OMRON

STI
SAFETY,
TECHNOLOGY
& INNOVATION

SAFETY COMPONENTS

Techinical Guide

Fourth 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

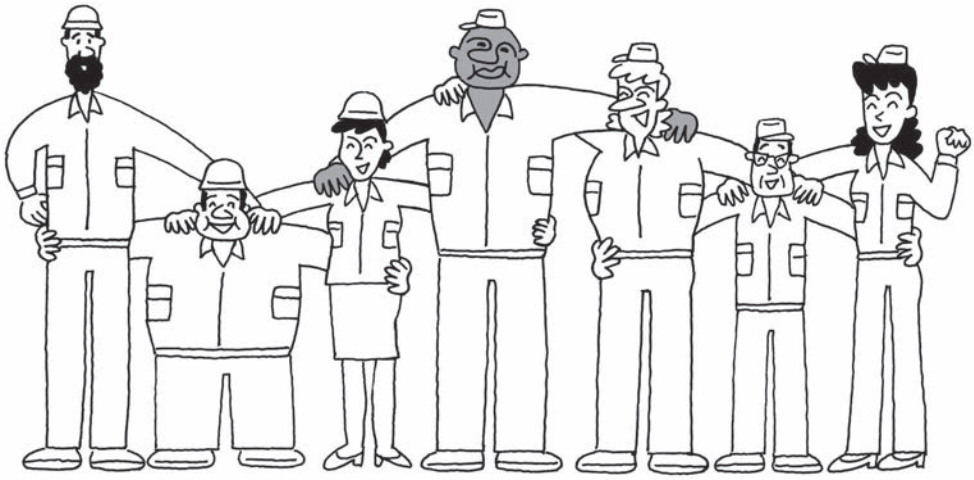
What Is Safety? The Social Background

In the manufacturing industry, production consists of processing, assembling, and transporting materials. In modern times, machines use large amounts of energy to absorb the burden from workers to assist in production. This result in the wide range of development in machines that we see today. And trained workers based on experience in operating the machines create more stable quality, causing the relationship between machines and production to continue and evolve into many forms today.

1. The Social Background to Safety of Machinery

(1) Changes in People

In some countries, changes in social structure have brought changes in the people that work at production sites. For example, many experienced workers are retiring while the working population shrinks due to lower birth rates. At the same time, forms of employment continue to diversify, such as the increasing number of temporary employees and there is a continued increase in employees working overseas. Diversification also continues to increase in other ways, such as age, sex, experience, language, and social habits.

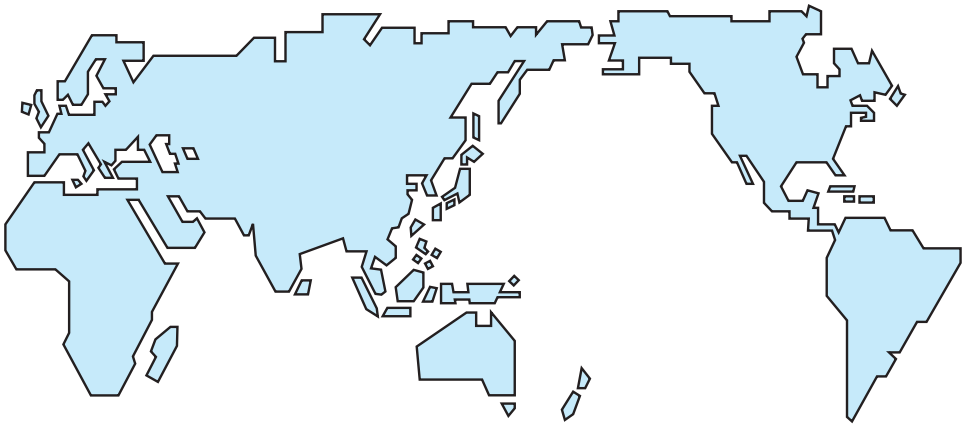


(2) Changes in Machines and Production Facilities

Today's society is facing more diversification in consumer needs driving demands for more variation in products. Production sites are required to change between many different products at relatively short intervals, resulting in frequent changes to production facilities. Machines required for production must support more functionality.
This and many other changes require that workers must master new techniques and working procedures.

(3) Changes in Production Locations

Market globalization has taken production sites from fixed sites across national borders. Domestic production is faced with the need for more competitive products and new markets combined with demand for production sites in newly industrialized countries, such as BRICs. Offshore production means dealing with different laws, infrastructures, cultures, and values. The machines and production facilities resulting from the accumulated knowhow of industry domestically must now be used in different human environments.



(4) Changes in Social Consciousness

In mature civil societies, companies must take social responsibility for their activities. For example, they must assume product liability for the products that they produce. Although conditions vary by country, all countries now have laws requiring product safety to protect the consumer. (For example, Japan and the USA have product liability laws and the EU has the EC directives.) It is not necessary to provide examples of product accidents to realize the very strict monitoring of manufacturing liability for safety and ease of mind in societies that share a common ideal of respect for human beings. And based on these ideals, the responsibility of companies for the safety of workers on production sites is also strictly monitored. (For example, OSHA in the USA, the Revised Industrial Safety and Health Law in Japan, and EC directives in the EU.) Companies face not only criminal, civil, and damage liability for any accidents that might occur, but their corporate image is greatly hurt as a result. The social liability of companies for the safety of their workers has skyrocketed in recent years.

The relationship between workers and machines and the environment in which they operate has thus changed on a global scale. And yet, manufacturing is not possible until a worker operates a machine. Across changes in the operating environment, society demands that machines and production facilities can be used safely regardless of where they are used or who uses them. This is required not only in the workers, but also in the machines and hardware technology. As a result, global standards for safety are required for today's production sites. This is the concept of Safety of Machinery.

2. Safety of Machinery

Security assurance which was not enough by the human scheme is intended to be secured against the machines themselves by the engineering means for a higher level of assurance. Safety standards define the requirements for the safety of machinery.
ISO 12100 was officially issued in November 2003 as an international safety standard.
Publication of ISO 12100: 2010 was followed by the integration of ISO 12100-1, ISO 12100-2 and ISO 14121 into "General principles for design - Risk assessment and risk reduction."
Typical standard for the safety of machinery is an European Standard (EN).
EN standard is established as the engineering criteria for meeting the basic safety requirements defined in the machinery directive within the European Union and the conformity with the EN standard is a prerequisite for the EC Declaration of Conformity which is mandatory for the distribution within the EU.
Thus, conformity with the directives or standards is performed as part of the mechanical design or engineering and some technical files are treated as a complete set of documents for machinery.

(1) Strategies for Selecting Safety Measures

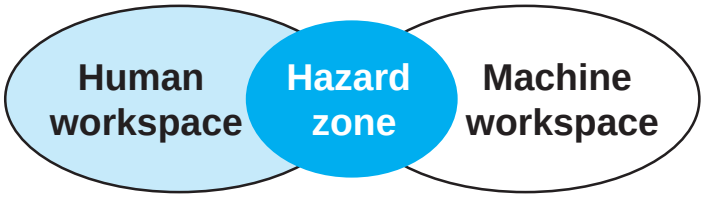
1) Separation between human and machinery

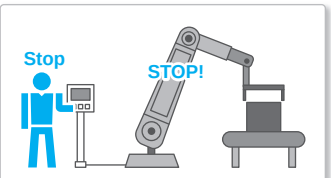
Machinery hazards occur in hazard areas, where the human workspace overlaps the machine workspace.
Preventing machinery hazards begins by eliminating mechanisms that facilitate hazardous conditions.
The following strategies are generally used to achieve this goal.

1. Spatial separation between human and machine workspaces (Isolation principle: Safeguarding with guards)

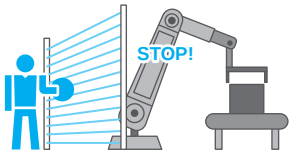
2. Temporal separation (Stoppage principle: Safeguarding with interlocking devices *)

* An interlocking device refers to a mechanical or electrical device that was designed to prevent machines from operating unless certain conditions are met, such as closing a guard for example. (ISO 14119)

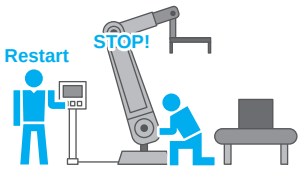




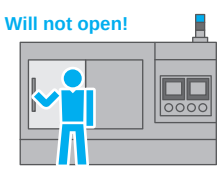
Emergency stop ensures termination of the power source.



The machine stops safely even if a failure occurs on light curtains.



Unauthorized personnel intrusion disables the restart.



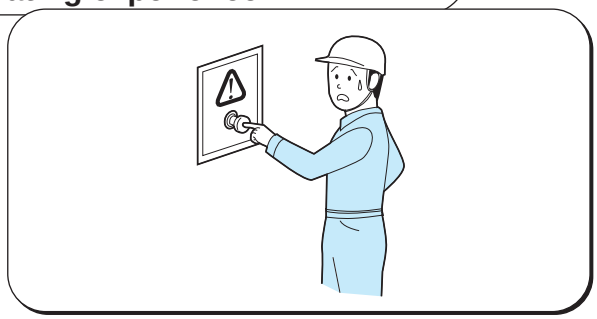
A door will not open until a machine stops.

2) Safety Measure Strategy

All machines fail and everyone makes mistakes.
Therefore, basic designs that take every precaution to ensure the safety of operators is required in the event of a fault.

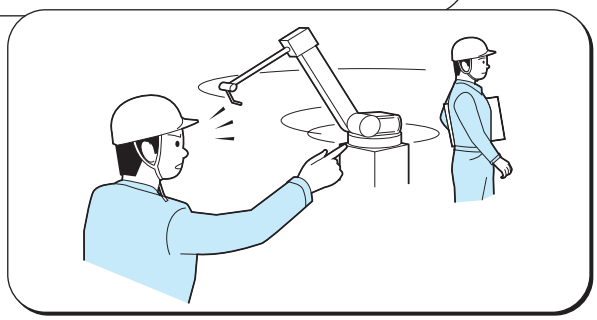
Humans make mistakes.

Ensuring safety irrespective of operating experience



Machines fail.

Ensuring safety during machine setup and maintenance



3) Safety secured by de-energizing

Isolating the human and machine states of operation with respect to time by controlling the interlocking devices can be achieved in principle by shutting down the machine power source and thus reducing the risk derived from the motion of the machine.

Note: If, however, de-energizing increases another risk (such as fall, scatter or overturn due to the loss of retention power), this does not apply.

IEC 60204-1 defines how the power is shut off with the stop categories of 0 to 2 depending on the behavior from the request of emergency stop to the machine operation termination. Take the optimum scheme for shutting down the energy from the selected risk reduction measures.

Note: Depending on the risk reduction measures, there are some cases where the stop categories are specified by the standard's requirement.

Type of Stop Functions

Stop Category 0

Stop category 0 is an uncontrolled stop that is achieved by immediately removing power to the machine actuators (e.g., directly cutting off the power supply).

Stop Category 1

Stop category 1 is a controlled stop that is achieved by sending a stop command from the control circuit to stop (e.g., brake) the machine actuators and then removing power to the actuators (e.g., cutting off control circuit power) after the stop is achieved.

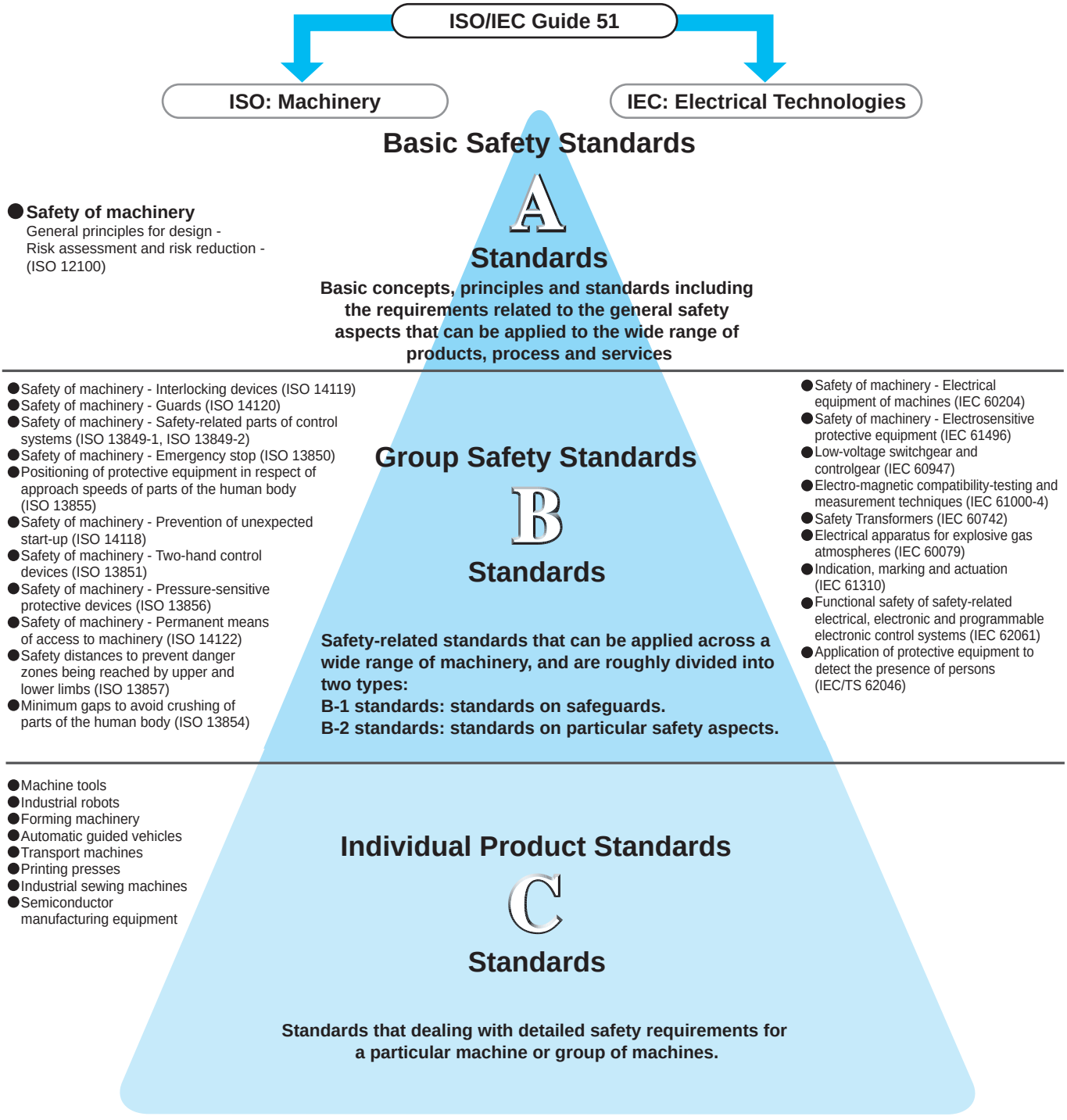
Stop Category 2

Stop category 2 stops machine actuators without cutting off the power.

3. Safety Requirements

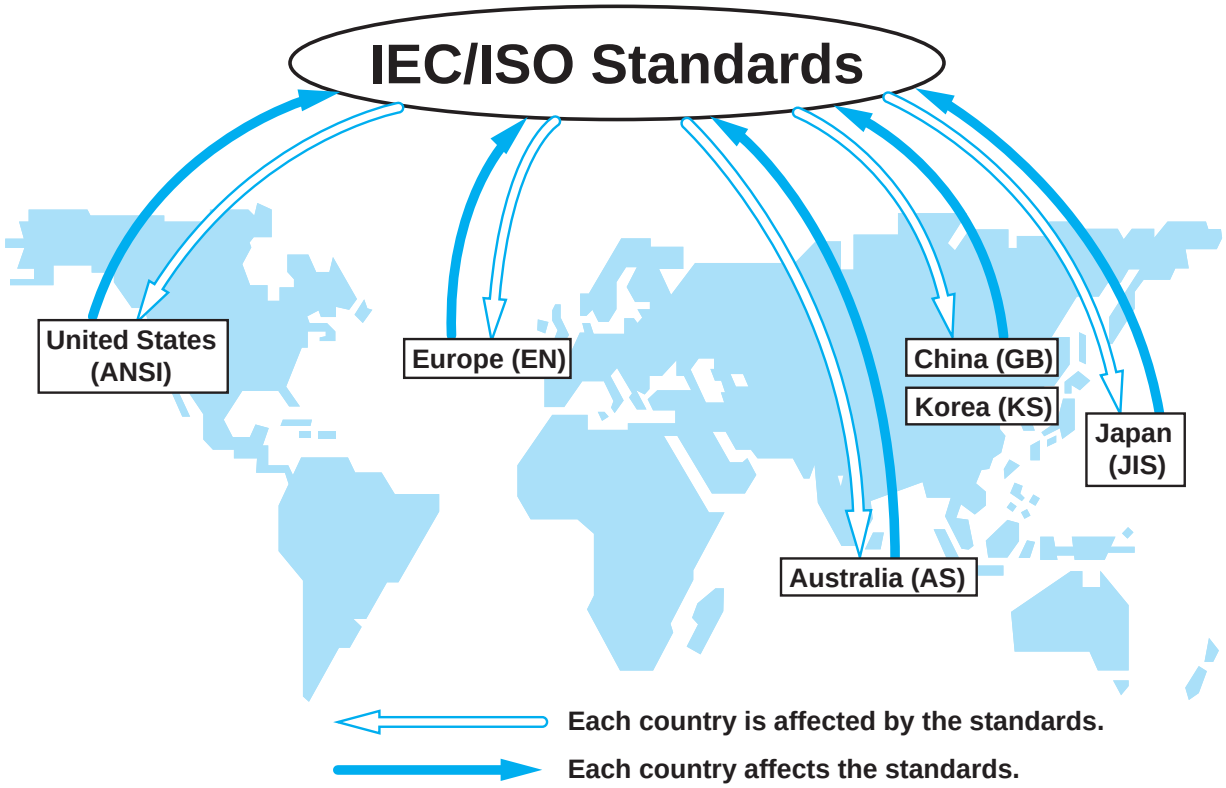
(1) System of Standards for Safety of Machinery

The International Electrotechnical Commission (IEC) prepares international standards for all electrical, electronic and related technologies, and the International Organization for Standardization (ISO) prepares international standards for all technologies other than electrical and electronic technologies (machinery and management). European countries often take the initiative in proposing the standards and establishing them as ISO/IEC international standards. The standards referred to here are related to the safety aspects and they are classified into three tiers of standards of A, B and C as shown below for coverage of wide variety of machinery as well as fulfilling the specific purposes.



Accelerated international harmonisation of safety standards

The international standards which have been created by each country in its own way are now geared to the harmonisation with the ISO/IEC international standards by the WTO Standards Alliance.
It is mandatory for WTO members to adopt its policy into their safety regulations of each country. With the technological advancement, the international standards are actively greeted with new proposals and amendments by years and the way to the integrated standards is now under way throughout the world.

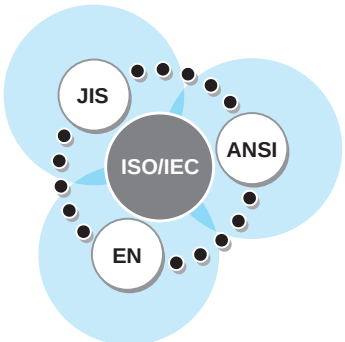


International Standards and Design of Machines and Devices

Responding to Machine and Device Design Standards Today

International standards

(1) The newest information on international standards and industry standards must be collected, and the contents of new and revised standards must be understood.



(2) The differences between EN, UL, JIS, and other standards must be understood.

(3) Global designs must be created that taking into account the differences.

MEMO

Chapter 2

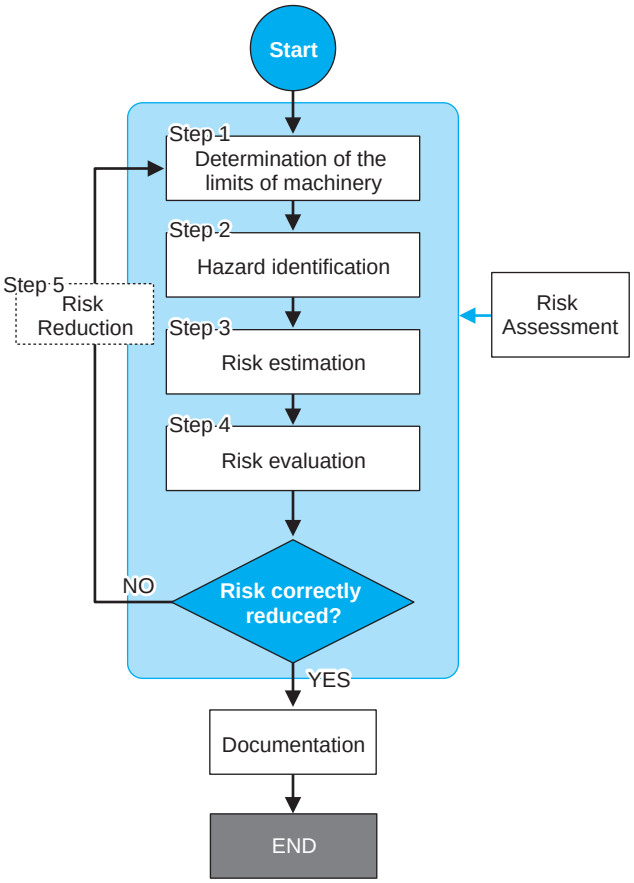
Risk Assessment and Risk Reduction

1. Risk Assessment

To operate machines safely, risk must be reduced by analyzing/assessing machine hazards. ISO standards define the procedure to achieve risk reduction.
The hazards and risk levels present at the machine are different for each phase of the machine lifecycle (construction, modification, transportation and disassembling, decommissioning, etc.). Machines must be designed and produced so that they operate safely in every phase of their lifecycle.
The risk assessment can be logically performed by leveraging ISO 12100: 2010 and operating it as a design procedure and the subsequent risk reduction measures can be correctly selected.
This chapter discusses how to assess the risk according to ISO 12100: 2010 and then reduce identified risks.

Risk Assessment

The risk assessment identifies machine hazards and specifies the measures to prevent the resulting accidents.
The safety of machines can be determined in 5 steps.
Documentation of the risk assessment process must be kept.



• Step 1 Determination of the limits of machinery

Defining the limits of machinery requires the following points to be considered when assessing risk.

- Requirements for each phase of lifecycle
- Defining the intended use and operation and the reasonably foreseeable misuse and malfunction
- Defining the machine's range of use as limited by factors such as the operator's gender, age, dominant hand, and physical abilities (e.g., impaired eyesight or hearing, size, and strength)
- Expected user training, experience, and competence
- Possibility that people may be exposed to machine hazards
- Possibility that people may be exposed to machine hazards if a
- foreseeable machine hazard occurs

• Step 2 Hazard Identification

Hazard identification means checking for all the hazardous conditions and hazardous events associated with the machine. This involves predicting hazards that may be caused by the machine, such as the following:

- Mechanical hazards: Severing, entanglement, crushing, etc. Electrical hazards: Contact with live parts, static electricity, etc. Thermal hazards: Health disorders due to contact with high temperature parts or working in a high temperature or low temperature environment (refer to the figures on the next page)

Methods for clarifying hazards include the following:

- Check lists
- Hazard and Operability Study (HAZOP)
- Failure Mode and Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)
- "What-if" method

• Step 3 Risk Estimation

The following set of operations are called "Risk Estimation": after checking for hazardous conditions and hazardous events, the risk factors are determined and the risks are estimated from the severity or possible harm and the probability of the hazard occurring. During the risk estimation, risks are estimated as quantitatively as possible against each hazards (including sources appearing unexpectedly as well as lasting sources).

• Step 4 Risk Evaluation

After estimating the risk, the risks are evaluated to determine whether the level of risk must be reduced.
If the level of risk must be reduced, safety measures as described in step 5, such as changing the design or providing safeguards, are taken. Repeat steps 1 to 5 to perform appropriate risk reduction measures for each risk.

• Step 5 Risk Reduction

Taking the following safety measures against each risk is called "Risk Reduction."

- Eliminate or reduce exposure to hazard as far as practical.
- Reduce the probability and severity.
- Use safeguards and safety devices.
- Determine that the performance and functional characteristics of the safety measures are suitable for the machine and its use.

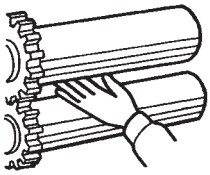
In the next section the measures to achieve the above actions are detailed.

Classifications and Examples

In ISO 12100 2010, Annex B, the following examples are listed as the typical hazards which machines can generally generate.

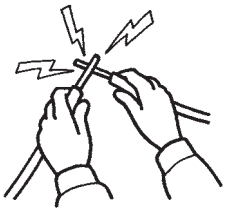
1) Mechanical Hazards

Crushing, entanglement, stabbing or puncturing, shearing, drawing-in or trapping, friction or abrasion, cutting or severing, high-pressure fluid ejection, etc.



2) Electrical Hazards

Contact by a person with live parts, i.e., parts that normally carry a voltage, or parts that have become live under faulty conditions, especially as a result of an insulation failure, etc.

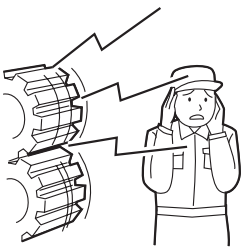


3) Thermal Hazards

Burns and scalds from flames, explosions, radiation from heat sources, etc.

4) Noise Hazards

Hearing loss, tinnitus, etc.



