact.
(1) In a usually dry place where human bodies are unlikely to widely contact with live parts: AC 25 V or less or DC 60 V (the RMS of ripple voltage must be 10 % or less of DC components)
Otherwise: AC 6 V or less or DC 15 V (the RMS of ripple voltage must be 10 % or less of DC components)
(2) Either side of the circuit or one point of power source must be connected to a protective bonding circuit.
(3) Live parts of PELV circuits must be electrically isolated from other live circuits. This electrical isolation must satisfy criteria required for the interface between the primary and secondary circuits of safety isolating transformers.
(4) Conductors for each PELV circuit must also be physically isolated from other circuits. When this cannot be implemented, use insulation measures stipulated in the IEC 60204-1, 13.1.3.
(5) When using plugs and sockets:
- Plugs cannot be inserted into other power voltage system sockets.
- Sockets cannot accept plugs from other power voltage systems.

Note: these criteria may be different for other standards.

2) Switch/Relay Terminology

• Rated Operational Voltage (U_e) (IEC 60947-1)

The rated operational voltage (U_e) of equipment is the voltage applied to equipment, and is combined with the rated operational current (Ie) as references for utilization categories (i.e., AC-15).

• Rated Operational Current (I_e) (IEC 60947-1)

The rated operational current (I_e) is the current applied to equipment.

• Conventional Free Air Thermal Current (I_{th}) (IEC 60947-1)

The Conventional Free Air Thermal Current (I_{th}) is the maximum value of testing current used for temperature rise tests (under open air) of devices that are not sealed within free air.

• Conventional Enclosed Thermal Current (I_{the}) (IEC 60947-1)

The Conventional Enclosed Thermal Current (I_{the}) is the flowing current value declared by the manufacturer to use for temperature rise tests of highly sealed devices.

• Rated Impulse Withstand Voltage (U_{imp}) (IEC 60947-1)

The rated impulse withstand voltage (U_{imp}) is the peak value for an impulse voltage of prescribed form which equipment is capable of withstanding without failure and to which clearance values are referred.

• Rated Insulation Voltage (U_i) (IEC 60947-1)

The rated insulation voltage (U_i) is the maximum operating voltage that can be withstood without damage. It is the reference voltage for dielectric strength tests and creepage distance for insulation material. The maximum value of the rated insulation voltage (U_i) must be greater than that of the rated operating voltage.

• Switching overvoltage (IEC 60947-1)

The switching overvoltage is the maximum reverse voltage generated during load switching. Do not exceed Uimp value.

• Rated Conditional Short - Circuit Current (IEC 60947-1)

The rated conditional short-circuit current is the current stated by the manufacturer that a product can withstand provided the product is protected by a device (10-A fuse model gI or gG/IEC 60269 for the D4BL) that is designated by the manufacturer under conditions specified by related product standards.

• Contact rating designation (UL 508, IEC 60947-5-1)

Electrical rating of contacts based on load types is expressed with one alphabetic character and 3 digit numerical value. The following example is provided for A600.

Name	Utilization category	Conventional enclosed thermal (I_{the})
A600	AC-15	10A

120V(U_e)	... 380V(U_e)	... 600V(U_e)
6A(I_e)	1.9A(I_e)	1.2A(I_e)

• Utilization Category for Switching Capacity (IEC 60947-1)

Utilization Category for Switching Elements

Current	Category	Typical switched load
AC	AC-12	AC resistive loads and solid-state loads with isolation by optocouplers.
	AC-13	AC solid-state loads with transformer isolation.
	AC-14	AC small electromagnetic loads (≤72 VAC).
	AC-15	AC electromagnetic loads (>72 VAC).
DC	DC-12	DC resistive loads and solid-state loads with isolation by optocouplers.
	DC-13	DC electromagnetic loads.
	DC-14	DC electromagnetic loads having economy resistors in circuit.

3) Sensor Terminology

• Type4 (IEC 61496-1)

Type 4 safety equipment satisfy the PL = e requirements prescribed in ISO 13849-1.

• ESPE (IEC 61496-1)

Electro-Sensitive Protective Equipment
Equipment electrically detects people and outputs a control signal for their protection.

• AOPD (IEC 61496-2)

Active Opto-electronic Protective Device
Electro-sensitive protective equipment that operate on the principle of detection by emitted and received light.

• Detection zone (IEC 61496-1)

The range within which objects can be detected. In case of a light curtain, the detection zone is rectangular in shape. In OMRON, to express dimensions of a detection zone, the length between an emitter and a receiver is called an operating range, and the length from the 1st beam to the last one is called a protected height.

• Response Time (IEC 61496-1)

The response time is the maximum amount of time it takes from the moment someone is detected in the detection zone until the output turns OFF. The time it takes to turn output ON again once it goes off is also listed in catalog specifications mainly for system design.

• Muting (IEC 61496-1)

The muting function temporarily disables the detection function.
When the muting function is turned ON, the protective equipment remains ON regardless of whether someone enters the detection zone or not.

• Test Piece (IEC 61496-2), Test Rod

A test piece (test rod) is an opaque rod equivalent to the smallest detectable object. It is used to check the detection performance of area sensors.

• Minimum Distance (ISO 13855)

The minimum distance is the distance that must be allowed from hazardous parts of machinery to the protection equipment. The detection zone need to be designed so that machinery will turn OFF before someone reaches hazardous area.

• Effective Aperture Angle, EAA (IEC 61496-2)

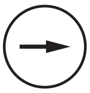
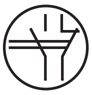
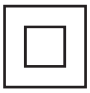
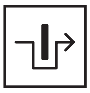
The effective aperture angle is the angle to which area sensors must be rotated to switch the output from ON to OFF. Measurements can be taken in two directions with lateral rotation as long as the rotation follows the axis formed by the light beams.

• Lock-out condition (IEC 61496-1)

Lock-out condition disables normal operation and it occurs when the output is forced OFF. When safety light curtain's control output remains OFF because diagnostic system results have determined that operation cannot be resumed as a result of a fault, this is called a lock out.

(3) Markings

Cautions are displayed with symbols on nameplates for using safety devices. The followings are typical safety-related symbols.

Meaning	Mark
Arrow indicating direct opening action (displayed on conforming products to IEC 60947-5-1, Annex K)	
Indicates type A forcibly guided (linked) contact marking. (displayed on conforming products to IEC 61810-3)	
Indicates double insulation (displayed on conforming products to IEC 61140 Class II)	
Indicates equipment with guard lock monitoring function (displayed on conforming products to ISO 14119)	

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN

Contact: www.ia.omron.com

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31)2356-81-300/Fax: (31)2356-81-388

OMRON ASIA PACIFIC PTE. LTD.
No. 438A Alexandra Road # 05-05/08 (Lobby 2),
Alexandra Technopark,
Singapore 119967
Tel: (65) 6835-3011/Fax: (65) 6835-2711

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900/Fax: (1) 847-843-7787

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-5037-2222/Fax: (86) 21-5037-2200

Authorized Distributor:

Cat. No. Y221-E1-03 1018(0317)