5) Vibration Hazards

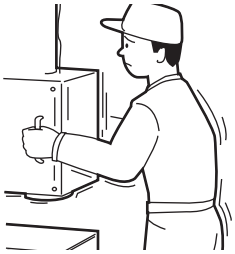
Serious damage to the entire body, particularly to the hands, arms, and lower back.

6) Radiation Hazards

Low frequencies, radio frequencies, ultraviolet, infrared, X-rays, etc.

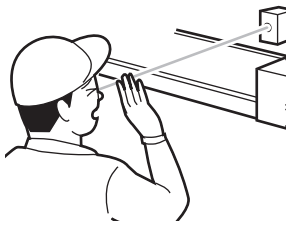
7) Materials and Substances Hazards

Toxins, irritants, dust, explosions, etc.



8) Hazards generated by the neglect of ergonomic principles in the design of machinery

Unhealthy postures, human error, etc.



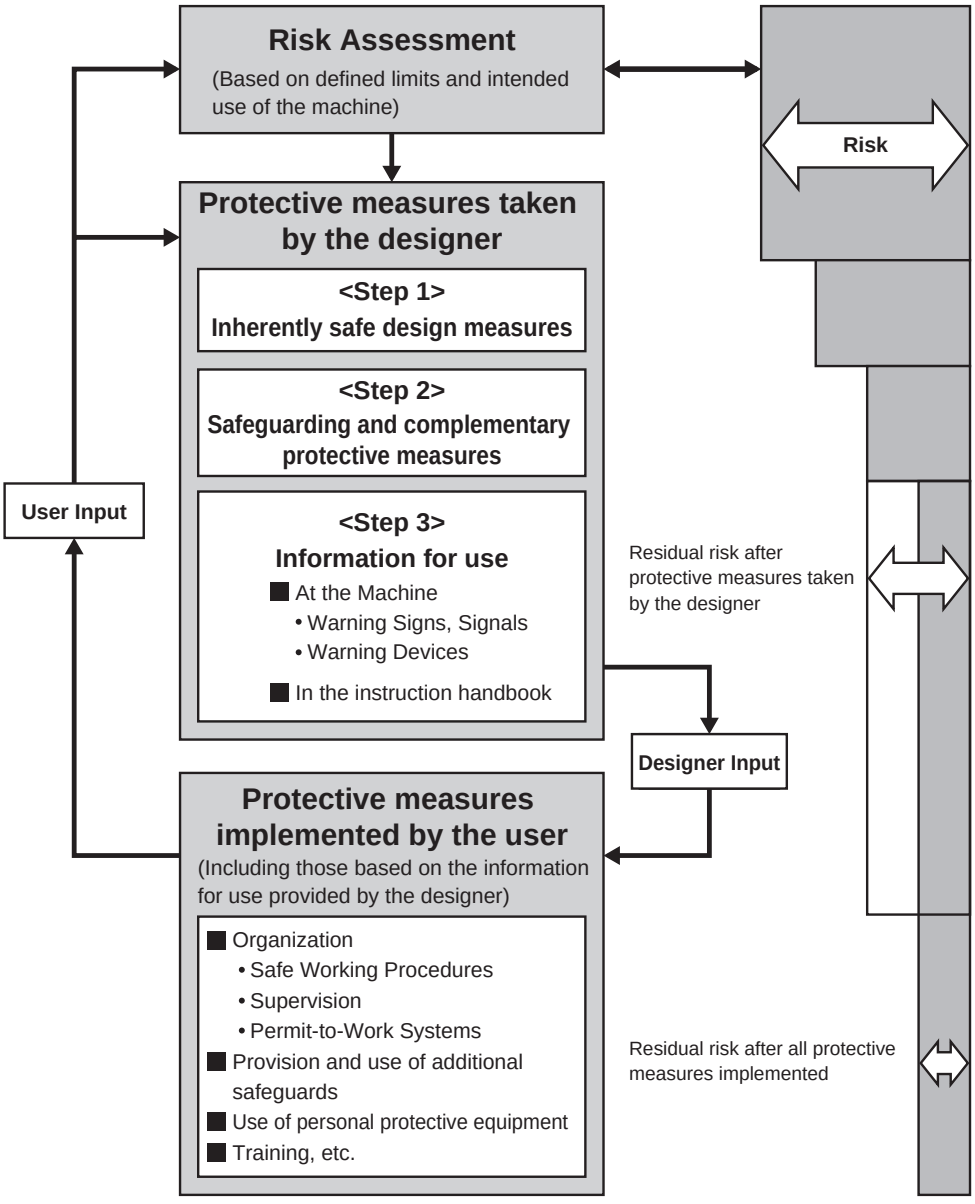
9) Hazards associated with the environment in which the machine is used

10) Combination Hazards

2. Risk Reduction Measures

• Risk Reduction under ISO12100:2010

ISO 12100:2010 is a standard into which ISO 12100-1, ISO 12100-2, and ISO 14121 are integrated.
This standard introduces the basic concept of the designing procedures required for designers to design safe machines.
The introduction of ISO12100-1:2010 states that “The concept of safety of machinery considers the ability of a machine to perform its intended function(s) during its lifecycle where risk has been adequately reduced”. The 3-step method, which is an expression of this methodology for making a work environment where risk has been adequately reduced, has been further implemented into the “Risk Reduction Process” illustrated on the following diagram.
ISO12100:2010 sets out examples of various measures, a sample of which are shown below.

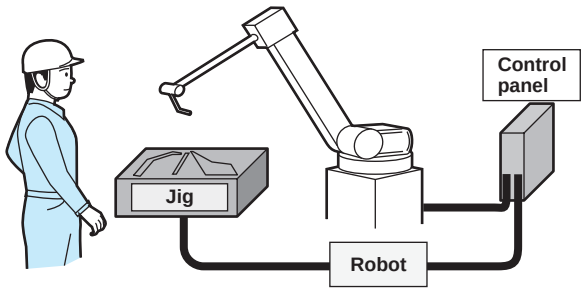


(1) Step 1: What is Inherently Safe Design?

(ISO 12100:2010 6.2)

- Remove hazards and reduce exposure frequency (6.2.1 General)
- Maintain visibility, and avoid dangerous projections and parts (6.2.2.1 Geometric Elements)
- Use alternative materials with few dangers that reduce noise and radiation levels (6.2.2.2 Physical Elements)
- Select appropriate materials (Material quality, stresses, corrosiveness etc.) (6.2.3 General Technical Information on Machine Design)
- Use inherently safe design measures in the below control system (6.2.11)
  - Perform automatic surveillance of safety functions implemented under safeguarding measures (6.2.11.6)
  - Employ diagnostic system to support fault detection (6.2.11.12)
- Use measures listed below that minimize the failure probability of safety functions (6.2.12)
  - Use reliable components (6.2.12.2)
  - Use "oriented failure mode" components (6.2.12.3)
  - Employ redundant systems for components and sub systems (6.2.12.4)
- Automatically limit exposure to hazards (6.2.14)
- Limit exposure to hazards through location of setting and maintenance points outside hazard zones. (6.2.15)

Example: Welding (assembly) robot



- Considerations under the inherently safe design (an example)
  - Ability of robots, optimization of specifications (size, number of control axes, movable range)
  - Positional relation between an operator and robot (mechanical hazards, thermal hazards)
  - Considerations of workability (handling workpieces, repeated operations, manual operations)
  - Optimization for air pressure circuits for jigs (behaviors at restart, residual pressure purge mechanism)
  - Teaching operability for robots (operating procedure, operating position)
  - Safe maintenance (visibility, lockout and tagout of main breaker)

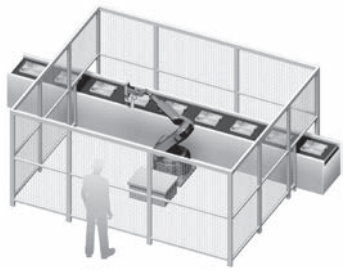
(2) Step 2: What are Safeguarding and complementary protective measures?

(ISO 12100: 2010 6.3)

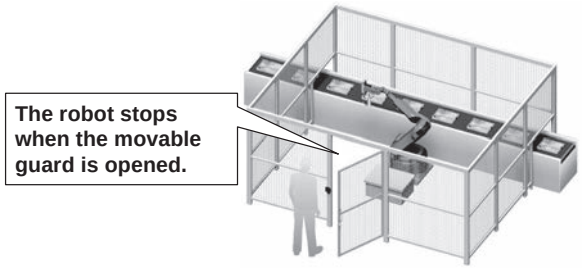
1 Safeguarding

- Employ Sensitive Protective Equipment (Safety Light Curtain, Safety Laser Scanner, Safety Mat, etc.) (5.2.5)
- Employ fixed guards (6.3.3.2.2)
- Employ movable guards (interlocking guard) (6.3.3.2.3)

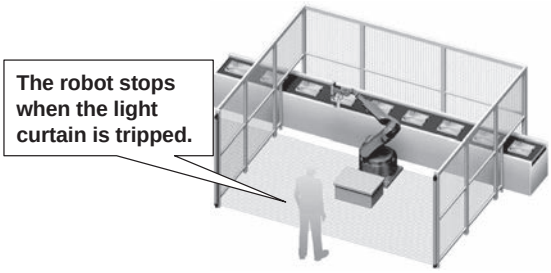
Example 1: Protection with a fixed guard (Isolation principle)



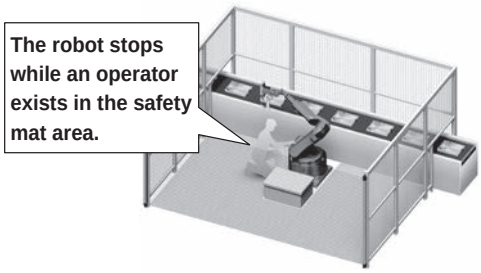
Example 2: Protection with a movable guard and interlock circuit (Stoppage principle)



Example 3: Protection with a safety light curtain and interlock circuit (Stoppage principle)



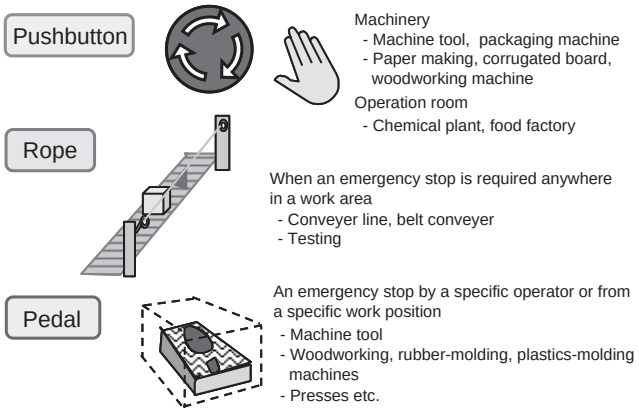
Example 4: Protection with a safety mat and interlock circuit (Stoppage principle)



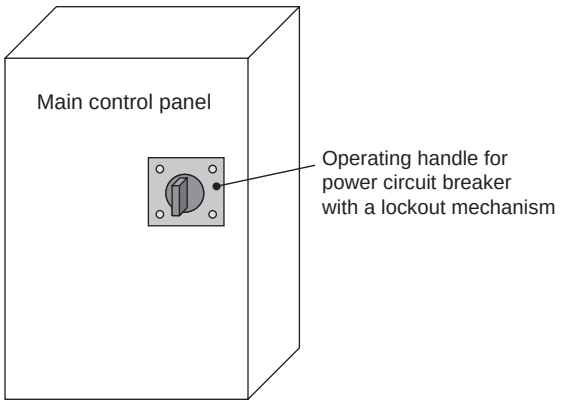
2 Complimentary Protective Measures

- Emergency stop function designed to be clearly identified and quickly applied (6.3.5.2)
- Employ an isolation device that can be locked (6.3.5.4)

Example of emergency stop equipment



Example of isolation device that can be locked

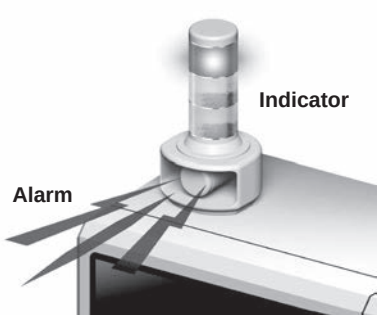


(3) Step 3: What is Information for use?

(ISO 12100: 2010 6.4)

- Supplementary documentation or labels should notify of residual risks, and necessary training, personal protective equipment, and additional protective devices (6.4.1.2)
- Emit an audiovisual warning (6.4.3)
- Display manufacturer, model, and specifications of the machine (6.4.4)
- Supplementary documentation to include storage conditions, mass, dimensions, and installation and disposal methods (6.4.5.1)

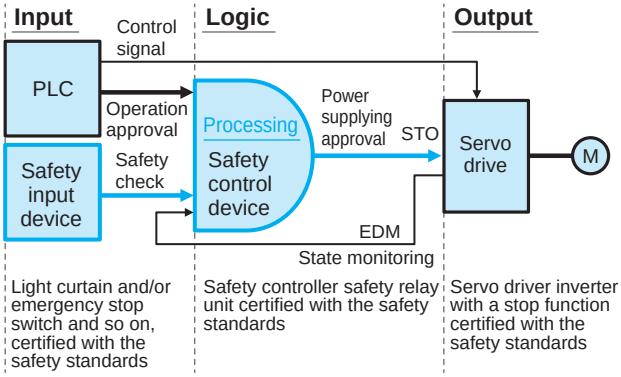
Warning sign (lamp, sound)



Warning label

3. Achievement of Safeguarding Depending on Controlling

(1) What are Safety-related Parts of Control Systems?



The Safety-related Parts of Control System (SRP/CS) implement the function of the safeguarding measures determined in the risk assessment. The Safety-related Parts transfer the operation demands of the safety functions (e.g. guard opening) to the actuator and execute the required operations (e.g. isolating hazardous energy). This transferring path consists of the detection function (I: input device), judging function (L: logical operation device), and power control function (O: output device) and forms a single channel. This is usually called "Safety circuit." When the safeguarding measures determined by the risk assessment are implemented by depending on controlling, the control circuit and all the components used within it are included in the range of a safety-related parts.

Note: The following safety measures that do not depend on controlling are not discussed in this manual. Refer to individual safety standards.
- Purely mechanical inherently safe design (e.g. entanglement prevention by narrowing down opening)
- Physical safeguarding, such as fixed guard
- Risk reduction with administrative measures (e.g. lockout and tagout) and others

MEMO

Chapter 3

Safety Components

The Definition of Safety Components

The need for safety components within safety-related control systems arises when devising basic principles to prevent mechanical accidents and attain safety in machines.

• Definitions in the Machinery Directive

Safety components are defined in the broadest sense as shown below according to Article 2 of the Machinery Directive.

(1) Parts provided to ensure safety functions.
(2) Parts distributed independently within markets.
(3) A part that poses a threat to the safety of operators if damaged or functionally imperfect.
(4) A part that is unnecessary for the machine to work or its function can be achieved with a normal component.

• Items Specified in the Machinery Directive

The following items are designated safety components in the Annex V. Refer to the Machinery Directive for details.

- Protective devices to detect operators
- Power interlock guards related to Annex IV 9 10 11
- Logic units that ensure safety functions
- Emergency stop devices
- Two-hand control devices

• OMRON's View of Safety Components

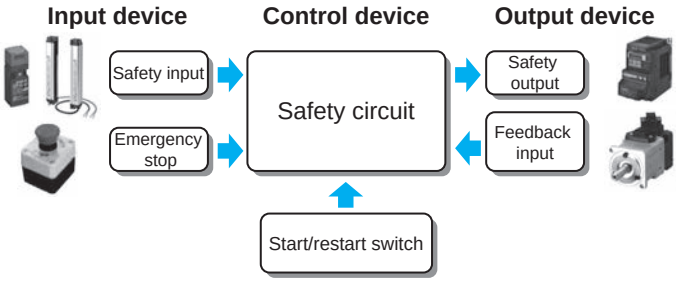
OMRON generically defines safety components as parts in the broadest meaning as previously mentioned as well as safety-related parts that are stipulated for use in safety circuits.

• The Function of Safety Components

Control systems that affect safety must be designed to minimize the possibility of danger occurring even when there is a failure in an interlocking device. Safety devices are equipped with functions such as a direct opening action for switches and a forcibly guided mechanism for relays, as required by standards. These functions are designed to operate correctly within the control system in which they are used.

The following describes safety components that are commonly used to develop safety functions.

<Safety Components>



<OMRON products>

Input Detects state to ensure the safety.


Safety Door Switches


Safety Limit Switches


Safety Light Curtains


Safety Mat


Safety Laser Scanner


Emergency Stop Switch


Enabling Switch

Logic Receives signals from an input device and controls whether the machine should be started or not.


Safety Relay Units


Safety Controllers


Safety Network Controllers


Safety Control Unit

Output Receives signals from a safety controller and shuts off power.


Safety Relays


Servo Motor/Driver


Compact Inverter

1. Interlocking movable guards

These devices prevent workers from entering in hazardous machine areas.
They detect whether or not fences or doors are not opened and, if opened, stop machines before operators are injured.

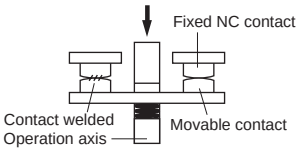
(1) Basic elements of the safety switch

The safety switch has the following functions and structures and ensures safe operation even when there is a failure.
The functions and structures required for the safety switch are as follows:

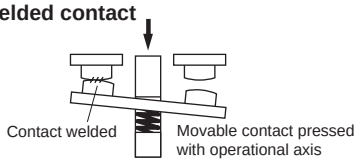
Direct Opening Action (IEC 60947-5-1)

This is a mechanism where contacts can be opened through the pressing operation even if a contact is welded.

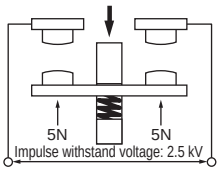
(1) Contact welded



(2) Opening welded contact



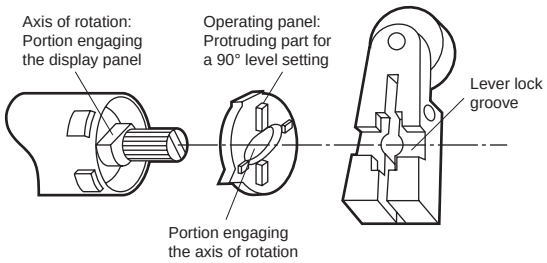
(3) Completed Positive Opening



The contacts must withstand the impulse voltage specified by IEC 60947-5-1 after the contacts have been forcibly opened with the positive operating force (POF) and positive overtravel (POT) exceeding the contact welding force, which is equivalent to 10 N.

Formlock Mechanism of Safety Limit Switch

This is a mechanism that can prevent actuators from failing.
The actuator for the safety limit switch must not be deformed or displaced by a strong force which may be applied on it when a contact is welded so that the positive opening works correctly.
Therefore the safety limit switch has a direct opening action that consists of inelastic, uneven parts engaged with one another. The following figure shows the example of the mechanism with the axis of rotation and the lever.



Note: The lever is secured with uneven parts so that the lever will not fail if a strong force is applied to it. The lever cannot be attached backwards.

Structure not easily defeated

"Defeating" means intentionally disabling the safety effects. The safety switch has a structure not easily defeated.
For more details, see (2) Guard interlock switch.

Safety Door Switch
D4NS

Safety Limit Switch
D4N

(2) Guard Interlock Switch

The guard interlock switch detects that a fence and/or door provided for preventing operators from entering in hazardous machine areas is opened, and stops the machine before operators are injured. Switches such as safety door switch and safety limit switches are classified as the guard interlock switch.

1) Guard Monitoring and Interlocking

Guard monitoring and interlocking switches are one of the most important types of protective devices to prevent dangerous situations by shutting power off from the machine.

When it is decided to protect the machine with protective fences, we must be sure that the only way inside the dangerous area is through the guard. If the guard is opened, a mechanically actuated position detector stops the machine. Every guard in the protective fence must have position detector switches to ensure the safety of personnel. A basic requirement is that it the door is opened, the machine must stop before anyone can reach the hazardous moving parts of the machine.

The most import selection criteria of an interlocking device are:

- the conditions of use and intended use (ISO 12100)
- the hazard present at the machine (ISO 12100)
- the severity of the possible harm
- the probability of failure of the interlocking device
- stopping time and access time considerations
- the frequency of access
- the duration of person's exposure to the hazard
- performance considerations

The position switch shall be actuated in positive mode (for more details, refer to the section "Negative operation and Positive operation"). The break contact of the position switch shall be of the "direct opening action" type. (IEC60947-5-1)

The security of an interlock switch is dependent on its ability to withstand attempts to "cheat" or defeat the mechanism. An interlock switch should be designed so that is cannot be defeated in a simple manner. "Defeating in a simple manner" is an illegal nullification by measures other than valid mode changing procedure using an operating switch etc. For example, the following readily available objects can be used as a defeating tool:

- screws, needles, sheet-metal pieces;
- objects in daily use such as keys, coins, tools required for the intended use of the machine

2) Standards for guard interlock switches (ISO 14119)

ISO 14119 "Interlocking devices associated with guards" provides the designing standards for interlocking devices. To design interlocking switches and interlocking circuits, ISO 13849-1 must be conformed.

3) Requirements for Guard Monitoring

Interlocking guards must ensure that the safety door protects the hazardous area as defined in ISO 12100.
The sensors and the signal processing must comply with all required norms and directives.

- Switches shall be designed to withstand all expected and foreseeable stresses
- Switches shall comply with safety standards, especially, direct opening action and safety door switches shall be completely equipped.
- The principles of redundancy and diversity shall be considered in the mechanical design of switches and signal processing, if necessary.
- Safety-related parts in the associated control circuit must meet at least the required level (PLr) defined in the risk assessment.

4) Requirements for Guard Locking

An interlocking device with a guard locking shall be used when the stopping time is greater than the access time taken by a person to reach the danger zone.

The interlocking device with a guard locking is intended to lock a guard in the closed position and linked to a control system so that:

- the machine cannot operate until the guard is closed and locked;
- the guard remains locked until the risk has passed.

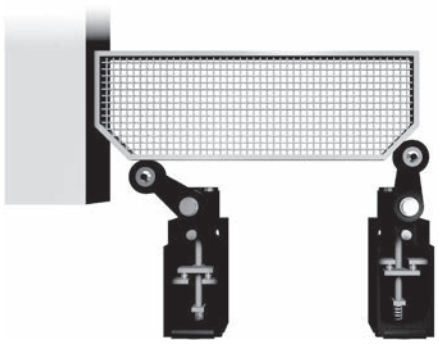
For applications requiring frequent access, the interlocking device shall be chosen to provide the least possible hindrance to the operation of the guard.

Because the guard might be defeated, requirements of intended use, conditions of use, risk assessment and stopping time and access time must be taken into account. In some cases to reduce the frequency of guard opening/closing, the machine processes must be reviewed.

5) Interlocking devices

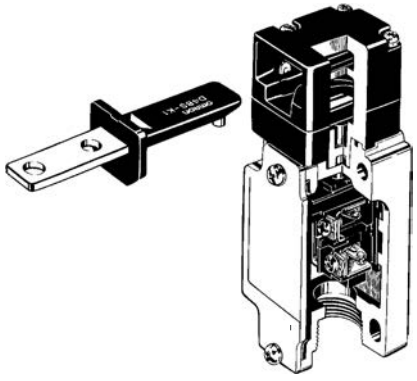
1. Cam operated actuation

When one single safety switch is used it shall be installed to actuate in positive mode to prevent the safety switch from being defeated in a simple manner. A higher level safety protection against defeat can be achieved, e.g., by enclosing the cam and safety switch in the same housing.



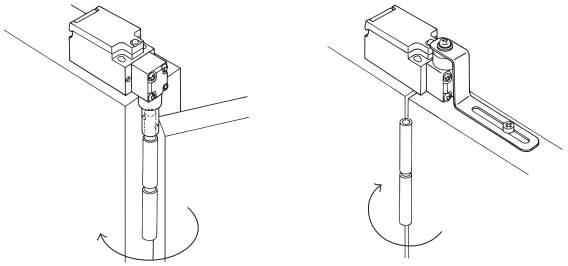
2. Tongue-actuated operation

The tongue-actuated operation switch requires a dedicated tongue and can prevent easy cheating of the switch.
However care should be taken because it can be defeated by using a spare tongue.



3. Hinge operated actuation

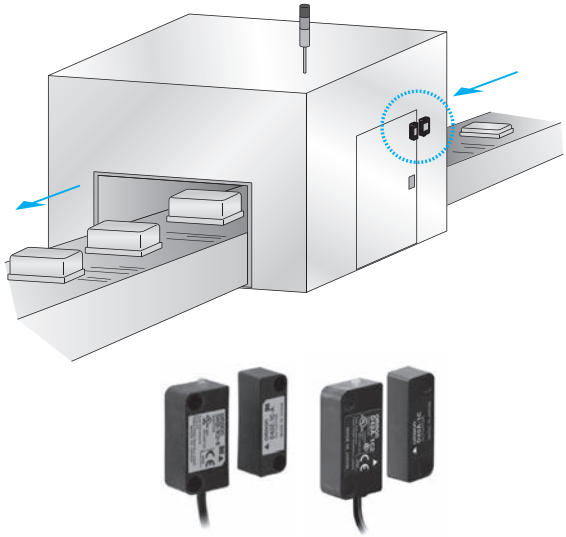
Hinged door switches have two features. One is that it is difficult to defeat the switch. The other is that it can be used for small size guards thanks to no limitation to tongue radius as opposed to operation key operated switches. Prior confirmation is required for very large wide guard doors because a significant gap may be generated when the opening of the door is detected.



Safety-door Hinge Switch
D4NH

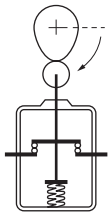
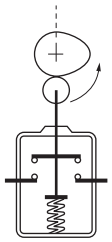
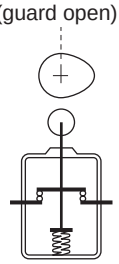
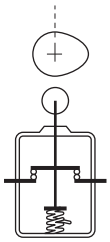
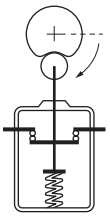
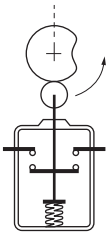
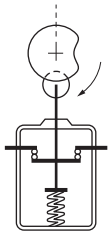
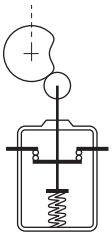
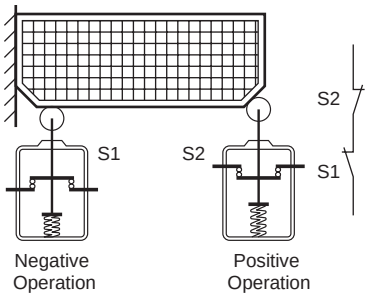
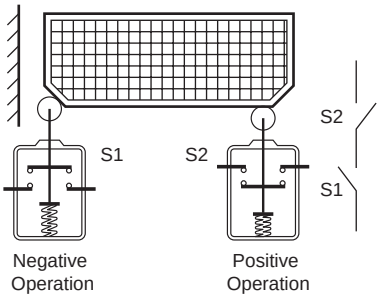
4. Actuation by non-contact method

Non-contact door switches require a dedicated actuator for sensor parts and can prevent the switches from being easily defeated. These switches do not utilize the mechanical operating method as opposed to the cam operated and/or tongue-actuated switches. As a result, they are unlikely to suffer from the mounting limitation compared to the other switches because of the easy positioning during installation.



Compact non-contact Door Switch
D40Z/D40A

Direct and Non-direct Mechanical Action

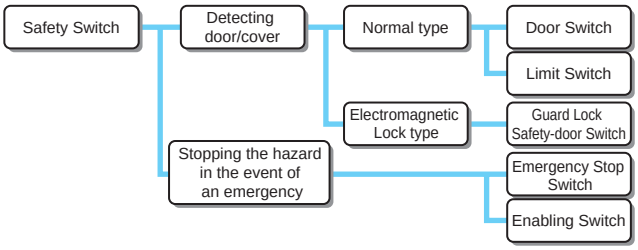
		(A) Non-direct mechanical action		(B) Direct mechanical action		(C) Combined action
Safety		In general, never use non-direct mechanical action switches alone in safety applications.		Direct mechanical action switches are recommended when used alone as the switches offer a higher level of safety than non-direct mechanical action switches.		Switches in combined operation offer an even higher level of safety than direct mechanical action switches alone.
Category		B or 1 (using approved parts)		B, 1, 2, 3, 4		B, 1, 2, 3, 4
		Normal operation	Abnormal operation	Normal operation	Abnormal operation	Normal operation
Operating status		Contacts closed (guard closed)  Contacts open (guard open) 	a) No reset due to contact welding (guard open)  b) No reset due to spring damage (guard open) 	Contacts closed (guard closed)  Contacts open (guard open) 	a) Contact not open due to cam abrasion (guard open)  b) Contact not open due to improper cam position (guard door open) 	Contacts closed (guard closed)  Contacts open (guard open) 
Contact opening methoda		Opened by built-in spring.		Opened directly by externally operating unit like cam or dog.		Opened by a combined action.
Applicable contact		NO contacts		NC contacts (⊖)		NO and NC contacts (⊖)
Characteristics	Pros	The negative operation is a fail-safe operation that ensures safety in case of cam abrasion, improper cam positioning or unexpected cam removal.		The actuator forcibly opens contacts if a contact welds or a spring is broken.		A combined action eliminates the disadvantages of both modes.
	Cons	The actuator may move accidentally with unexpected force and close the contacts. The result may be a relatively dangerous situation.		There is a danger that contacts may close due to cam abrasion, improper cam positioning or unexpected cam removal.		The safety switch circuit may work normally for a while if one of the switches fails to operate.

2. Emergency Stop Device

This is a switch to interrupt machine operations in the event of an emergency.

(1) Emergency Stop Switch

An emergency stop switch is a switch which stops the machinery in the event of an emergency.



1) Types

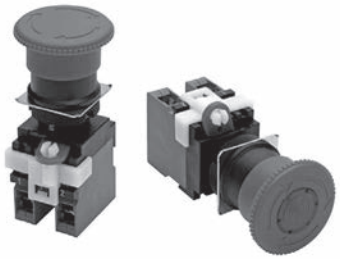
The following are typical types of emergency stop devices:

- A pushbutton switch
- A pull-cord switch

2) Requirements

- Electric contacts must have a direct opening action.
- Emergency stop devices must have a holding function that will mechanically hold in the stop position until the device is manually reset.
- Actuators of an emergency stop device must be colored red and of a mushroom shape. The background immediately behind the actuator must be colored yellow.
- Consideration must be given to the following items when a wire is used as an actuator.

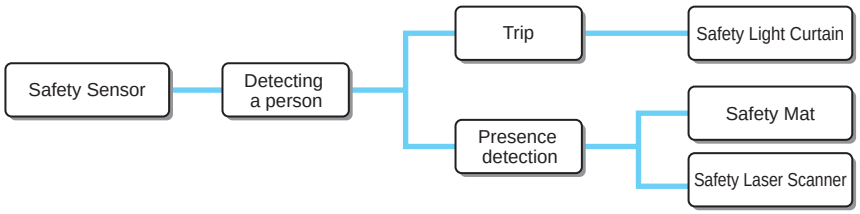
(1) The amount of deflection needed to generate the emergency stop signal
(2) The maximum deflection possible
(3) The minimum clearance between the wire and the nearest machine in the vicinity
(4) The amount of force required for operation
(5) The ease with which an operator can locate the device, by use of a marker flag or other method
(6) The automatic generation of an emergency stop signal in the event that the wire breaks or becomes detached



Emergency Stop Switch
A22E

3. Safety Sensor

Safety sensors are used to stop the machinery when detecting an entry or presence of a person during the machine operation.

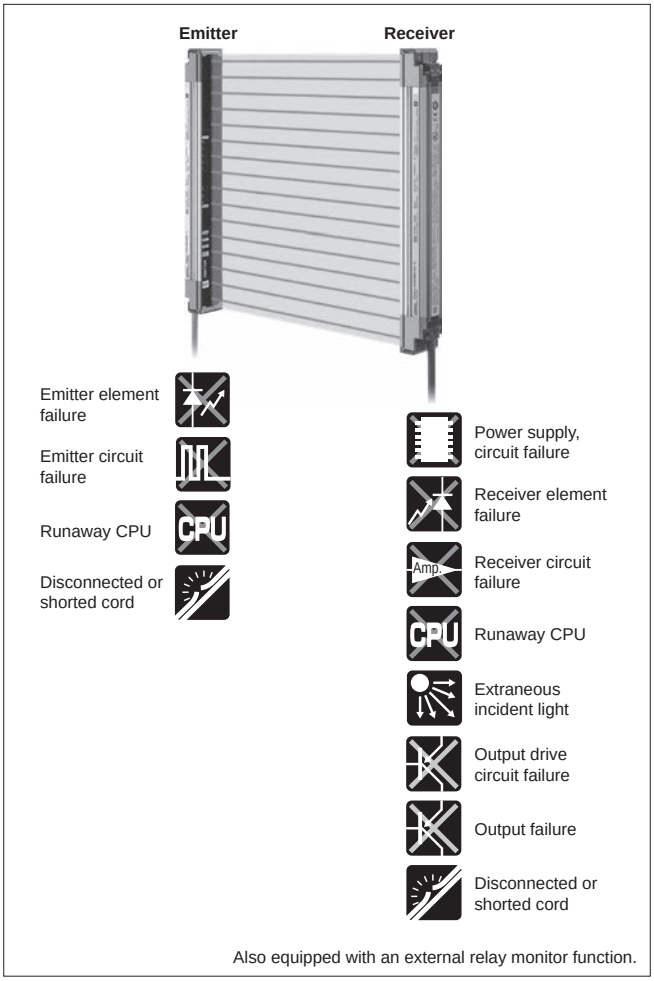


(1) Trip Function

This function stops the machine when detecting entry of a person.

1) Safety Light Curtain

Safety Light Curtain detects operators entering hazard zone by light beams and stops the machine before they are harmed. Unlike ordinary sensors, safety area sensors use a combination of hardware and software to check constantly for internal faults to ensure safe operation.
The following section describes the faults and malfunctions the safety light curtain detects to ensure safety.



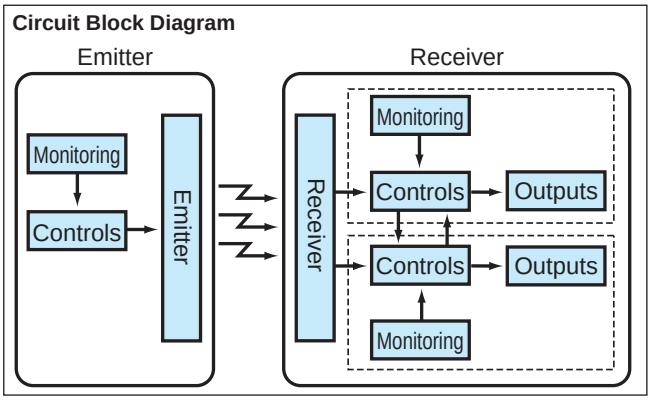
F3SJ Series Safety Light Curtain

1. Diagnostic system

The safety standards for safety area sensors are the same essential health and safety requirements stipulated for safety in the Machinery Directive, and European standards like IEC 61496 ensure compliance with those requirements. IEC 61496-1 stipulates exactly how type 4 sensor will ensure safety for an accumulation of up to three faults. In the safety light curtain safety was designed in by using dual CPUs that check each other as well as by using redundant signal processing and output circuits. FMEA * was also used to demonstrate safe operation and thus maintain safety.

* FMEA: Failure Mode & Effects Analysis

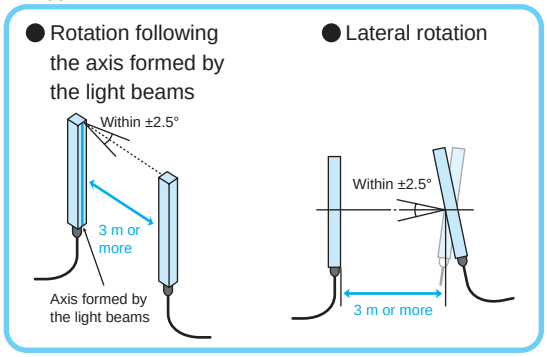
Circuit Block Diagram



2. Effective Aperture Angle

The effective aperture angle is the angle to which area sensors must be rotated to switch the output from ON to OFF. A narrower effective aperture angle is required to minimize the influence of optical reflections.

For type 4



Sensor type	3.0m	1.5m	0.75m	0.5m
Type 2	5°	10°	19.3°	27.7°
Type 4	2.5°	5°	10°	14.7°

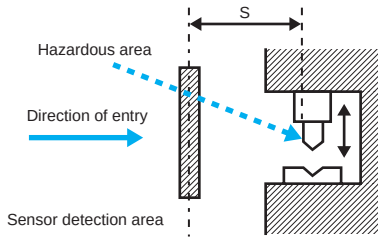
3. Safety Distances

When installing electro-sensitive protective equipment, such as a Safety Light Curtain, the minimum distance that is required to stop the machine before a person who enters the detection zone will reach the machine is stipulated by ISO 13855 and other standards.

• Calculating the minimum distance based on ISO 13855

Minimum distance (S) = Person's approach speed × response time + additional distance due to the sensor's detection capability

A. Vertical approach



Finger or hand detection

• S = (K × T) + 8 (d - 14) d ≤ 40

K = 2,000 mm (assuming entry speed of finger)
T = Machine's maximum stop time + Light Curtain response time
d = Light Curtain's minimum detection object value

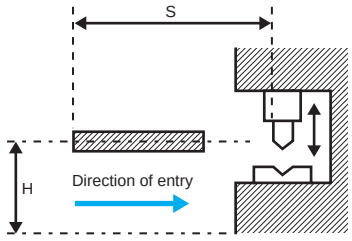
Note: If S = ≤ 100 mm, S = 100 mm
If S = ≥ 500 mm, recalculate with K = 1,600
If the calculation result is S ≤ 500 mm, S = 500 mm

Body detection

• S = (K × T) + 850 40 < d ≤ 70

K = 1,600 mm (assuming person's walking speed)
T = Machine's maximum stop time + Light Curtain response time
C = 850 mm (assuming entry with an outstretched arm)

B. Horizontal approach

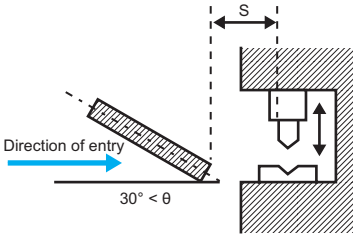


• S = (K × T) + (1,200 − 0.4 H)

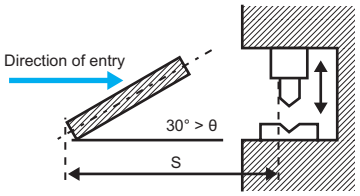
K = 1,600 mm (assuming person's walking speed)
T = Machine's maximum stop time + Light Curtain response time
H = Light Curtain installation height

Note:1. H ≥ 15 (d − 50). However H must not exceed 1,000 mm and drop below 0 mm.
Note:2. If H exceeds 300 mm (200 mm for non-industrial applications), there is a danger of someone slipping under. This must be considered in the risk assessment.
Note:3. When detecting entry with a Safety Mat
S = (1,600 × T) + 1,200

C. Entry at an angle

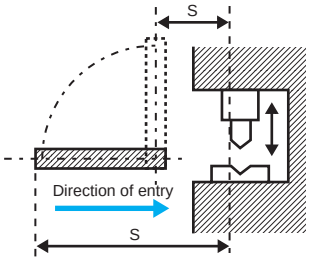


When the installation angle is more than 30°, the entry is generally considered as normal and the vertical approach calculation is applied.



When the installation angle is less than 30°, the entry is generally considered as horizontal and the horizontal approach calculation is applied.

D. Two-point switching device



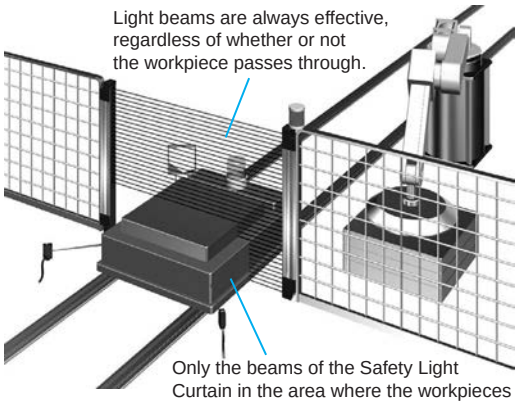
When the installation position is switched, the minimum distance is calculated in response to the resulting conditions

General formula		S = K × T + C
d ≤ 40 mm	100 mm ≤ S ≤ 500 mm	S = (2,000 mm/s × T) + 8 (d - 14 mm)
	S > 500 mm	S = (1,600 mm/s × T) + 8 (d - 14 mm)
40 mm < d ≤ 70 mm		S = (1,600 mm/s × T) + 850 mm
Single beam/Safety mat		S = (1,600 mm/s × T) + 1,200 mm

4. Muting Function (IEC 61496-1)

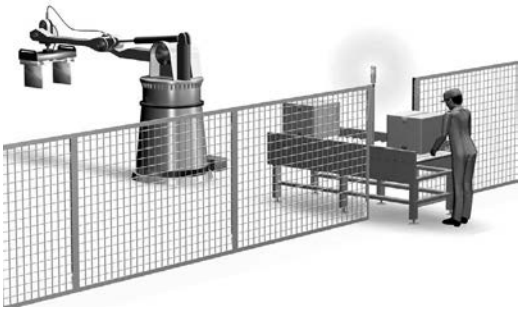
The muting function temporarily stops the detection function of the Safety Light Curtain and automatically keeps it ON regardless of whether the light is incident or tripped.
The muting function can be added to the Safety Light Curtain by connecting the Safety Light Curtain with accessories (F3SJ + Muting Cap).
Conventionally when objects such as AGVs or transport pallets passed through the detection area, the work process was stopped by tripping of the Safety Light Curtain each time they passed. With the addition of the muting function, the safety output can be turned OFF only when a person enters the area, while automatically maintaining the safety output when a workpiece passes through. This makes it possible for work to continue without stopping the production line.
However, when muted, the safety detection function is deactivated, which means that it cannot output an OFF signal to the hazard when a person enters the detection area. Therefore various conditions exist for the methods to install and/or control muting sensors.

Partial muting



Only the beams in the area where the AVG passes through is defeated, and the safety output is turned OFF only when a person enters the area.

Position detection muting



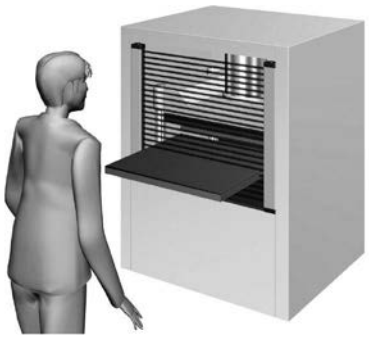
Workpieces can be set without stopping the robot

5. Blanking function

The blanking function is a function to take out zones from the protection field.

Fixed Blanking

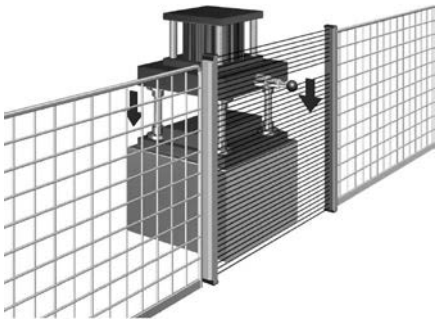
Example:
Invalidating specific beams that are always tripped by the working table.



When the tripping objects is **fixed**:
Possible to be introduced for the machines where the specific objects such as workpieces always trip the light curtain by invalidating the specified beams.

Floating Blanking

Example:
Invalidating beams by the width of workpieces when the beams to be invalidated cannot be specified due to movement up/down of workpieces. If additional beams are tripped, the output will be turned OFF.



When the tripping objects **moves**:
Possible to be introduced for the machines where the specific objects such as workpieces interrupt the light curtain by invalidating the specified beams.

(2) Presence Sensing

This function detects the presence of a person and stops the machine until the person escapes from the hazardous area.

1. Basic Safety

Basic safety is broadly classified into the following categories.
(1) Machines and equipment will not start until it is safe to do so.
(2) Machinery will be stopped whenever a hazardous condition is detected.

In order to maintain a safe environment, measures must be employed on one level to detect operators entering or present in a hazardous area and on another level to eliminate hazardous conditions.

2. Safety Requirements

The safety requirements for presence sensing, such as those shown below, are defined by the standards and guidelines of each country.

- Guidelines Related to the Comprehensive Safety Standards for Machinery: Ministry of Health, Labor and Welfare
  Attached Table 3: Procedure for Safeguarding Against Mechanical Hazards
  A device that will detect operators must be installed in a protected area if an operator can pass through an opening and enter that protected area to perform his job.
- ANSI/RIA R15.06: US robot-related safety standards
  Article 10.4.7 Starting and Restarting
  When an operator is required to enter a protected area, the operator must be protected from inadvertent starting or restarting of the robot and/or robot system. (Part omitted) If the protected area is clearly marked and the cell cannot start or restart, some means of detecting operators in hidden areas must be provided. The ideal means would be automatic detection. (Remainder omitted.)
- EN 201: European safety standards for injection molding machines
  Article 5.3.1
  If an operator can fit between the movable guard and the mold, a device that will detect the presence of the operator must be installed there.

3. Safety Distance

When an operator enters a hazardous area, the machine in the area must come to a complete stop before that operator reaches the hazard of the machine.
Safety distance refers to the minimum calculated distance that the protective device must be installed from the hazard of the machine.

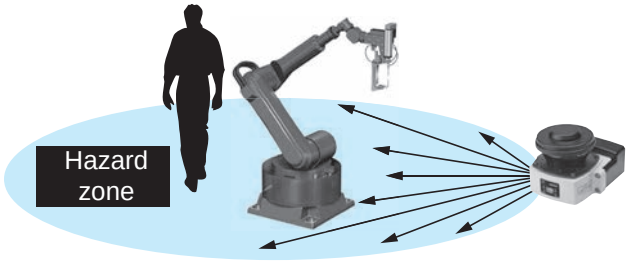
1) Safety Laser Scanner

The sensor detects the presence of an operator in dangerous environments.

Detection Methods

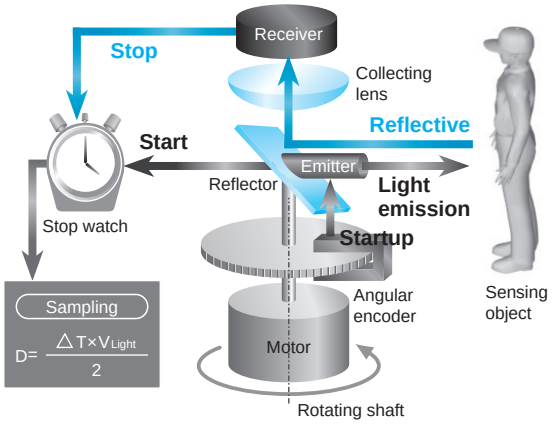
- **Reflective**

Features: Relative freedom in defining protected areas.



- **Active Opto-electronic Protective Device responsive to Diffuse Reflection (IEC 61496-3)**

As shown in the figure below, the laser scanner emits a beam that is reflected by surrounding objects. It calculates the distance to the object from the time that it takes to receive the reflected light.



OS32C Safety Laser Scanner

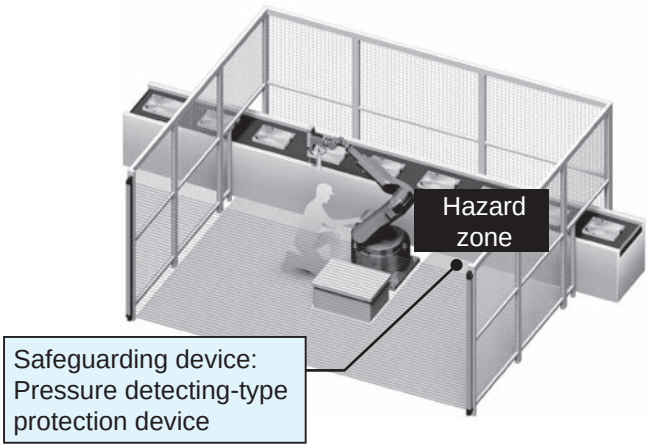
2) Safety Mat

The sensor detects the presence of an operator in dangerous environments.

Detection Methods

- **Pressure detection**

Features: Excellent environmental resistance



- **Pressure detecting-type protection device (ISO 13856-1)**

Two plates inside the Safety Mat make contact when an operator steps on the Mat. A Controller detects the contact and generates an output.

UM/MC3 Safety Mat/Mat Controller

4. Safety Controller

The Safety Controllers receive signals from a safety input device, control whether the machine should be started or not, and notify each device of their determination. They can be broadly categorized into the following four types:

(1) Safety Relay Unit

A typical configuration for the operation control of machinery and equipment is shown in Fig. 1. This is a safety-relay-based control device and suited to single input/single output applications.

• Non-safety-related Parts

The role of non-safety-related parts is to start and continue the operation of devices upon receiving an operate command signal from an automatic control system.

• Safety-related Parts

The role of safety-related parts is to enable operation only when the safety of the machinery and equipment is confirmed.

• Processing

The processing sends an operate signal to a power control element only when it has processed that both the above-mentioned operate command signal, which is sent from a non-safety-related part, and the safety check signal from a safety-related part, which confirms the safety of the machinery, allow operation.

• Processing Elements

The processing element cannot be created by simply combining multiple elements.
Its circuit must incorporate elements that will minimize risks caused by a failure in machinery or equipment. These circuit configuration elements typically include items (1) to (5) shown below.

• Necessity of Safety Relay Units

It is possible to configure a safety-verified circuit by incorporating safety relays with forcibly guided contacts. However, this requires a certain level of technology to configure the circuit and some expense for its certification. As a result, it has become general practice to use standard units that specialized manufacturers have developed by incorporating safety relays. These are provided as a series of Safety Relay Units with proven functional safety.

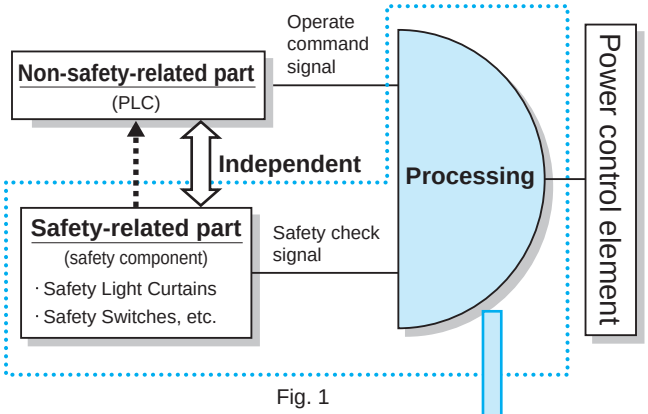


Fig. 1

[Processing Circuit Configuration Example]

When configuring a processing circuit, it is necessary to consider mainly the following circuit configuration measures for minimizing risks caused by a failure in the system.
(1) The use of proven circuit technology and components
(2) Periodical implementation of functional tests
(3) Redundancy
(4) Single fault detection
(5) Short-circuit protection detection

[Relay with Forcibly Guided Contacts]

It is possible to configure a safety-verified circuit by combining safety relays with circuit elements in consideration of the above circuit configuration measures.

However, the following conditions must be satisfied.
(1) A certain level of know-how is required for creating a judging function circuit.
(2) There are expenses involved in obtaining circuit certification.

[Safety Relay Units]

The above problem can be easily solved by using Safety Relay Units because they already have the following.
(1) A safety-verified circuit with built-in safety relays
(2) Circuit certification

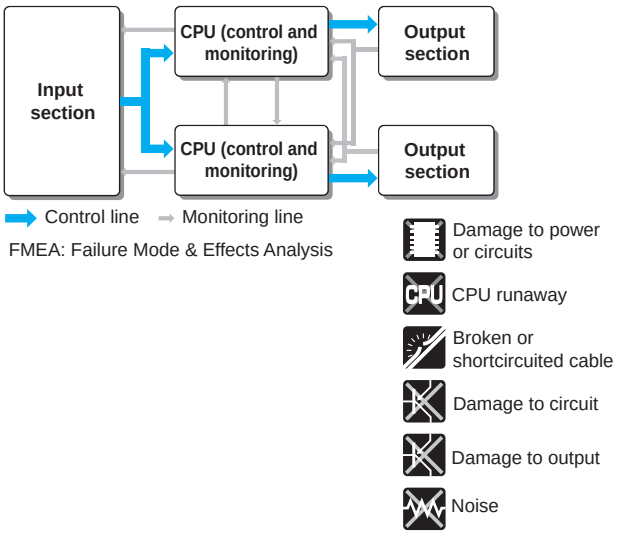
G9SA Safety Relay Unit

(2) Flexible Safety Unit

Electronic units are suited to simple relay sequence configurations for single input/single output applications. In addition the following techniques have been used to handle complicated applications (with multiple inputs and outputs) that are difficult for simple relay sequences.

• Dual CPUs

We pursued safety to the limit to deliver safety and reliability backed by the highest level of safety design and FMEA. Two CPU Units perform mutual checking and diagnostic monitoring of each I/O section, and the safety of operations is further verified by FMEA and process-controlled design and production.



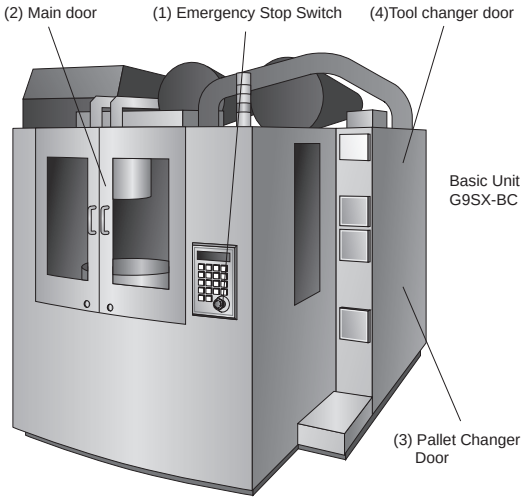
G9SX Flexible Safety Unit

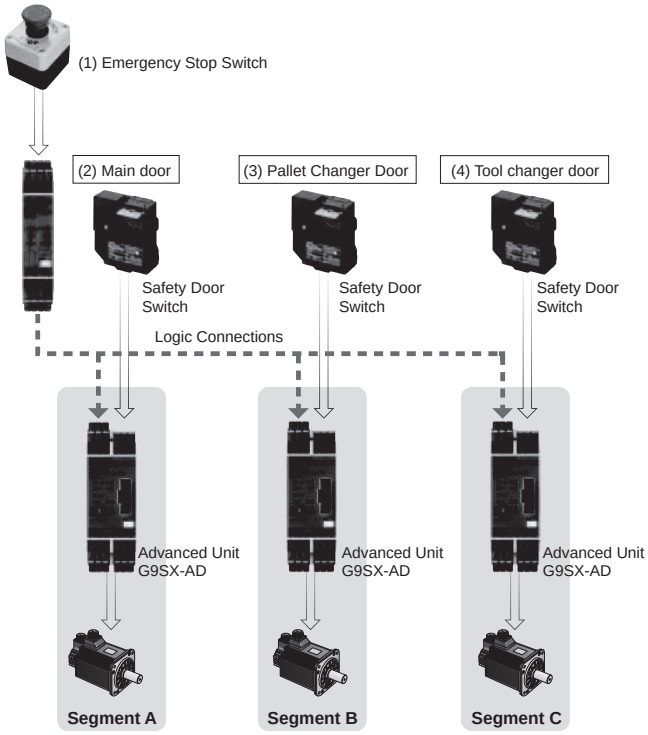
• Effective Functions

1. Logic Connections

For example, when partially stopping each module of a device as well as stopping the entire device are required, they can be achieved by making the AND logic into a function. The logic connection function allows them to be easily achieved and enables flexible response to applications.

- When the Emergency Stop Switch is pressed, the entire machine will stop.
- When a door is open, the corresponding part will not activate.





(3) Safety Controller

By creating safety programs, the designer can more flexibly handle complex applications.
There are, however, some requirements for safety in programming safety circuits.

(1) Preventing User Programming Errors

Safety functions (such as emergency stop buttons and two-hand operating buttons) are provided as verified function blocks to ensure safety at the function block level.
The verification and validation are necessary in addition to the confirmation of the safety of the combination of function blocks to demonstrate final safety as an machinery control system.

(2) Preventing Unintended Operation from Incorrect Wiring

External wiring faults are detected, including incorrect wiring, ground faults, short circuits, and disconnection. Internal circuit faults are also detected.

(3) Preventing Unintended Settings

Checks are performed to ensure that the parameters input by the user are correctly transferred to and set in the devices before automatically enabling starting.

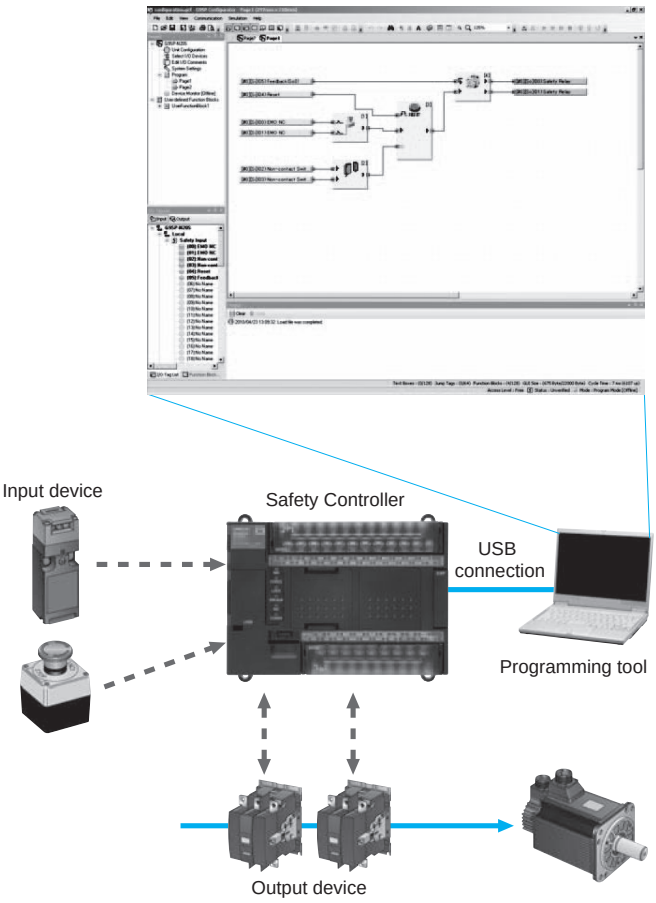
(4) Preventing System Access Except by Administrators

Passwords are set for devices to allow only administrators to change parameters, operating modes, or others aspects of operation.

When designing the safety-related parts, such as equipment and devices, with the programmable safety device, safety validity for software must also be checked.
For more details, see "10. Validation for Programmable Devices" in Chapter 5.

G9SP Safety Controller

Connection example



(4) Safety Network Controller

Networking

Creating networks for safety circuits enables applications that require distributing safety devices, as well as expansion of I/O capacity.
The following four measures are taken in implementing safety circuit networks.

(1) Checking Communications Data (System Redundancy)

Redundancy is implemented for safety data by sending inverted data together with safety data and checking response messages sent from destinations to improve safety.

(2) Special Check Code for Safety Data (Safety-CRC)

Check codes called Safety-CRC are attached to the safety data to ensure that any message corruption and/or impersonation are detected.

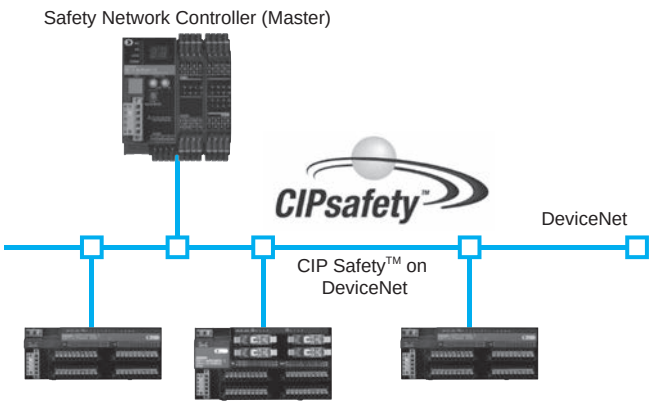
(3) IDs for Transmitters and Receivers

Mutually monitoring safety devices' unique ID code and/or implementing an unique ID code into the transferred data prevent data communications between incorrect devices.

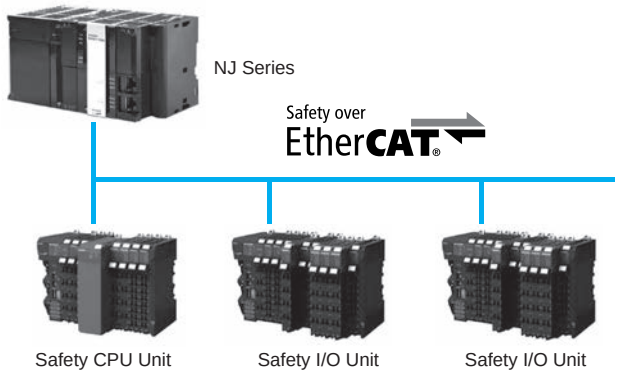
(4) Data Time Management

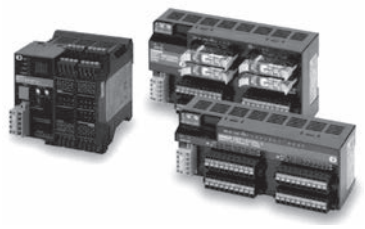
Reversed or late communications data are monitored by attaching time stamps by the safety devices to data they send and/or detecting the data reception time by destination nodes of transferred data.

CIP Safety™ on DeviceNet

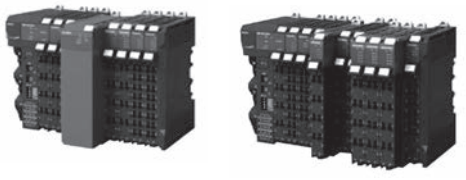


Safety over EtherCAT (FSoE)





NE1A/DST1 Safety Network Controller



NX Series Safety Control Unit

5. Safety-related Operating Switches

These switches maintains safety areas and/or safe conditions by sending safety signals via controllers through manual operations.

(1) Mode Selector

These switches change the machines from operation mode to maintenance mode during machine maintenance, setup, cleaning and others to ensure the safety of operators.
In IEC 60204-1 (JIS B9960-1), if operation mode is explicitly changed and the safety function and/or safety measures are interrupted, a mode change is required. In this case, the safety of operators suitable for operation mode is ensured by combining with the safety controller.

A22TK Safety Key Selector

(2) Two-hand Controller

One way to prevent operators from approaching hazardous areas too closely when conditions are hazardous is to install two-hand controllers at specified locations.
In this case a controller supporting two-hand controllers shall be used.

1) Standards for the two-hand controllers: ISO 13851

The guidelines for designing Two-hand Controllers are given in ISO13851. The major safety requirements for Controller design are listed there under Functional Aspects and Principles of Design for Two-hand Controllers.

Note: Conduct actual designing in compliance with the detailed stipulations of ISO 13851.

2) Main Characteristics

The characteristics that must be provided are categorized by type into Type I, Type II, and Type III categories. The major characteristics listed here are Type III characteristics used in Category 3 and 4, as determined by risk assessment.

(1) Two hands must be used together to start up the machine.
(2) Two input signals are required to produce an output signal.
(3) The output signal must turn OFF if either or both input signals turn OFF.
(4) The output signal cannot be restarted until the both signals are turned OFF.
(5) Both input signals must turn ON within 0.5 s to enable synchronous startup output.
(6) Prevention of accidental actuation and of defeat: Refer to Article 3.

3) Preventing Accidental Actuation and of Defeat

1. Prevention of defeat using one hand

The two startup switches must be at least 260 mm (inside dimensions laterally) apart.

Note: A shield must be installed between the two controllers. This does not apply to applications where inadvertent startup prevention is possible.

2. Prevention of defeat using the hand and elbow of the same arm

The two controllers must be at least 550 mm (inside dimensions laterally) apart.

Note: A shield must be installed between the two operation devices. This does not apply to applications where inadvertent startup prevention is possible.

3. Prevention of defeat using the forearm(s) or elbow(s)

Install a cover or enclosure.

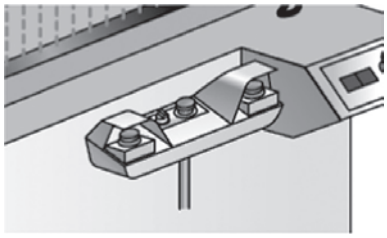
4. Prevention of defeat using one hand and any other part of the body

Install the controllers at least 1,100 mm off the floor or from the operating level to prevent operators from employing inadvertent startup prevention with one hand and another part of the body (e.g. knees, hips, etc.).

Note: Safety Distance
The safety distance from the startup switches to the hazardous area must be calculated using factors such as hand and arm speed, response time of the startup switches, and maximum time required to eliminate a hazard according to ISO 13855.

5. Typical Example

Fig. 1 shows a typical example of a Two-hand Controller according to Articles 2) and 3).



G9SA-TH Two-hand Controller

(3) Enabling Switches

An enabling switch is a safety component used so that various hazards such as inadvertent entanglement can be avoided or reduced when performing non-scheduled maintenance work or other non-scheduled operations in hazardous areas, such as those inside safety fences.

When an operator is using a hand-held console with operation switches to teach a robot, retool, or perform maintenance, unexpected movement of a hazard and/or operator's inadvertent behaviors can result in a hazardous state. In a such situation, it's impossible to predict whether the operator will instinctively release the console or will grip it with force.

A normal switch thus does not turn OFF when excessive force is applied, which may result in an operator accident. With an Enabling Switch, machines or robots can be controlled only when the switch is gripped lightly to the middle position. If the switch is gripped with force past the middle position or if the switch is released, the machine or robot will be shut OFF, disabling operation.

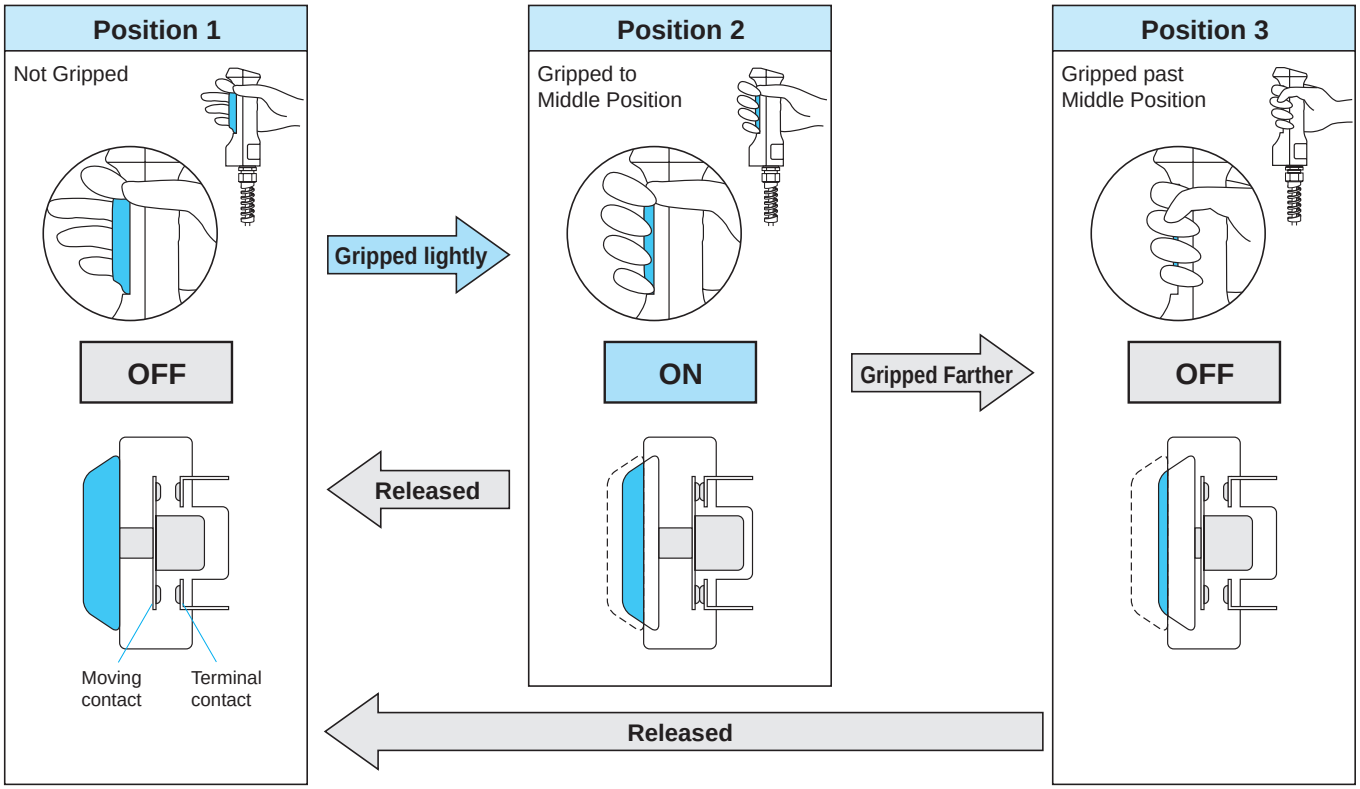
Enabling Switches are normally used built into teaching pendants, grip switches, and other hand-held controls. They can be combined with safety circuits built with Safety Relay Units and other devices to ensure safety.

A4EG Enabling Grip Switch

1) Structure of Enabling Switches

Enabling Switches operate through three positions: OFF - ON - OFF.
They are OFF when not pressed, ON when pressed to the middle position, and then OFF again when pressed past the middle position.

- Three Positions: OFF - ON - OFF



6. Safety Relays

Unlike other relays, safety relays has the function to detect its welding state and allow determination by the control circuit if contacts are welded together because they have forcibly guided (linked) contacts (EN 50205).

Note: Welding cannot be pulled apart.

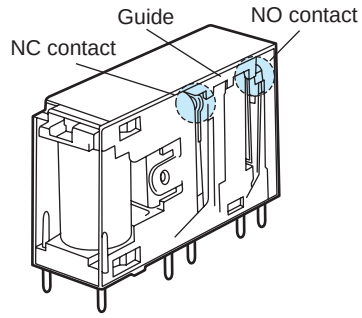
1) Main Safety Relay Requirements

The gap between contacts must be at least 0.5 mm during normal operation or when a fault occurs. For more details, see 3).

Contact load switching must conform to AC-15 and DC-13 (IEC 60947-5-1).

The mechanical service life must be at least 10 million operations.

2) Forcibly Guided (Linked) Contact Structure



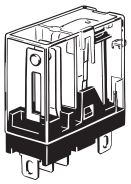
If at least one normally open contact is welded, when the coil is deenergized, all normally closed contacts maintain a gap of at least 0.5 mm.

Even if a normally closed contact is welded, all normally open contacts maintain a gap of at least 0.5 mm in the coil energized mode (in accordance with EN 50205).

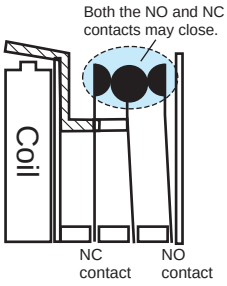
Relays in which all the contacts are linked by forced guide are called Type A and indicated by the mark.

3) Structural Comparison of General Relays and Relays with Forcibly Guided Contacts

General Relay

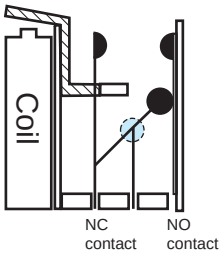


G2R Structure
(Coil: Not energized)



(a) When contact welding occurs

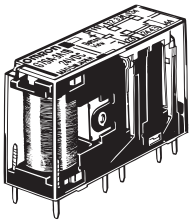
G2R Structure
(Coil: Not energized)



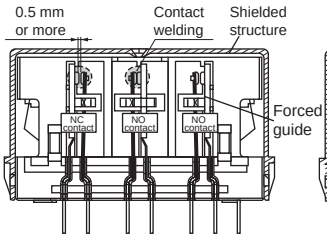
・A broken movable spring may cause a short-circuit between electrodes

(b) When a movable spring is broken

Relay with Forcibly Guided Contact

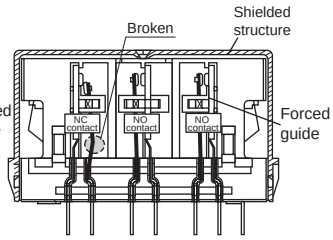


G7SA Structure
(Coil: Not energized)



(a) When contact welding occurs in the NO contacts
(The NO contacts will not close if contact welding occurs in the NC contacts.)

G7SA Structure
(Coil: Not energized)

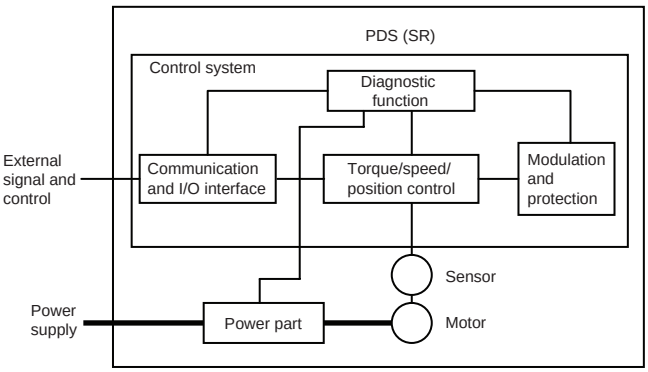


・The above shielded structure protects other contacts from being affected by the failure.

(b) When a contact spring is broken (broken NC contacts)

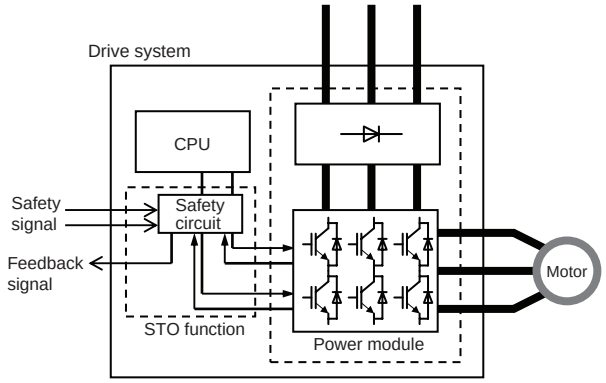
7. Drive Devices Equipped with the Safety Function

The safety functions for drive devices are defined in IEC 61800-5-2. The following figure shows the range of the safety-related parts (PDS (SR)) of the electric-power drive systems.

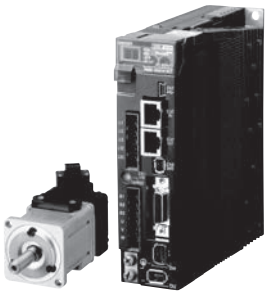


Block diagram for PDS (SR)

STO (Safe Torque Off) function, which is a typical safety function, is explained here.
As shown in the following figure, STO cuts off the power, which generates turning forces (thrust) of the motor, from the motor.
In STO additional measures, such as mechanical brakes, may be required because the stop state is not controlled. In addition, when a driver/motor should be accessed for maintenance and others, disconnection from the power source using devices such as breaker and contactor is required because STO does not have an electric-shock prevention function.



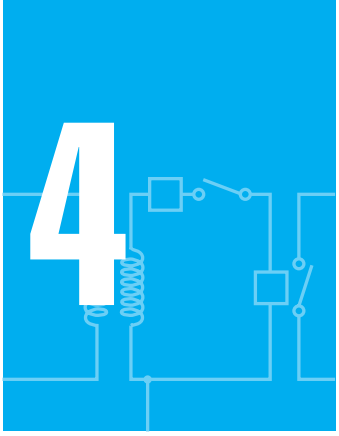
OMRON products implementing STO function



G5 Series AC Servo Motor/Servo Drives

MX2 Series V1 Type Multi-function Compact Inverter

MEMO



Chapter 4

Safety Circuit Examples

1. Index

2. Precautions

1. Circuit Configurations for Safety-related Applications

A variety of connection examples for interlocking devices are presented here, divided into categories and PL combinations. These examples 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 standards in the following table, and any related standards, when designing and implementing circuit configurations, while also receiving confirmation from a third-party verification organization for the safety of the overall system.

Standards Number	Title
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	Safety-related parts of control systems -- Part 1: General principles for design
ISO 13849-2	Safety-related parts of control systems -- Part 2: Validation

Note: In some situations, it is also necessary to refer to other standards.

2. Determining PLr

PLr, which is a performance indicator of safety measures, is determined as a result of a risk assessment. To determine the actual PLr of safety-related parts, it is necessary to determine the PLr that is applicable to the entire machine by evaluating the machine specifications and the machine's equipment, usage, and operating environment for the duration of its service life.

3. About 2-channel Input

Applications in which the open/closed status of a guard is confirmed by the contact signals of position detection equipment such as Safety Door Switches need to be considered.
It is possible to provide 2-channel input of the open/closed confirmation signal to the Controller by using two contacts inside a single position detection unit. However, when this is done, an incorrectly inserted tongue or a certain degree of impact may damage the head of the position detection equipment, with the result in common cause failures on both output signals. The method for selecting 2-channel input depends largely on the risk assessment results for the entire system, but it is recommended that two position detection units with a reciprocal mode be used for a single door to ensure correct confirmation of the open/closed status of guards. Parts selection as well as category selection are important as ISO/TR 23849: 2010-7.2.2.5 describes that achievement of PLe using two contacts inside a single position detection unit is in general impossible. For more details, see ISO/TR 23849, ISO 14119, each C standard, and others.

4. The Role of Safety Components

Safety-related control systems must minimize the possibility of danger occurring even when there is a failure in the 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 control system 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.
Particularly you must use clamps, couplings, etc., to secure doors fitted with a guard lock safety-door switch. When a switch is used as a direct guard lock, errors in the guard lock safety-door switch functions can occur due to the weight of the guard itself, vibration from machinery, or impacts during erroneous door opening/closing in holding status.

6. Detecting Trip and Presence

The basic feature of the Safety Light Curtain is to detect the tripping of a person's finger, hand, or body. When it is necessary to have a presence-detecting function in a hazardous area in response to the overall system risk assessment, e.g., due to frequent entry in the hazardous area, it is recommended that the Safety Light Curtain be used together with a Safety Mat, Safety Laser Scanner, or similar device. Refer to Chapter 3-3 "(2) Presence Sensing" for information on presence sensing.

7. Reset Methods

These connection examples use manual resetting.
In order to use an auto reset method, the dimensions from the opening to the hazard must be such that they will not allow a person to reach the hazard. For information on the connection for a system using an auto reset method, refer to the connection circuit examples in the relevant product catalog. Refer to ISO 12100:2010 6.3.2.5.3, to use auto reset and/or auto restart methods.

8. Contactors

It is recommended that the auxiliary NC contacts used as monitors for main contact welding be equipped with a function to prevent the same failure.

Note: As of Jan., 2014. These cautions are subject to change if required due to various reasons such as improvements of the specifications of products or accessories described in this manual.

3. Conditions for PL Evaluation

In the Circuit Diagram examples described in this manual, PL is assessed for the following requirements using the following models. However the models and PL assessment results are only an example. In the production circuits, you must assess PLs independently based on the actual requirements.

Device	Safety function (Safety component)	Assumed usage and frequency of operation demands	Number of operation demanded per year (Nop) When operating time is assumed as 12 hours per day for 220 days per year.	Reliability Data for Safety of Machinery
Input device	Emergency stop switch	Operation for inspection at shift start time (approx. twice per day)	500	Reliability Data for Safety of Machinery for each product (see the following:) If there is no applicable item, select one from ISO 13849-1: 2006 Annex C, Table C1 (refer to "International Standards dealing with MTTFd or B10d for components (quoted from ISO 13849-1: 2006 Annex C)").
	Safety limit switch (when used for guard interlocking)	Slightly frequent taking out of workpieces (approx. 125 times per day)	27,500	
	Safety door switch without guard lock function (including non-contact type door switches)	Taking out of workpieces (approx. 100 per day)	22,000	
	Guard lock safety-door switch	Maintenance, inspection, cleaning or others (approx. 50 per day)	11,000	
	Safety light curtain/multi-beam sensor/single-beam sensor	Slightly frequent taking out of workpieces (approx. 125 per day)	27,500	
	Two-hand control device	Slightly frequent taking out of workpieces (approx. 125 per day)	27,500	
	Safety laser scanner/safety mat	Maintenance, inspection, cleaning or others (approx. 50 per day)	11,000	
	Enabling switch/enabling grip switch	Retool or others (approx. twice per day)	500	
Control device	Safety relay	Safety functions are performed when the operation demand from the input device is detected.	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.	Safety functions are performed when the operation demand from the input device is detected.	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.			

4. Reliability Data for Safety of Machinery for OMRON Products

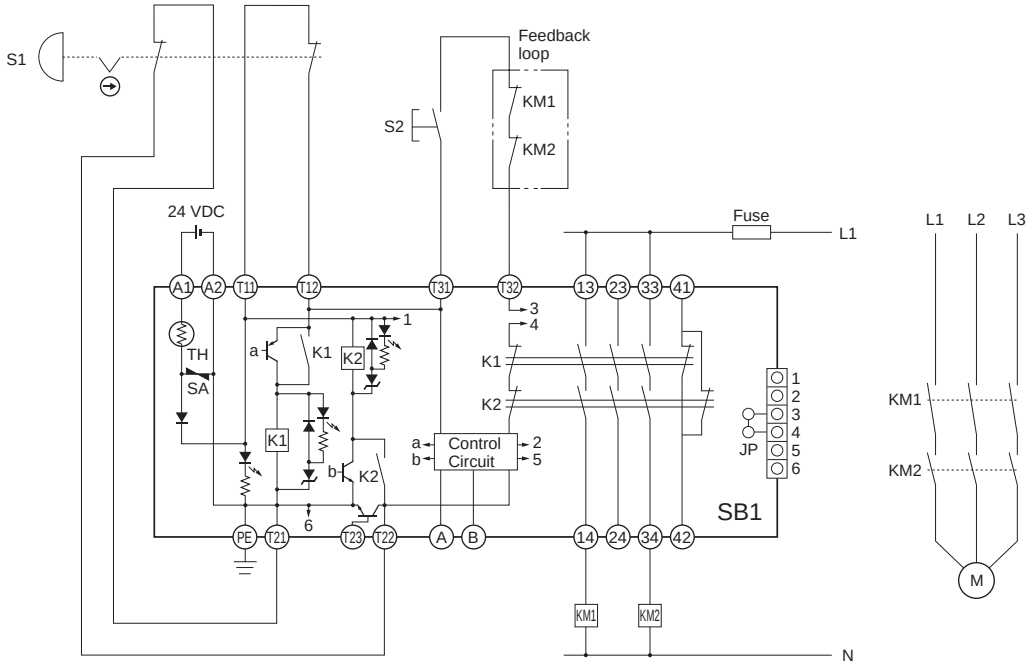
OMRON provides reliability data for safety of machinery for each product category by means of the parameter list (PDF file) and SISTEMA dedicated library to help customers to calculate PL of their devices.
Refer to our web site (www.ia.omron.com).

MEMO

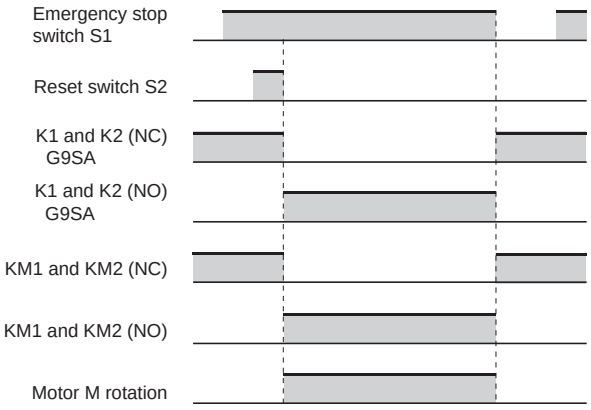
Connection Example 1: Emergency Stop Switch

• Safety Functions

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



• Timing Chart



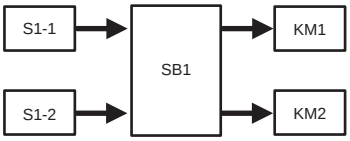
Note:1. Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.
Note:2. Use manual resetting for the emergency stop circuit. (ISO 13850)

• Model used and machinery safety reliability data

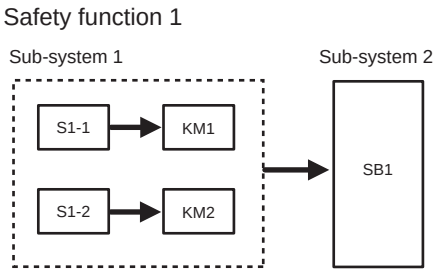
Symbol	Model used	Machinery safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B10d: 100,000
S2	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
SB1	Safety Relay Unit G9SA-301 (PLe certified on ISO 13849-1)	Category 4, MTTFd: 100 years, DCavg: 99%
KM1/KM2	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

• Developed logical block diagram

Electrical block diagram of safety-related parts



Developed logical block diagram



• PL of Safety-related Part

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	S1-1, S1-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d = 2,000,000 DC = 99%, nop = 500/year	4	100	99	2.47×10^{-8} *2	e
	2	SB1 (G9SA-301)		4	100	99	2.47×10^{-8} *2	e
	PFHd and PL for the entire safety-related parts						4.94×10^{-8}	e

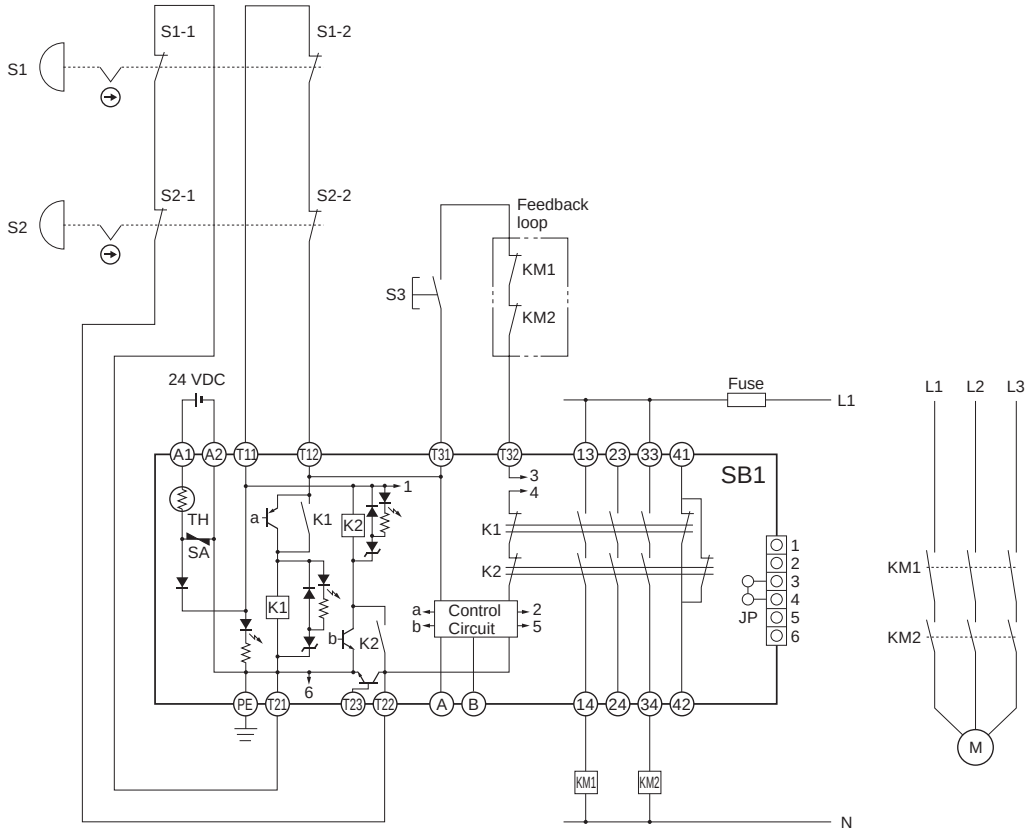
*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

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

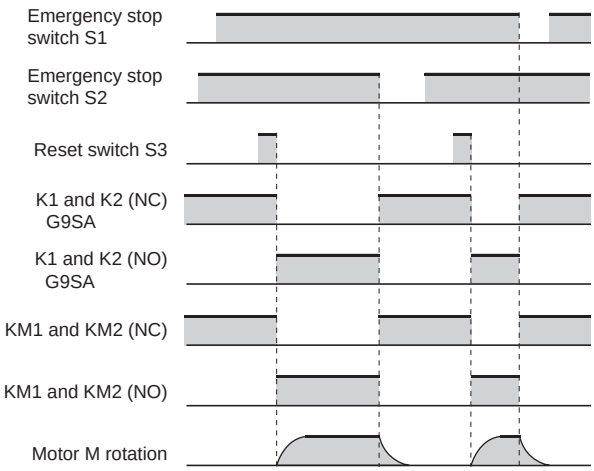
Connection Example 2: Emergency Stop Switch x 2

• Safety Functions

Safety function	Operation	Stop method	Restart method
1	• Immediately removes power to Motor M when Emergency Stop Switch S1 is pressed. • The power to Motor M is kept removed until the latch of the Emergency Stop Switch is released and Reset Switch S3 is pressed.	Stop category 0	Manual
2	• Immediately removes power to Motor M when Emergency Stop Switch S2 is pressed. • The power to Motor M is kept removed until the latch of the Emergency Stop Switch is released and Reset Switch S3 is pressed.	Stop category 0	Manual



• Timing Chart



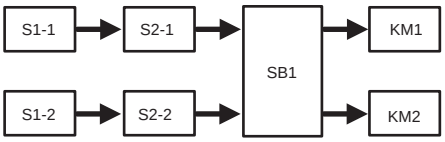
Note:1. Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.
Note:2. Use manual resetting for the emergency stop circuit. (ISO 13850)

• 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)	B10d: 100,000
S2-1/S2-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B10d: 100,000
S3	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
SB1	Safety Relay Unit G9SA-301 (PLe certified on ISO 13849-1)	Category 4, MTTFd: 100 years, DCavg: 99%
KM1/KM2	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

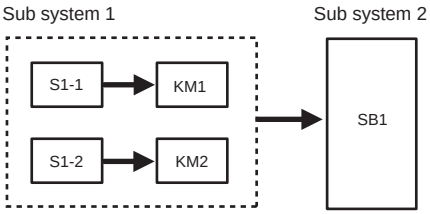
• Developed block diagram

Electrical block diagram of safety-related parts

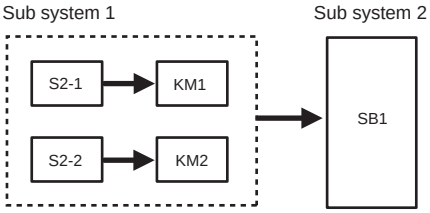


Developed logical block diagram

Safety function 1



Safety function 2



• PL of safety-related parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	S1-1, S1-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC = 99%, nop = 11,000/year	3	100	90	4.29×10^{-8} *2	e
	2	SB1 (G9SA-301)		4	100	99	2.47×10^{-8} *2	e
	PFHd and PL for the entire safety-related parts						4.94×10^{-8}	e
2	1	S2-1, S2-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=1,000/year	3	100	90	4.29×10^{-8} *2	e
	2	SB1 (G9SA-301)		4	100	99	2.47×10^{-8} *2	e
	PFHd and PL for the entire safety-related parts						4.94×10^{-8}	e

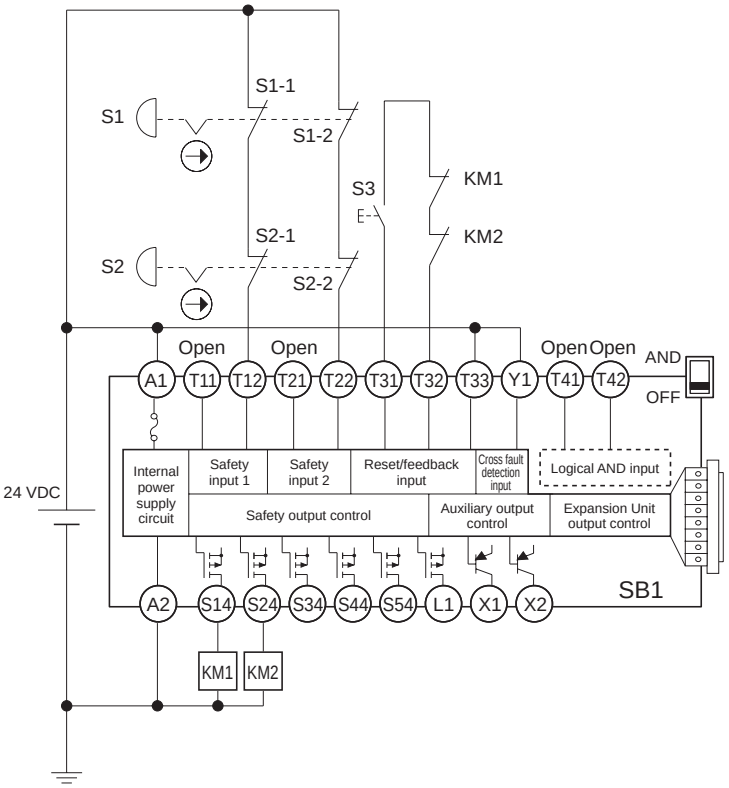
*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

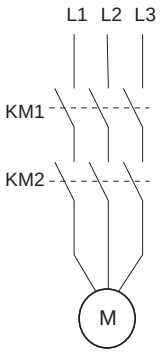
Note: The point of CCF shall be at least 65.

Connection Example 3: Emergency Stop Switch x 2

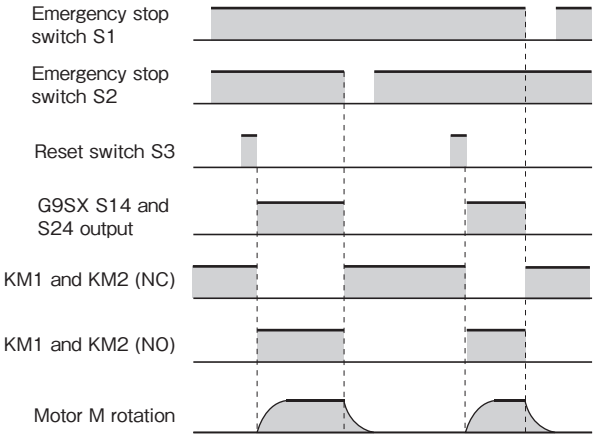
• Safety function

Safety function	Operation	Stop method	Restart method
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 latch of the Emergency Stop Switch is released and Reset Switch S3 is pressed.	Stop category 0	Manual
2	• Immediately removes power to Motor M when Emergency Stop Switch S2 is pressed. • The power to Motor M is kept removed until the latch of the Emergency Stop Switch is released and Reset Switch S3 is pressed.	Stop category 0	Manual





• Timing Chart



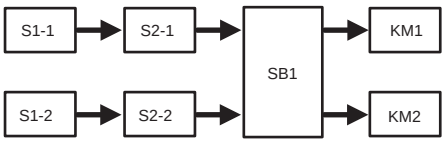
Note:1. Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.
Note:2. Use manual resetting for the emergency stop circuit.

• 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)	B10d: 100,000
S2-1/S2-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B10d: 100,000
S3	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
SB1	Flexible Safety Unit G9SX-AD322-T15 (IEC 61508 SIL3 certified)	PFHd: 5.70×10^{-9}
KM1/KM2	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

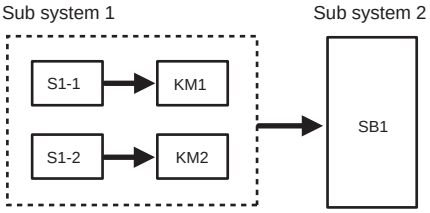
• Developed block diagram

Electrical block diagram of safety-related parts

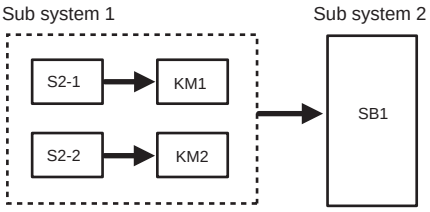


Developed logical block diagram

Safety function 1



Safety function 2



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	S1-1, S1-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=1,000/year	3	100	90	4.29×10^{-8} *2	e
	2	SB1 (G9SX-AD322-T15)		4	-	-	5.70×10^{-9}	e (SIL3)
	PFHd and PL for the entire safety-related parts						4.86×10^{-8}	e
2	1	S2-1, S2-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=1,000/year	3	100	90	4.29×10^{-8} *2	e
	2	SB1 (G9SX-AD322-T15)		4	-	-	5.70×10^{-9}	e (SIL3)
	PFHd and PL for the entire safety-related parts						4.86×10^{-8}	e

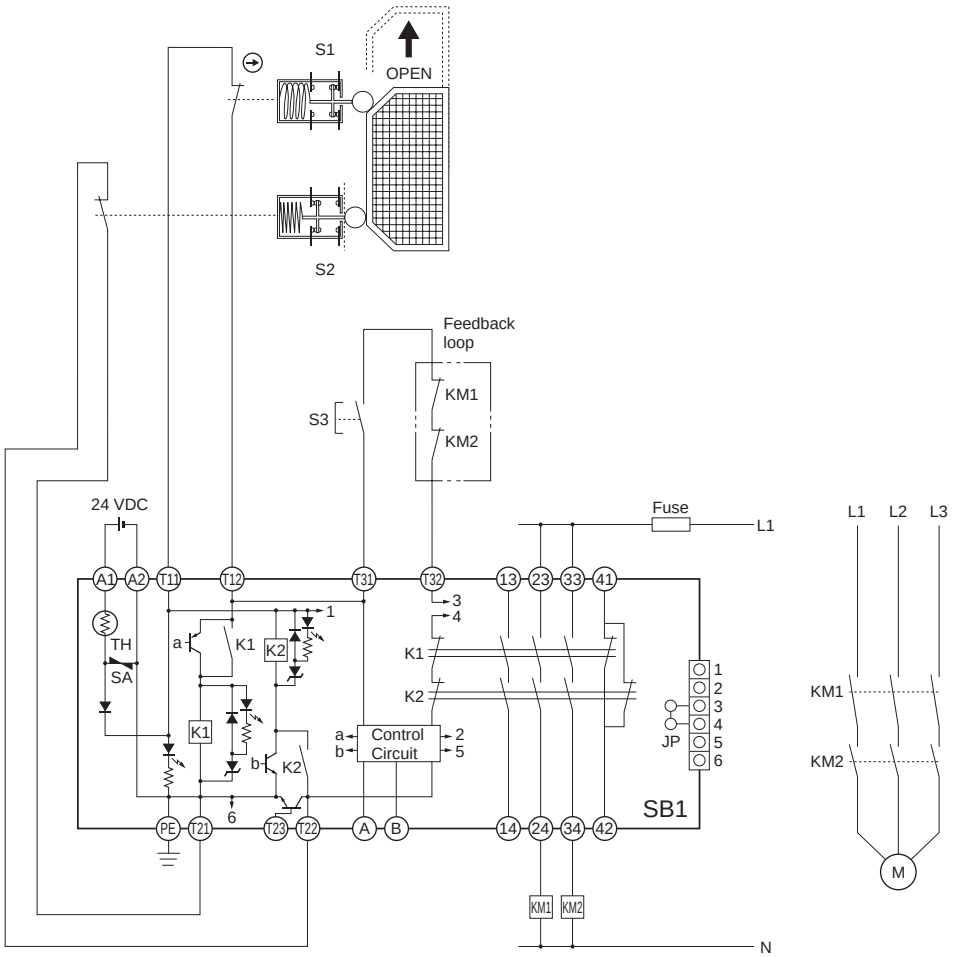
*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

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

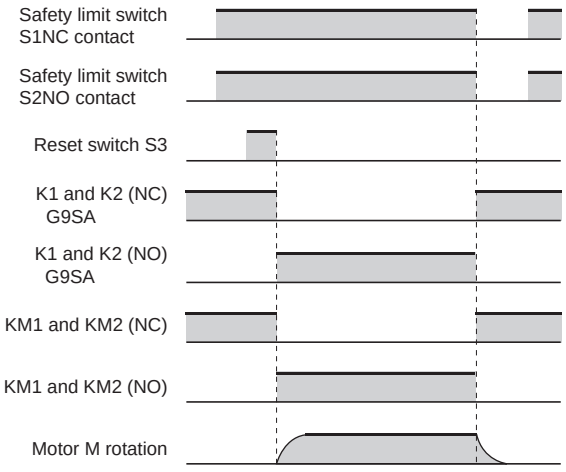
Connection example 4: Safety Limit Switch x 2

• Safety functions

Safety function	Operation	Stop method	Restart method
1	• Immediately removes power to Motor M when limit Switch S1 and S2 detect the opening of the Guard. • The power to Motor M is kept removed until Reset Switch S3 is pressed.	Stop category 0	Manual



• Timing Chart



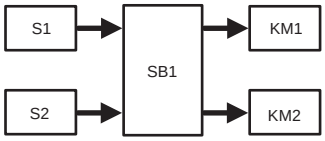
Note: Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.

• 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)	B10d: 20,000,000
S2	General limit switch (NO contact)	B10d: 10,000,000
S3	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
SB1	Safety Relay Unit G9SA-301 (PLe certified on ISO 13849-1)	Category 4, MTTFd: 100 years, DCavg: 99%
KM1/KM2	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

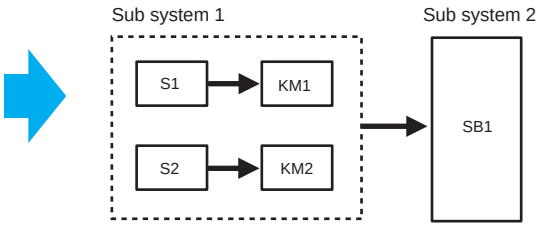
• Developed block diagram

Electrical block diagram of safety-related parts



Developed logical block diagram

Safety function 1



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	S1 (D4N-□□20 NC contact direct mechanical action)	B10d=20,000,000 DC=99%, nop=27,500/year	4	100	99	2.47×10^{-8} *2	e
		S2 General limit switch (NO contact)	B10d=10,000,000 DC=99%, nop=27,500/year					
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=27,500/year					
	2	SB1 (G9SA-301)		4	100	99	2.47×10^{-8} *2	e
	PFHd and PL for the entire safety-related parts						4.94×10^{-8}	e

*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

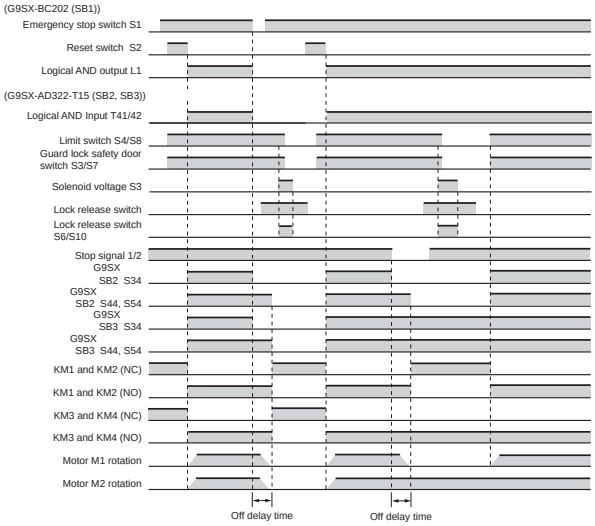
Note: The point of CCF shall be at least 65.

Connection Example 5: Logical Connection of Emergency Stop Switch and Door Switch

• Safety functions

Safety function	Operation	Stop method	Restart method
1	• Immediately removes power to Motor M1 and M2 when Emergency Stop Switch S1 is pressed. • The power to Motor M is kept removed until the latch of the Emergency Stop Switch is released and Reset Switch S2 is pressed.	Stop category 0	Manual
2	• S3 and S4 detect the opening of Guard 1 and the circuit only removes power to Motor M. • Starts power supply to Motor M after the Guard is closed and locked.	Stop category 1	Auto
3	• S7 and S8 detect the opening of Guard 2 and the circuit only removes power to Motor M2. • Starts power supply to Motor M after the Guard is closed and locked.	Stop category 1	Auto

• Timing Chart



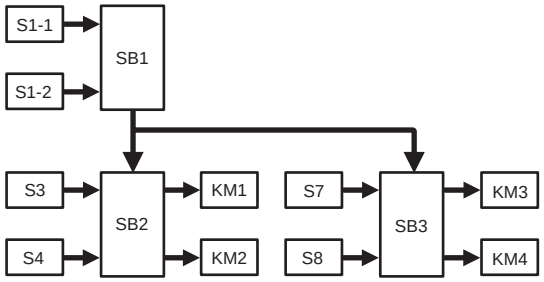
Note: Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.

• 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)	B10d: 100,000
S2	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
S3, S7	Guard Lock Safety-door Switch: D4NL	B10d: 2,000,000
S4, S8	Safety Limit Switch: D4N-□□20 NC contact direct mechanical action	B10d: 10,000,000
SB1	Flexible Safety Unit: G9SX-BC202 (IEC 61508 SIL3 certified)	PFHd: 4.10×10^{-9}
SB2, SB3	Flexible Safety Unit: G9SX-AD322-T15 (IEC 61508 SIL3 certified)	PFHd: 5.70×10^{-9}
KM1/KM2/ KM3/KM4	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

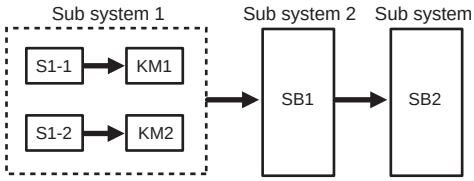
• Developed block diagram

Electrical block diagram of safety-related parts



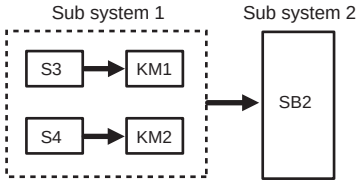
Logical development of block diagram

Safety function 1-1



Note.
The block diagram of safety function 1-2 (S1-1, S1-2, KM3, KM4, SB1, SB3) is developed.

Safety function 2



Note.
The block diagram of safety function 3 (consisting of S7, S8, SB3, KM3 and KM4) is developed in the same way.

• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1-1	1	S1-1, S1-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
		KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=11,500/year	4	100	99	2.47×10^{-8} *2	e
	2	SB1(G9SX-BC202)		4	-	-	4.10×10^{-9}	e(SIL3)
	3	SB2(G9SX-AD322-T15)		4	-	-	5.70×10^{-9}	e(SIL3)
	PFHd and PL for the entire safety-related parts The same result for safety function 1-2 that goes through SB3, KM3 and KM4.						3.45×10^{-8}	e
2	1	S3(D4NL)	B10d= 2,000,000 DC=99%, nop=11,000/year	4	100	99	2.47×10^{-8} *2	e
		S4 Safety Limit Switch: D4N-□□20 NC contact direct mechanical action	B10d= 10,000,000 DC=99%, nop=11,000/year					
		KM1, KM2 (Contactor with nominal load)	B10d 2,000,000 DC=99%, nop=11,500/year					
	2	SB2(G9SX-AD322-T15)		4	-	-	5.70×10^{-9}	e(SIL3)
	PFHd and PL for the entire safety-related parts The same result for safety function 3 that consists of S7, S8, SB3, KM3 and KM4.						3.04×10^{-8}	e

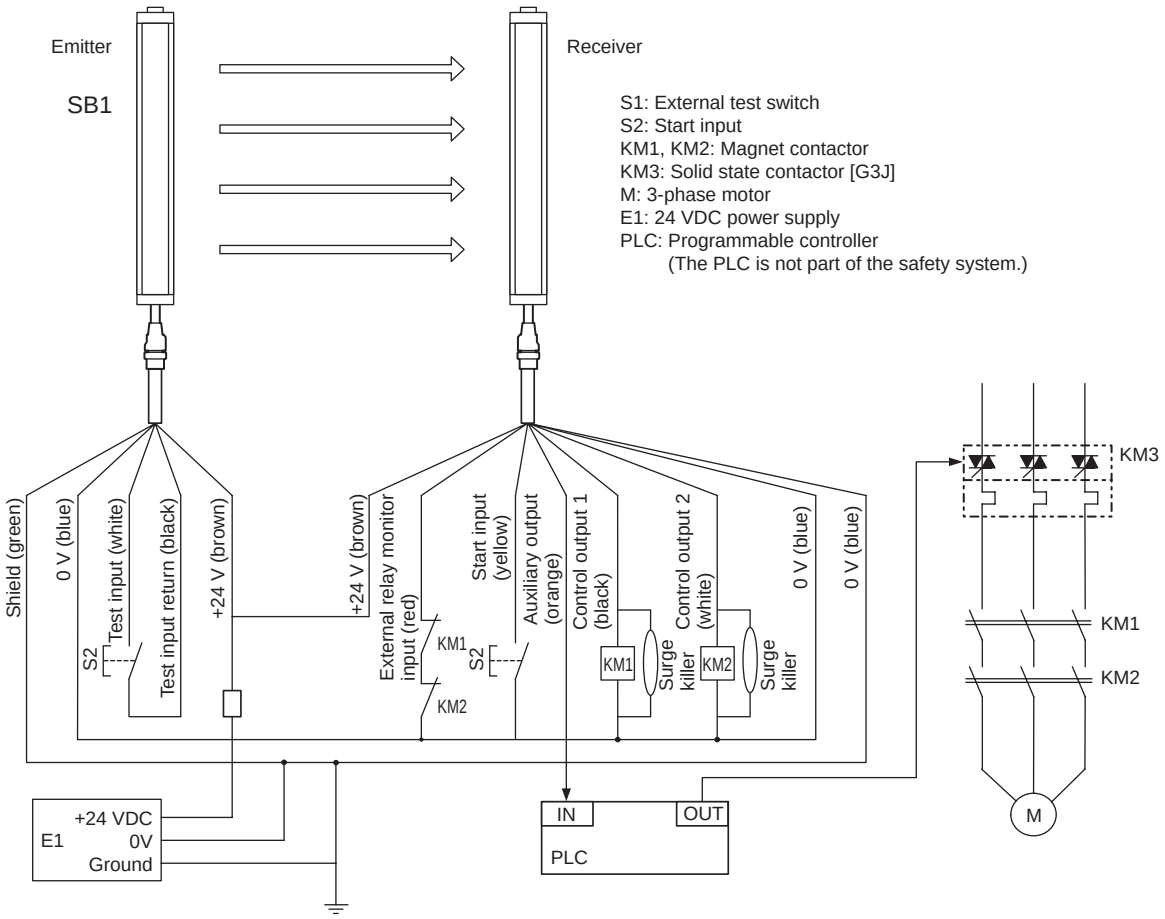
*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

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

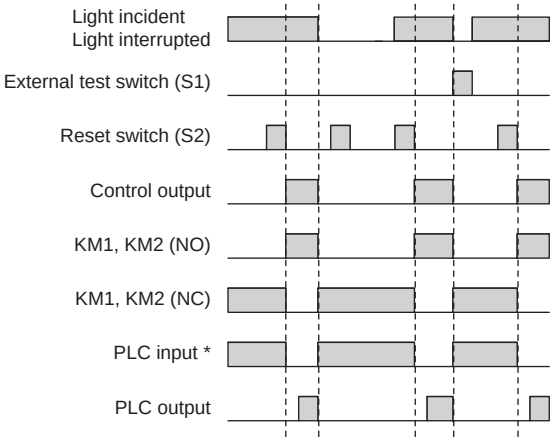
Connection Example 6: Safety Light Curtain (stand alone)

• Safety functions

Safety function	Operation	Stop method	Restart method
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



* ON output when light is interrupted for output operation mode of auxiliary output 1.

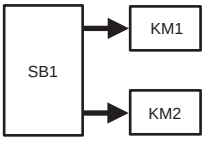
Note: Refer to "2. Precautions" in chapter 4 when actually configuring the circuit.

• Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
SB1	Safety Light Curtain MS4800A-30-□ (IEC 61508 SIL3 certified)	PFHd: 5.90×10^{-8}
KM1/KM2	Contactor with nominal load (from Annex C of ISO 13849-1)	B10d: 2,000,000

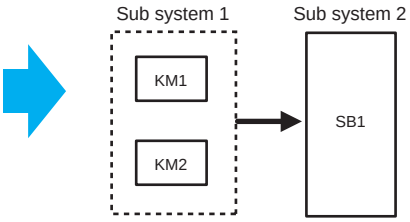
• Developed block diagram

Electrical block diagram of safety-related parts



Developed logical block diagram

Safety function 1



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	KM1, KM2 (Contactor with nominal load)	B10d= 2,000,000 DC=99%, nop=27,500/year	4	100	99	2.47×10^{-8} *2	e
	2	SB1 (MS4800A-30-□)		4	-	-	5.90×10^{-8}	e (SIL3)
	PFHd and PL for the entire safety-related parts						8.37×10^{-8}	e

*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

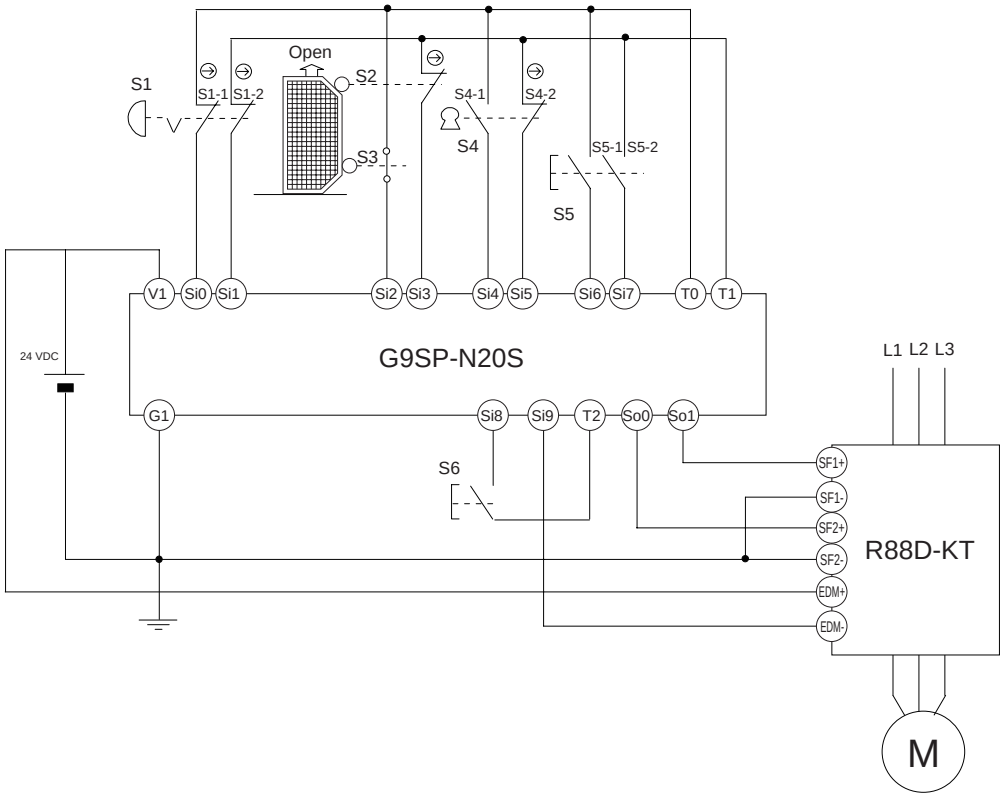
Note: The point of CCF shall be at least 65.

Connection Example 7: Mode Switching, STO

• Safety functions

Safety function	Operation	Stop method	Restart method
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 latch of the Emergency Stop Switch is released and Reset Switch S6 is pressed.	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.	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. • Interlocking by the Guard must be defeated during maintenance mode.	STO*	Manual
4	• Mode Selector S4 switches between scheduled operation mode and maintenance mode.	-	-

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

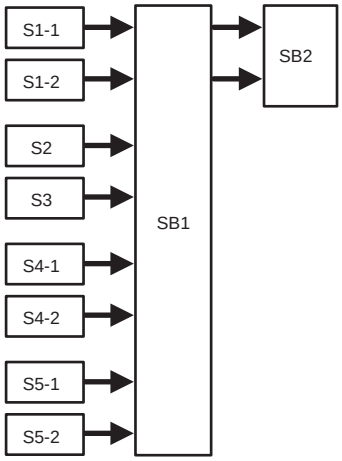


• Model used and machine safety reliability data

Symbol	Model used	Machinery safety reliability data
S1-1/S1-2	Emergency Stop Switch: A22E-M-02 (2NC contact)	B10d: 100,000
S2	Safety Limit Switch: D4N-□□20 (NC contact direct mechanical action)	B10d: 20,000,000
S3	General limit switch (NO contact)	B10d: 10,000,000
S4-1/S4-2	Mode Selector: A22TK-2□□-11 (1NC/1NO contact)	B10d: 100,000
S5-1/S5-2	Enabling Grip Switch: A4EG-C000041 (2NO contact)	B10d: 100,000
S6	Push Button Switch (from Annex C of ISO 13849-1)	B10d: 100,000
SB1	Safety Controller: G9SP-N20S (IEC 61508 SIL3 certified)	PFHd: 8.55×10^{-11}
SB2	AC Servo Driver G5 Series: R88D-KT/KN (IEC 61508 SIL3 certified)	PFHd: 2.30×10^{-8}

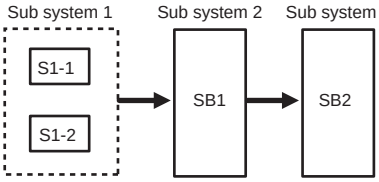
• Developed block diagram

Electrical block diagram of safety-related parts

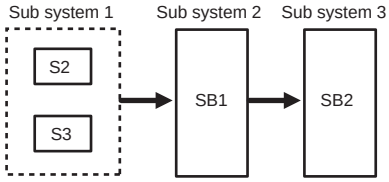


Developed logical block diagram

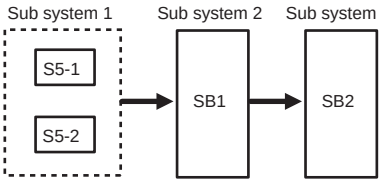
Safety function 1 (Emergency Stop Switch)



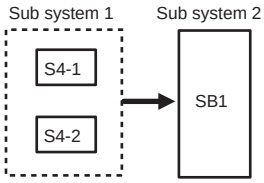
Safety function 2 (Guard)



Safety function 3 (Enabling Grip)



Safety function 4 (Mode Switching)



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL (SIL)
1	1	S1-1, S2-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
	2	G9SP-N20S		4	-	-	1.10×10^{-10}	e(SIL3)
	3	R88D-KT		3	-	-	2.80×10^{-8}	d(SIL2)
	PFHd and PL for the entire safety-related parts						2.81×10^{-8}	d*3
2	1	S2 (D4N-□□20 NC contact)	B10d=20,000,000 DC=99%, nop=27,500/year	4	100	99	2.47×10^{-8} *2	e
		S3 (General limit switch NO contact)	B10d=10,000,000 DC=99%, nop=27,500/year					
	2	G9SP-N20S		4	-	-	1.10×10^{-10}	e(SIL3)
	3	R88D-KT		3	-	-	2.80×10^{-8}	d(SIL2)
	PFHd and PL for the entire safety-related parts						5.28×10^{-8}	d*3
3	1	S5-1, S5-2 (A4EG-C000041 NO contact)	B10d=100,000 DC=99%, nop=500/year	4	100	99	2.47×10^{-8} *2	e
	2	G9SP-N20S		4	-	-	1.10×10^{-10}	e(SIL3)
	3	R88D-KT		3	-	-	2.80×10^{-8}	d(SIL2)
	PFHd and PL for the entire safety-related parts						5.28×10^{-8}	d*3
4	1	S4-1, S4-2 (A22TK-2□□-11 NC/ NO contact)	B10d=100,000 DC=99%, nop=500/year	4	100	99	2.47×10^{-8} *2	e
	2	G9SP-N20S		4	-	-	1.10×10^{-10}	e(SIL3)
	PFHd and PL for the entire safety-related parts						2.48×10^{-8}	e

*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.
*3. The SIL claim limit is applied.

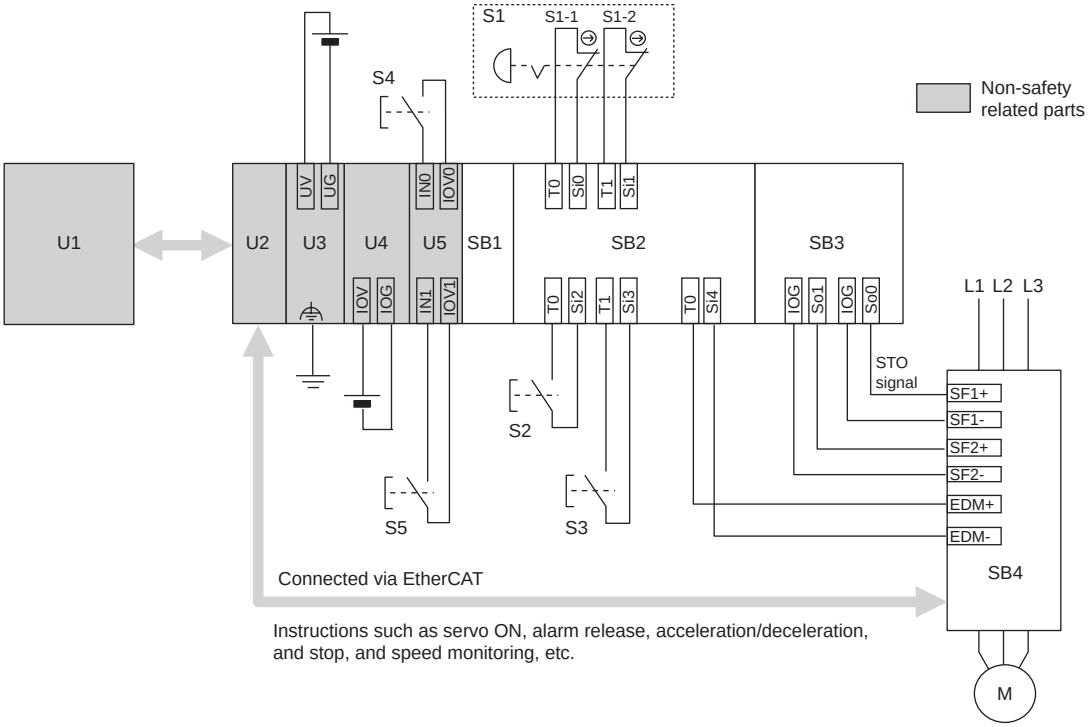
Note: The point of CCF shall be at least 65.

Connection Example 8: Removing Energy Supply with Emergency Stop Switch after Deceleration Stop

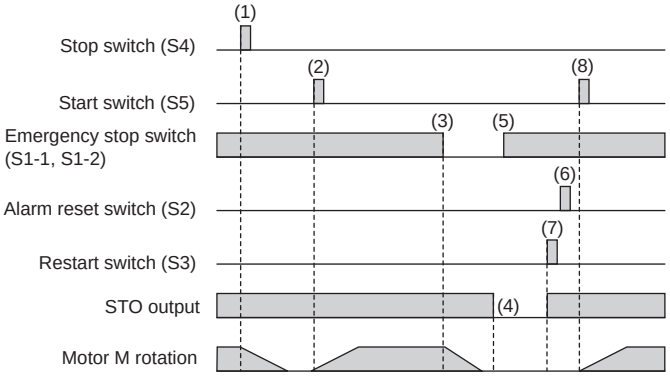
• Safety functions

Safety function	Operation	Stop method	Restart method
1	• Decelerates the speed of Motor M gradually when Emergency Stop Switch S1 is pressed, and removes power to Motor M after it stops completely. • The power to Motor M is kept removed until the latch of Emergency Stop Switch S1 is released and Reset Switch S2 is pressed. • The power to Motor M is kept removed until STO is released and the Restart Switch S3 is pressed.	STO*	Manual

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



• Timing Chart



(1) Press stop switch S4 in operation state (servo ON) and give a deceleration stop instruction from general control side to AC servo controller SB4.
(2) Press start switch S5 in stop state (servo ON) and give an acceleration instruction from the general control side to AC servo controller SB4.
(3) When emergency stop switch S1 is pressed in operation state (servo ON), give a deceleration stop instruction from the general control side to AC servo controller SB4.
(4) Remove power to motor M after a certain period of time since emergency stop switch S1 has been pressed. (Safety function 1)
(5) The latch of the emergency stop switch is released.
(6) After reset switch S2 is pressed, release alarm state of the servo driver to turn the servo ON.
(7) Release STO when restart switch S3 is pressed.
(8) Press start switch S5 and give an acceleration instruction from general control side to AC servo controller SB4.

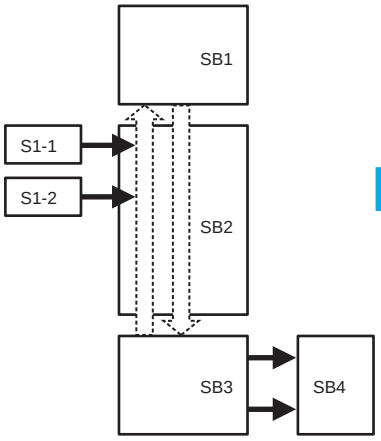
• Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
S1-1/ S1-2	Emergency Stop Switch: A22E-M-02	B10d: 100,000
S2	Reset Switch: General push button switch (NO contact, momentary)	B10d: 100,000*3
S3	Restart Switch: General push button switch (NO contact, momentary)	B10d: 100,000*3
S4	Stop Switch (For general control): General push button switch (NO contact, momentary)	Not evaluated as PL (Non-safety-related parts)
S5	Start Switch (for general control): General push button switch (NO contact, momentary)	Not evaluated as PL (Non-safety-related parts)
SB1	Safety CPU Unit: NX-SL3300*1	PFHd: 3.10 x 10^{-10}, Category 4
SB2	Safety Input Unit: NX-SID800*1	PFHd: 4.30×10^{-10}, Category 4
SB3	Safety Output Unit: NX-SOH200*1	PFHd: 3.60×10^{-10}, Category 4
SB4	AC Servo Driver G5 Series: R88D-KT*2	PFHd: 2.30×10^{-8}, Category 3
U1	Machine Controller (for general control): NJ301	Not evaluated as PL (Non-safety-related parts)
U2	NX Series EtherCAT Coupler Unit (for general control): NX-ECC201	Not evaluated as PL (Non-safety-related parts)
U3	Additional NX Unit Power Supply Unit (for general control): NX-PD1000	Not evaluated as PL (Non-safety-related parts)
U4	Additional I/O Power Supply Unit (for general control): NX-PF0630	Not evaluated as PL (Non-safety-related parts)
U5	Digital Input Unit (for general control): NX-ID4442	Not evaluated as PL (Non-safety-related parts)

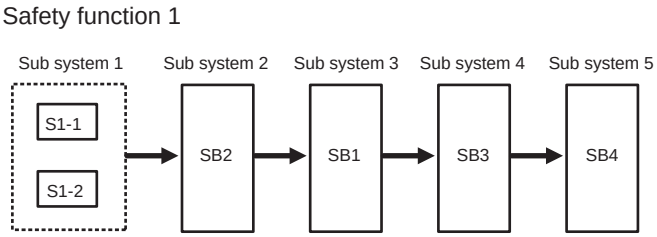
*1. IEC 61508 SIL3 certified.
*2. IEC 61508 SIL2 certified.
*3. According to Table C.1 of Annex C of ISO 13849-1.

• Developed block diagram

Pathway of safety functions



Block diagram of reliability



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL/ SIL
1	1	S1-1, S1-2 (A22E-M-02)	Faults excluded	-	-	-	-	-
	2	SB2 (Safety Input Unit: NX-SID800)		4	-	-	4.30×10^{-10}	e(SIL3)
	3	SB1 (Safety CPU Unit: NX-SL3300)		4	-	-	3.10×10^{-10}	e(SIL3)
	4	SB3 (Safety Output Unit: NX-SOH200)		4	-	-	3.60×10^{-10}	e(SIL3)
	5	SB4 (AC Servo Driver G5 Series: R88D-KT)		3	-	-	2.80×10^{-8}	d(SIL2)
	PFHd and PL for the entire safety-related parts						2.91×10^{-8}	d*2

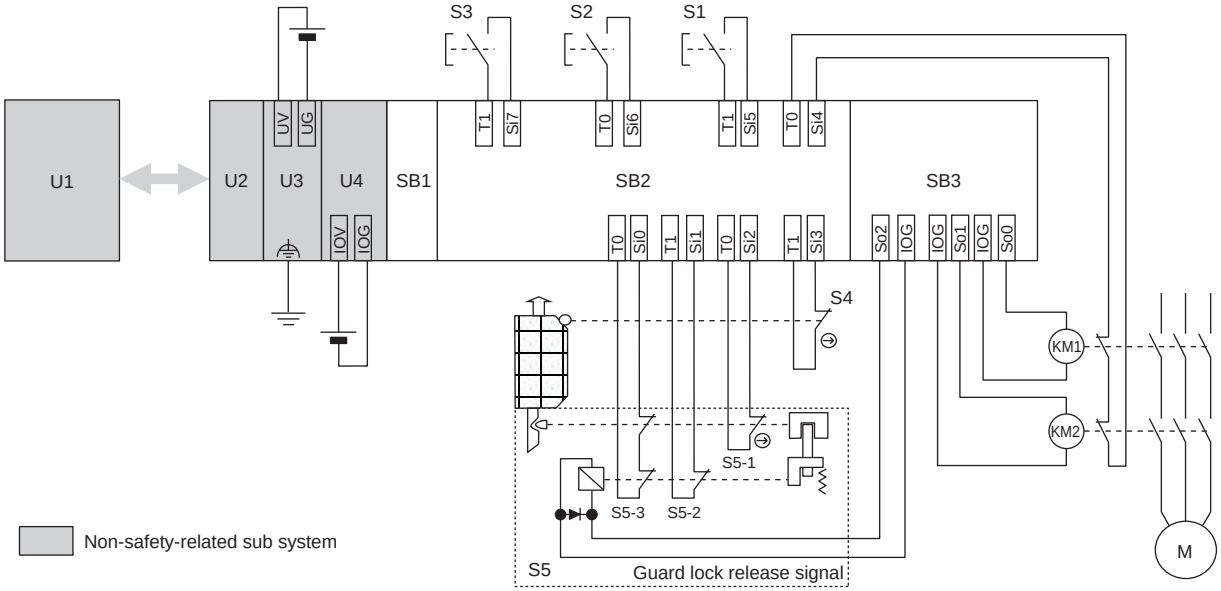
*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. The SIL claim limit is applied.

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

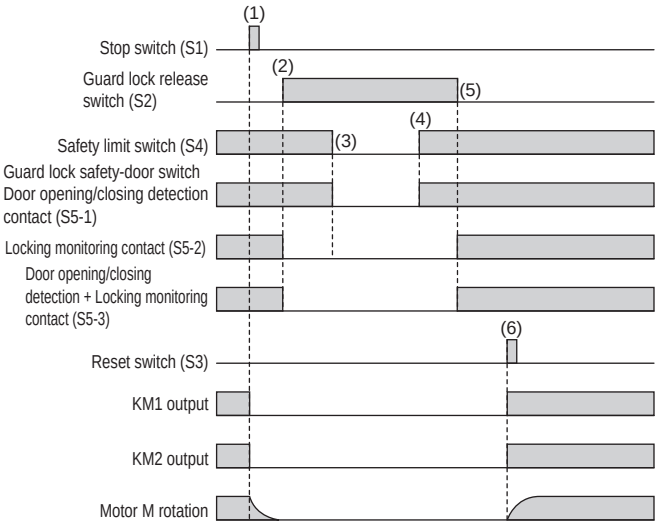
Connection Example 9: Guard Lock Safety-door Switch

• Safety functions

Safety function	Operation	Operation	Restart method
4	• Immediately removes power to Motor M when Stop Switch S1 is pressed. • Releases the solenoid lock of Guard Lock Safety-door Switch S5 after a period of time required for Motor M to stop. • The power to Motor M is kept removed until the Guard is closed and locked, and Reset Switch S2 is pressed.	Stop category 1	Manual



• Timing Chart



(1) Remove power to motor M when stop switch S1 is pressed.
(2) After motor M stopped, press guard lock release switch S2 to release the door lock.
(3) Open the guard.
(4) Move out of the hazard zone and close the guard.
(5) Lock the guard.
(6) Press reset switch S3 to restore the machine to operating state.

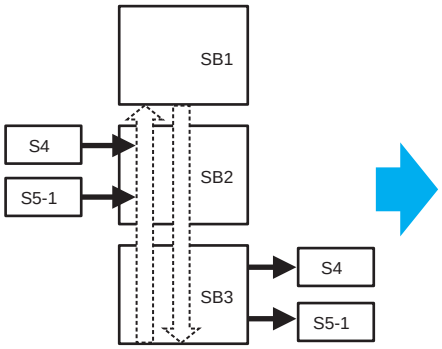
• Model used and machine safety reliability data

Symbol	Model used	Machine safety reliability data
S1	Stop Switch: General push button switch (NO contact, momentary)	B10d: 100,000*2
S2	Guard Lock Release Switch: General push button switch (NO contact, alternate)	B10d: 100,000*2
S3	Reset Switch: General push button switch (NO contact, momentary)	B10d: 100,000*2
S4	Safety Limit Switch: D4N-□□20	B10d: 20,000,000
S5-1	Guard Lock Safety-door Switches (Door opening/closing detection contact): D4SL-N2VFA	B10d: 2,000,000
S5-2	Guard Lock Safety-door Switches (Locking monitoring contact): D4SL-N2VFA	B10d: 2,000,000
S5-3	Guard Lock Safety-door Switches (Door opening/closing detection contact + locking monitoring contact): D4SL-N2VFA	B10d: 2,000,000
KM1, KM2	Contactor with nominal load	B10d: 2,000,000*2
SB1	Safety CPU Unit: NX-SL3300*1	PFHd: 3.10×10^{-10}, Category 4
SB2	Safety Input Unit: NX-SID800*1	PFHd: 4.30×10^{-10}, Category 4
SB3	Safety Output Unit: NX-SOD400*1	PFHd: 5.50×10^{-10}, Category 4
U1	Machine Controller (for general control): NJ301	Not evaluated as PL (Non-safety-related parts)
U2	NX Series EtherCAT Coupler Unit (for general control): NX-ECC201	Not evaluated as PL (Non-safety-related parts)
U3	Additional NX Unit Power Supply Unit (for general control): NX-PD1000	Not evaluated as PL (Non-safety-related parts)
U4	Additional I/O Power Supply Unit (for general control): NX-PF0630	Not evaluated as PL (Non-safety-related parts)

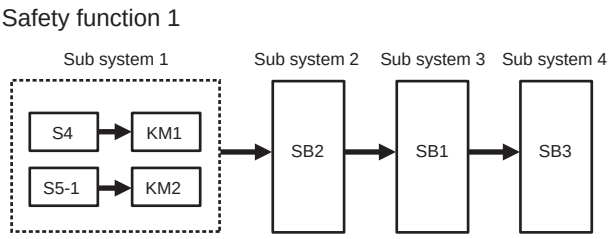
*1. IEC 61508 SIL3 certified. *2. According to Table C.1 of Annex C of ISO 13849-1.

• Developed block diagram

Pathway of safety functions



Block diagram of reliability



• PL of Safety-related Parts

Safety function	Sub system	Component		Category	MTTFd (year)*1	DCavg (%)	PFHd	PL / SIL
1	1	S4	B10d = 20,000,000, nop = 11,000/year, DC = 99%	4	100	99	2.47×10^{-8} *2	e
		KM1	B10d = 2,000,000, nop = 11,000/year, DC = 99%					
		S5-1	B10d = 2,000,000, nop = 11,000/year, DC = 99%					
		KM2	B10d = 2,000,000, nop = 11,000/year, DC = 99%					
	2	SB2 (Safety Input Unit: NX-SID800)		4	-	-	4.30×10^{-10}	e(SIL3)
	3	SB1 (Safety CPU Unit: NX-SL3300)		4	-	-	3.10×10^{-10}	e(SIL3)
	4	SB3 (Safety Output Unit: NX-SOD400)		4	-	-	5.50×10^{-10}	e(SIL3)
	PFHd and PL for the entire safety-related parts						2.59×10^{-8}	e

*1. The upper limit of MTTFd as a sub system shall be 100 years.
*2. Converted to PFHd based on Table K.1 of Annex K of ISO 13849-1.

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

MEMO

Chapter 5

Performance Level

1. What is a Performance Level (PL) ?

If a risk reduction measure is based on the control, the performance level of achievement is required depending on the scale of risk for both hardware and software in the safety-related parts for the control system. This level is defined in the ISO 13849-1 standard as the Performance Level (PL).
For the machines to be exported to Europe, the safety function PL is required to be met and the validity shall be certified based on the Machinery Directive for European regulation.
JIS B 9705-1 is the standard of Japanese counterpart and harmonized with the ISO 13849-1 being identified as the same. Regulations in each country are being standardized based on ISO 13849-1 and that is recognized as the standard method for evaluating the safety function of the machine control.

Roles of manufacturers of machines and control devices

PL is evaluated based on the control circuit structure for the safety function and reliability of the composites.
PL is evaluated by the device designers in the manufacturers of the machines. Evaluation is achieved by applying the machine safety reliability data specific to the control devices to the structural elements (such as category as described later or parameters as CCF) of the safety-related parts or usage conditions (such as nop or DCavg parameters) which are known only to the designers.

Control device manufacturers provide the device designers the machine safety reliability data required for the PL evaluation.

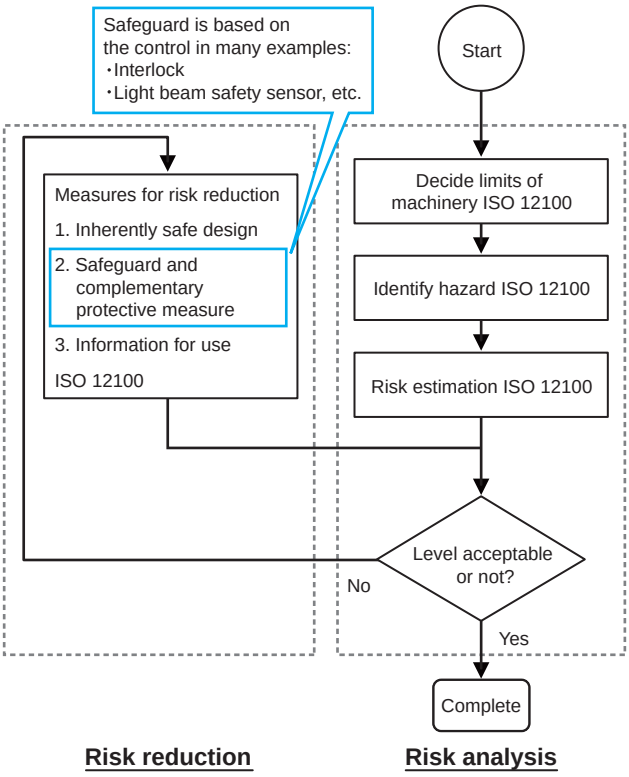
The following sections describe the relationship between a risk assessment and PL, and the specific PL evaluation procedures.

- Relationship between Risk Assessment and PL
- Organizing Safety Functions and Hazards
- PLr and PL
- PL Evaluation for the Safety-related Parts
- Subsystem Configured in Singular Parts
  -Categories
  -MTTFd
  -DCavg
  -CCF
  -PFHd
- Individual Subsystem
- PL Determination

2. Relationship between Risk Assessment and PL

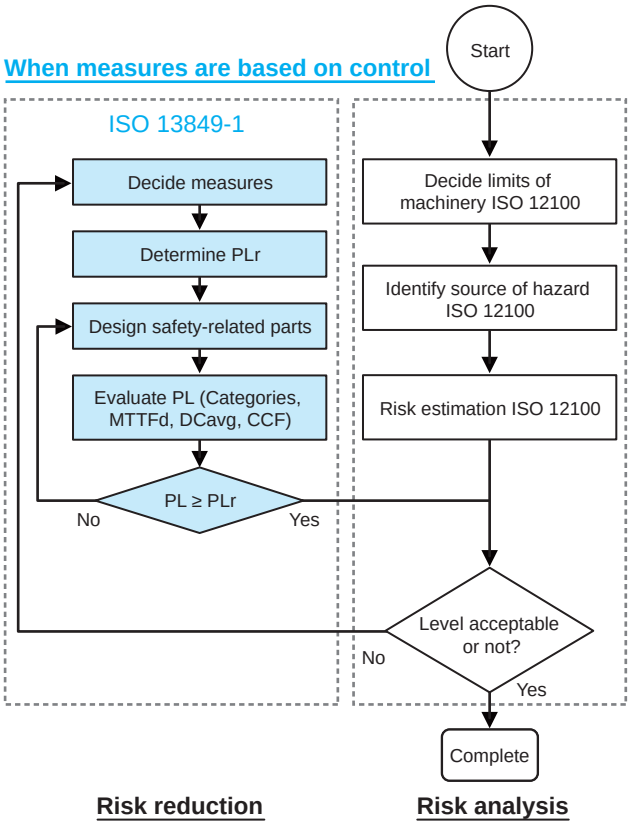
Risk Assessment Procedure

This section describes the risk reduction measures and PL for the safety-related parts.
ISO 12100: 2010 machine design procedure follows a series of flows for the risk reduction following the risk analysis.
The risk reduction measures contain the following three steps as described in Chapter 2.
1.Inherently safe design
2.Safeguard and complementary protective measures
3.Information for use
Of the measures above, safeguarding and the complementary protective measures are featured with the many safety functions such as the interlock mechanism of safety switches or safety light curtain or the emergency stop devices. These devices do not usually work individually but are integrated in a safety-related part of control system, followed by a processing function and a power control function.



Iterative Process of Risk Reduction

Control-based risk reduction measures only are subject to PL evaluation. Risk reduction process with ISO 13849-1 is specifically harmonized with ISO 12100 as shown in the diagram below.



Safety function and PL

The risk reduction measures, if not relevant with the control system, are not subject to the PL evaluation. The safety measures not taken by the control, such as those by mechanical protection structures as the fixed safety fences or by the operation such as lockout/tagout are not subject to PL evaluation. The safety measures, though controlled, which are positioned as the information for use such as the alarm function, are not subject to PL evaluation either.
The safety measures, though not subject to the PL evaluation, which are specified in other safety standards are required to meet the standard. For example, an overcurrent protection device as referred to in IEC 60204-1 safety standard is applicable.
It is recommended to start with extracting the items restricted for PL evaluation of the risk reduction measures in the process of reviewing the machinery risk assessment sheet.

NO	Device name	Hazard	Hazardous event	Risk	Allowance	Risk reduction measure	PL evaluation
1	Press machine	Crushing	During the press work, another operator puts a hand in to take out a workpiece, resulting in a hand pinched.	High	×	Protection by light beam safety device.	✔
2	Control panel	Contact with a live part	Electrically shocked by contact with a live part by mistake during a part replacement.	Medium	×	Install main power isolator.	
3	Conveyor	Entanglement, trapping	Work wear is entangled into a conveyor, bruised by dragging along.	Medium	×	Install an emergency stop switch in certain intervals.	✔
4	Cables	Trapping	A operator trips over an exposed cable on the floor and falls down.	Medium	×	Lay floor cable covers.	
5	Work piece table	Unnatural posture	Back pain occurs due to working long hours using a work piece table that is too low in height for the operator.	Medium	×	Adjust the bench height.	

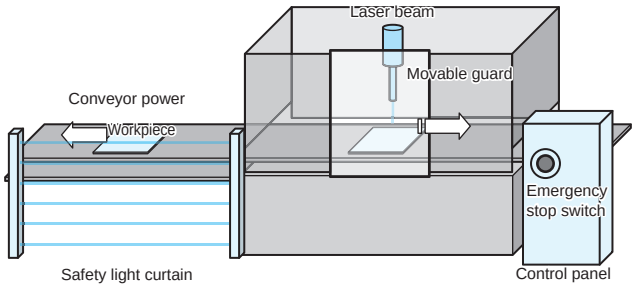
3. Organizing Safety Functions and Hazards

Each performance level from the multiple safety functions in a single machine will be briefly explained.

Multiple safety functions in the same machine

There are generally multiple measures for the risk reduction referred to in the risk assessment. Of the multiple measures, PL is required in the control-based risk reduction schemes for the safety function.

Following devices are assumed as an example. There are two hazards: laser beams (risk of blindness) and conveyor power (entanglement).



If the following risk reduction measures are taken against the hazards described above, the summary of the safety functional systems are as shown in the table below.

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

Device		Hazard	
		Laser beam	Conveyor power
Risk reduction measure	Emergency stop switch	System 1	System 2
	Movable guard	System 3	-
	Safety light curtain	-	System 4

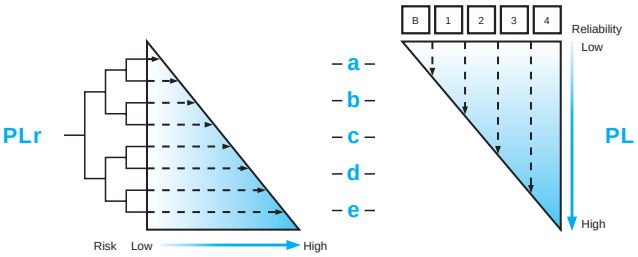
If a single risk reduction measure is shared with the measures against the multiple hazards, it is handled as a separate system. PL evaluation is performed to each system for these safety functions.
That means that PL for a machine having multiple hazards and multiple risk reduction measures is not restricted to one. It is recommended to clarify the relationships between risk reduction measures and hazards before starting the PL evaluation even if the safety functions are complicated in the actual machines.
With the relationships summarized, the safety functional system is evaluated in terms of the safety-related parts.

4. PLr and PL

Common Criteria

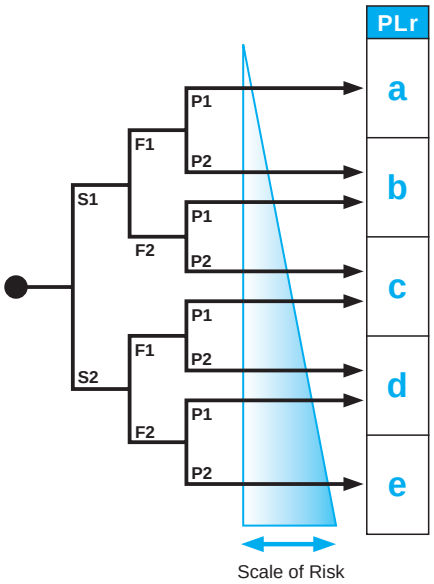
With the system of the safety functions in the machine being summarized, the required performance level for each safety system is evaluated.
PL is comprised of the performance (PLr) required in the safety related parts according to the scale of the risk and the result (PL) where an actual safety relevance validity is evaluated.
Both performances are evaluated in five levels from "a" to "e."

- Performance level required in the safety-related parts: PLr (Required Performance Level)
- Validity evaluation result in the safety-related parts: PL (Performance Level)



How to Determine PLr

Of the performance levels, what can be determined at the completion of the risk assessment is PLr. This can be a target performance on design for the safety-related parts.
PLr is evaluated using the risk graphs and scheme in terms of the Severity of Injury (S), Frequency and/or Exposure Time to the Hazard (F) and Possibility of Avoiding the Hazard (P). The results are subsequently divided into the indexes from a to e depending on the risk size.



<Meaning of Symbols>
S1: slight (normally reversible injury)
S2: serious (normally irreversible injury or death)
F1: seldom-to-less-often and/or exposure time is short
F2: frequent-to-continuous and/or exposure time is long
P1: possible under specific conditions
P2: scarcely possible

PL cannot be evaluated unless the safety-related parts design is specifically defined. The following section describes the PL evaluation procedure, assuming the safety-related parts design is embodied.

Validity evaluation result (PL) for the safety-related parts is required to be equivalent to the required performance level (PLr) or more.

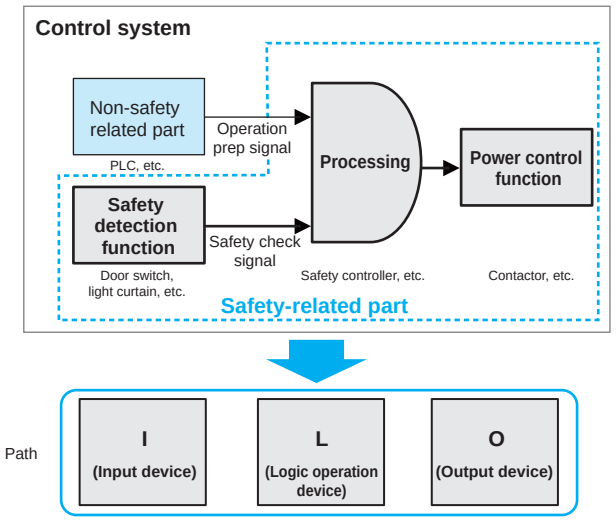
5. Safety-related Parts PL Evaluation Procedure

This section describes the safety-related parts PL evaluation procedure for achieving the safety function system.

Evaluating the Safety-related Parts by Path of Safety Function

Request for safety function operation request is performed via the transmission path different for each system. For example, a certain safety function tells the actuator that the event of guard opening occurs and shuts off the hazardous energy. And another safety function tells the actuator that the emergency stop switch is being pressed and shuts off the hazardous energy. There are some common phenomena, but they are transmitted in different paths. Each transmission path is comprised of the detection function: I (Input device), judging function: L (Logic operation device) and power control function: O (Output device), forming a path. This is a safety-related part.

By turning the sequel of the safety function being transmitted from the control circuit through the system into the block diagram as shown on the right and further into a pattern may facilitate the PL evaluation.



1) Extracting safety-related parts

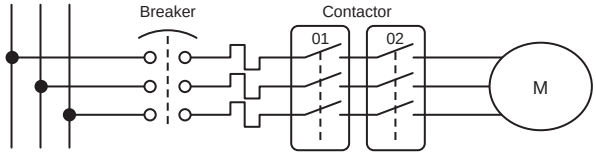
Representing the safety-related parts of a certain safety function in a block diagram can be started with isolating the parts which are related to the safety function implementation from the parts which are not in the control circuit diagrams. The parts not relevant to the safety function or those whose failure does not cause the loss of the safety function are not needed to be incorporated into the PL evaluation even if they are on the transmission path.

Example:

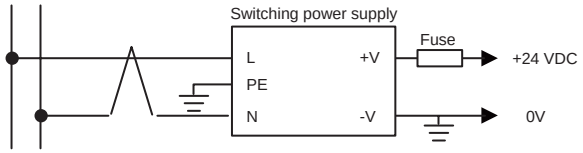
- Overcurrent breaker, transformer, etc.: Important parts for the electric safety (such as IEC 60204-1 (JIS B 9960-1)), but they are not within the scope of the application of ISO 13849-1.
- Cable, connector, or signal splitter/divider: They are not active parts and they are least likely to be the cause of the loss of the safety function. (If "fault exclusions" in ISO 13849-2 is applicable)

Assume the safety function control circuit diagram where hazards are shut off by the stop category 0 via the emergency stop switch.

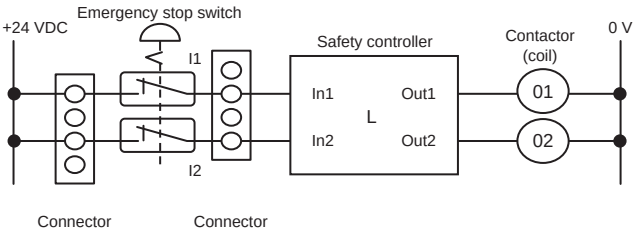
3-phase power supply (200 VAC system)



Single phase power supply (100 VAC system)



Control power supply (24 VDC)



2) Assigning to the Block Diagram and Judging the Category

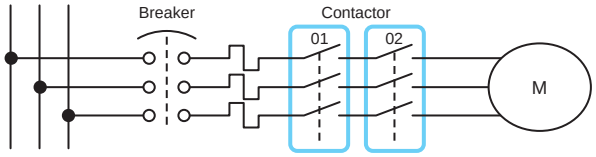
Assign the extracted individual safety-related part to the block diagrams of I, L and O. It is important to note here how many paths are available to transmit each safety function. This passage is called a channel. The category is determined by a number of channels. Assign the safety relevance parts to a block diagram of the designated architecture.

Input and output are provided with two channels each (Two contacts inside the emergency stop switch which are connected to each channel are assumed to be two channels). The safety controllers are assumed to be internally made redundant. The block diagram in that case is category 3 or category 4.

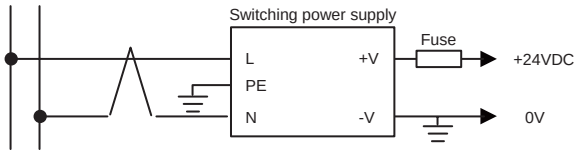
NOTE: A block diagram shows the probability of a dangerous failure of the safety-related parts being accumulated. This does not represent an electric signal flow. The parts are expanded in series even if the power supply system differs.

Each category has specific requirements according to the PLr of the safety function. For further details, see (1) Category in Section 6. Subsystem Configured in Discrete Components in Singular Parts in Chapter 5.

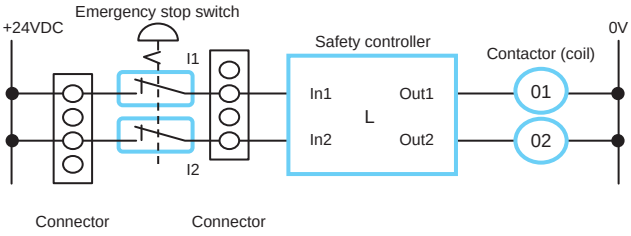
3-phase power supply (200 VAC system)

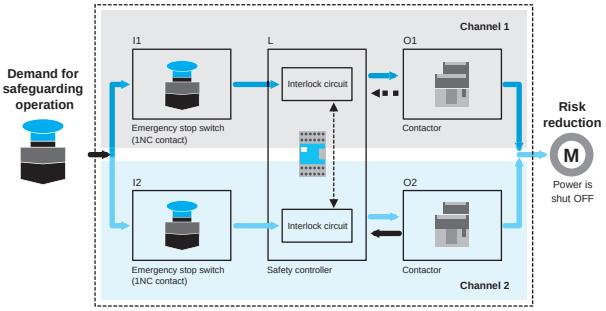


Single phase power supply (100 VAC)



Control power supply (24 VDC)



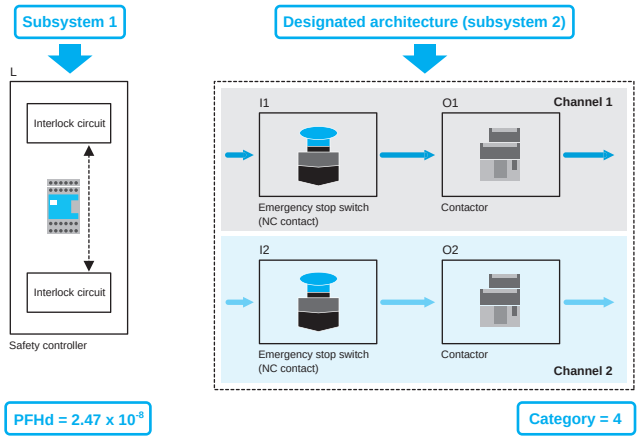


3) Dividing the Entire Safety-related Parts into Subsystems

As a matter of fact, making a safety relevance PL evaluation based on the ISO 13849-1: 2006 scheme alone is complicated and difficult. So the subsequent description will be made according to the scheme presented in the technical report ISO/TR 23849 as an application guide to ISO 13849-1.

Dividing the safety-related parts block diagram into some functional chunks (which are called subsystems in a sense of system sublayers) may help PL evaluation more easily. For example, in the safety controller in the above diagram, there are some safety-related parts where two channels are formed within a device for PL evaluation being established as a device. Such a safety device is a subsystem for itself. To avoid the duplicated evaluation, the subsystems are viewed separated from the block diagram. Consequently, what are assigned to the block diagrams are restricted to the individual parts whose PL is not yet evaluated (such as switches, relays or contactors). These individual parts are called a block.

Devices such as safety controllers whose PL is evaluated by the control device manufacturers are evaluated as an independent subsystem. A portion of discrete parts are handled as a subsystem assigned to the designated architecture of a combination of those portions.



Reference: Classification of Omron Safety Components

Classification	Discrete components (block)	Complex Subsystem
Features	• No PL declaration per se • No diagnosis (passive)	• PL declared in a device • Failure diagnosis self-contained (active)
Input device	 Safety Limit Switch: D4N Series  Emergency Stop 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 etc.
Control device	 Safety Relay: G7SA etc.	 Safety Relay Unit: G9SA series  Flexible Safety Unit: G9SX series  Safety Controller: G9SP  Safety Control Unit: NX series etc.
Output device	Contactor, etc.	 AC Servo Motor/Driver: G5 series  Multi-function Compact Inverter: MX2 series V1 type etc.

In a subsystem composed of singular devices, devices are assigned to a designated architecture and out of the following four parameters

- Category
- MTTFd
- DCavg
- CCF

and ultimately the following parameter

- PFHd

is derived for evaluation.

For further details, see Section 6. Subsystem Configured in Discrete Components in Chapter 5.
For the independent subsystem, the control device manufacturers provide the four parameters or PFHd in the above.
For further details, see Section 7. Complex Subsystem in Chapter 5.

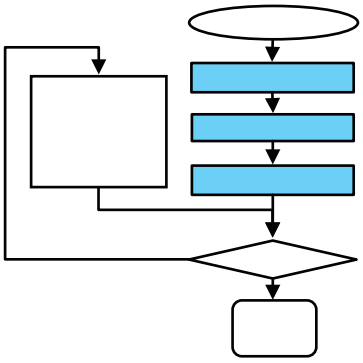
4) Linking the Subsystems

Overall evaluation is made by summing together the subsystem PL evaluation comprised of the discrete components obtained in 3) and the individual subsystem PL evaluation.
PFHd is used for linking the subsystems.
For further details, see Section 8. PL Evaluation in Chapter 5.

PL Evaluation Procedure

Work flow up to the present point is as follows.
Those diagrams represent the evaluation procedure overview for the safety-related parts performance (PL) as indicated in the ISO 13849-1: 2006 and ISO/TR 23849.
Proceed to the detailed safety design along with the description in each chapter.

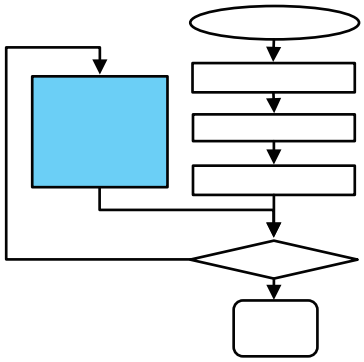
A



Enumerate the risks by the risk assessment.

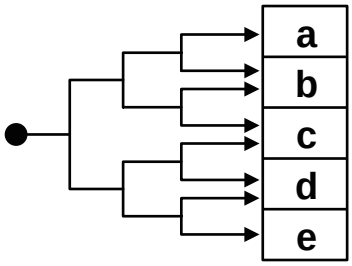
See **Risk Assessment Procedure in 2. Relationship between Risk Assessment and PL in Chapter 5.**

B



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

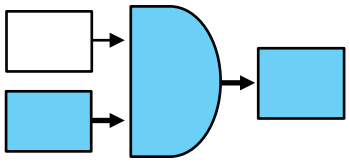
See **Risk Assessment Procedure in 2. Relationship between Risk Assessment and PL in Chapter 5.**



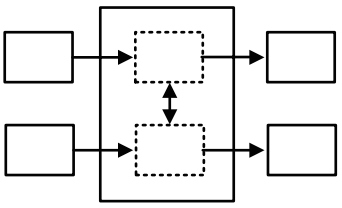
If a measure is control-based, determine the required performance level (PLr) to meet the measure (safety function).

See **How to Determine PLr in 4. PLr and PL in Chapter 5.**

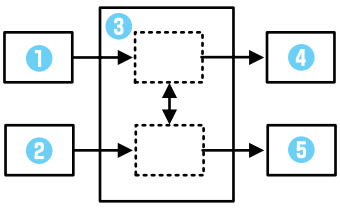
C



Design a control circuit to implement the required safety function.
To achieve PLr in the safety-related parts, it is necessary to select the parts having the circuit of designated architecture (category) and reliability to meet the requirements.



Extract from the control circuit the safety-related parts for transmitting the operating demands for safety function and expand into the logical block diagram.



Of the safety-related parts, isolate what are already evaluated with PL per se and what are functionally evaluated for safety (SIL) from the discrete components.

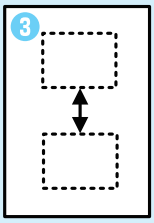
See **7. Complex Subsystem in Chapter 5.**

a

b

b

Complex subsystem



Complicated electronic circuits (including safety light curtains, safety controllers) comprised of the electronic parts are mainly evaluated by the parts manufacturers.

Products in conformity to IEC 62061/IEC 61508

SIL only declared

Converted into PL **via PL decision table on page 104**

PFHd is given by a manufacturer

Products in conformity to ISO 13849-1

PL only declared

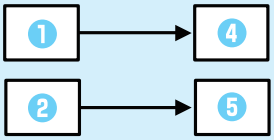
- Category
- MTTFd
- DC
- CCF

are given by a manufacturer

Converted into PFHd **via PFHd conversion table on page 103**

a

Safety-related parts or subsystem comprised of designated architecture



Consumable mechanical parts (including switches, relays or contactors) are mainly evaluated by the machinery manufacturers

- B10d
- DC

are given by a manufacturer

- nop is assumed

- Identify category
- Calculate MTTFd
- Calculate DCavg
- Check CCF

Converted into PFHd **via PFHd conversion table on page 103**

Converted into PL **via PL decision table on page 104**

Simplified evaluation

Which is the lowest PL in the subsystem?

Determine PL in **3) Simplified estimation in 8. PL Evaluation in Chapter 5**

Quantitative evaluation

Sum of PFHd in all the subsystems

Determine PL in **1) Combination of Subsystems in 8. PL Evaluation in Chapter 5**

PLr achieved? — YES → Risk reduced to an acceptable level? — YES → All risks assessed? — YES → **Completed**

NO → Reconsider circuit configuration and parts **C**

NO → Consider additional safety measures **B**

NO → Continue risk enumeration **A**

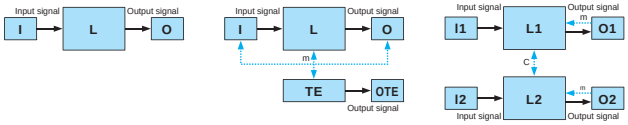
6. Subsystem Configured in Discrete Components

Singular parts basically indicate the consumable parts (such as switches, relays or contactors) or sensors which are not provided with the active diagnostic functions. Reliability of the subsystems configured in these discrete components are evaluated by the following parameters. The same is true if the entire safety-related parts are comprised of the singular parts. If the parts themselves, however, are already certified by ISO 13849-1 or IEC 62061 (or IEC 61508) and their reliable values are known, different values are to be consolidated. Such certified parts are called subsystem. How they are consolidated into the entire safety-related parts is described in 8. PL Evaluation in Chapter 5.

PL parameter

Category

Safety control system's architecture (configuration of I, L and O)



MTTFd

- B10d
- nop*

* The machine designer him/herself needs to know nop.

(1) Component block

1. Use MTTFd provided by the manufacturer.
2. Use MTTFd or B10d specified in Annex C.
3. 10 years if no data is available

When B10d is provided, use the right-hand side equation to obtain MTTFd.

$$MTTFd = \frac{B10d}{0.1 \times N_{OP}}$$

(2) Channel

$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

(3) Entire subsystem

If Channel 1 and Channel 2 MTTFd are equivalent, assume the equation (2) result as MTTFd for the subsystem.
MTTFd for the subsystem, however, is limited up to 100 years.

$$MTTFd = \frac{2}{3}\left[MTTFdc1 + MTTFdc2 - \frac{1}{\frac{1}{MTTFdc1} + \frac{1}{MTTFdc2}}\right]$$

DCavg

(1) Component block → Select the relevant DC from Table 1 in Annex E.

- DC
- MTTFd

(2) The entire subsystem

$$DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

CCF

The score in the checklist in Annex F must be 65 or over

Criteria for determination

- B
- 1
- 2
- 3
- 4

5 categories

- High (30 or more years and less than 100 years)
- Medium (10 or more years and less than 30 years)
- Low (3 or more years and less than 10 years)

3 levels

- High (99% or more)
- Medium (90% or more and less than 99%)
- Low (60% or more and less than 90%)
- N/A (Less than 60%)

4 levels

- Yes (65 or more)
- No (Less than 65)

2 levels

(1) Category

This section describes the types of category and its requirements as a framework of the safety-related parts.

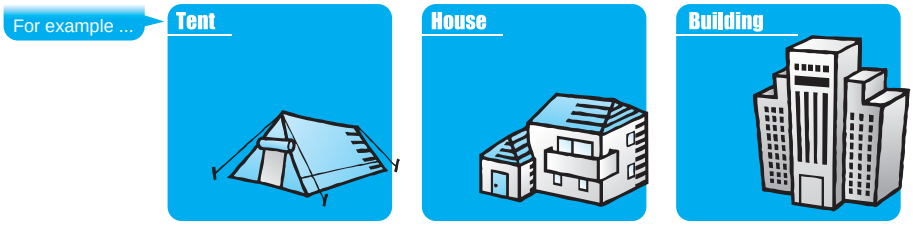
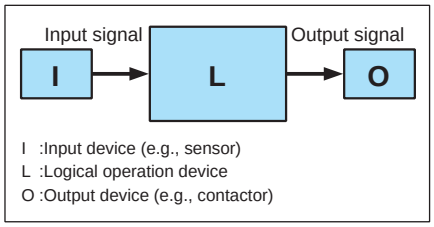


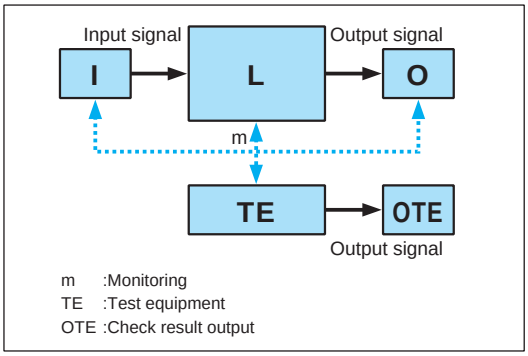
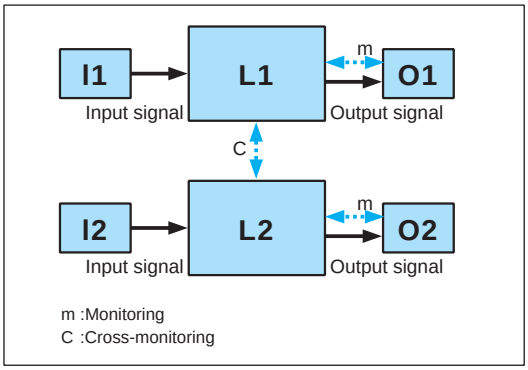
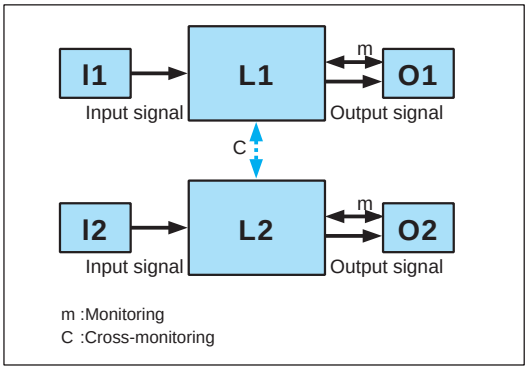
Fig. 1: Space for avoiding rains and winds

Concept of category

The safety-related parts have different structures (architectures) depending on the purpose of the machines, degree of hazards, scale of the machinery or its frequency of usage in spite of the common purpose of safety to be secured. Take an example of the space for avoiding the rains and winds (see Fig.1). There are different types of spaces such as tents, wooden houses or office buildings, with the varying basic structures including the bases, skeletons, external walls or roofs. Such a basic structural pattern in the safety-related parts is called a designated architecture, which is a basic form for each category. Each category has its structural requirement to be met.

The dangerous failure rate required for the safety-related parts is different with the categories.

Category	General guideline of requirements	Applicable designated architecture
B	What is required in the safety-related parts in the category is that the target safety function can be achieved. For the fulfillment, the use of the parts is required to tolerate the usage environmental stress as shown below. • Expected operation stress, such as the reliability of the breaking capacity and the frequency of breaking • Chemical impact Example: Corrosion by chemicals • Other external factors Example: Mechanical vibration, electromagnetic noise, interruption or vibration in the control power supply Essentially, the parts are to be selected in conformity with the standard best suited to the purpose. Note: Resistance to the external factors is subject to the relevant standard. It is necessary to design circuit and assemble based on the basic safety principles. As exemplified by NC contact selected to turn off when a wire is disconnected. In category B, which is a single channel system in nature, the safety function is impaired with the occurrence of failure. Category B does not have diagnostic coverage (DCavg = 0%). And CCF is not applied. PL is determined by the channel MTTFd. Maximum PL achievable in the category B is PL = b.	 I :Input device (e.g., sensor) L :Logical operation device O :Output device (e.g., contactor) Note: The above block diagram represents a conceptual view of the channel flow; the number of blocks may be different from the actual electrical circuit diagram. For example, in category B and in category 1, there are cases where an input device (I) and an output device (O) alone are used without a logical operation device (L). On the other hand, there is also a case where three or more blocks may be used.
1	What is required in the safety-related parts in category 1 is high reliability as well as the achievable safety function. So the structure in the safety-related parts is required to be designed and assembled based on the well-tried safety principles with the well-tried components in addition to the category B requirements. Well-tried components apply to either of the following. (See ISO 13849-2 for details.) a) Widely used in the similar usages in the past with the actual achievements. (What are composed of the complicated electronic components, such as general PLC, are not entitled to be included in the track record.) b) Conformity with the safety-related usage and the reliability verified. In category 1, as well as category B, which is a single channel system in nature, the safety function is impaired with the occurrence of a failure. There is no diagnostic range (DCavg = 0%). And CCF is not applied. However, since MTTFb is higher than category B, the safety function is less likely to be impaired than category B. Maximum PL achievable in category 1 is PL = c. Note: "Well-tried parts" and "Fault exclusion" in Section 9. Basic Safety Principles for Risk Reduction in the Failure in the Event of a Fault in Chapter 5" should be clearly distinguished.	

Category	General guideline of requirements	Applicable designated architecture
2	What is required in the safety-related parts in category 2 is to make up for the possible impairment of the safety function caused by the dangerous failure with the supplementary checkup. To achieve this, it is necessary to be able to perform design and assembly based on the well-tried safety principles in addition to the requirements in category B and the checkup function in the machinery control system being capable of checking the safety function in appropriate intervals. The checkup function is composed of the test equipment (TE) and the output device (OTE). Following requirements are observed for checking the safety function. • Check shall be performed on the occasion of the following: - On starting up the machine - Before the occurrence of the hazardous situation (for example, before a new cycle start or periodically if required during operation) • Result of a checkup - Operation shall be approved when no failure is detected - If the failure is found, feed the controlled output of the failure safely. If the output is disabled (e.g., in case of dangerous failure due to a welded contactor), the alarm shall be made to output. The current status shall be retained until the failure is removed. • Hazardous situation shall not be caused by the check itself (such as increased response time for safety function) The safety function may be impaired by the failure between checks in category 2. Maximum PL achievable in the category 2 is PL = d. Note: In ISO 13849-1: 2006, category 2 is handled as redundant system. MTTFd is, however, evaluated for the safety main channels of I, L and O and the check device TE only and not for OTE. DCavg is evaluated only for I, L and O only.	
3	What is required in the safety-related parts in safety category 3 is that even if a portion of the safety function fails, the entire safety function is not impaired. So, in addition to the requirement in category B, it is necessary to be able to design and assemble based on the well-tried safety principles and to have the means to detect the failure in the safety function and, if detected properly, failure is required to be detected on requesting the next safety function operation or earlier. The safety function is maintained by the safety channel redundancy (two channels), interlock based on the feedback from each device and interchannel cross-monitoring. The safety function is not compromised by a single fault, but it could be impaired by the accumulation of the undetected faults. Maximum PL achievable in category 3 is PL = e.	
4	What is required in the safety-related parts in category 4 is that the safety function is not impaired even with a certain amount of the accumulation of faults in the safety function. So, in addition to the requirement in category B, it is necessary to be able to design and assemble based on the well-tried safety principles and to have the means to detect the failure in the safety function and, failure is required to be detected on requesting the next safety function operation or earlier. Configuration of the safety functions is the same as in category 3, but category 4 requires higher performance of failure detection. A higher DCavg yields less likely impairment of the safety function due to the accumulation of faults. Achievable PL in the category 4 is PL = e. Note: Both categories 3 and 4 are configured in redundant system with only difference of DCavg and MTTFd for each channel.	

* Complex structures not applicable to these block diagrams, such as having inputs of three channels or more based on the majority decision logic cannot be handled by ISO 13849-1. If that is a case, it is necessary to use another standard such as IEC 62061.

(2) MTTFd (Mean Time to Dangerous Failure)

This section describes the mean time taken by the safety-related parts leading to a dangerous failure in terms of "MTTFd".

1) Concept of MTTFd

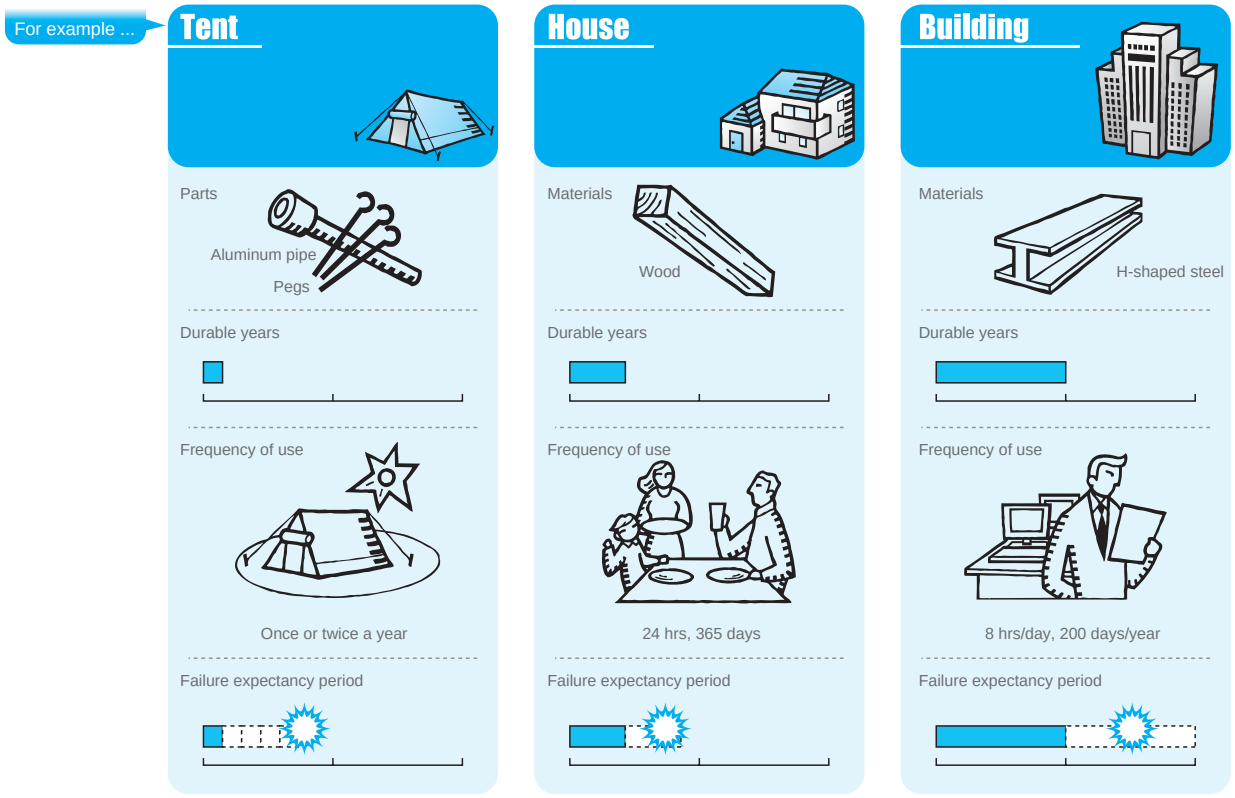


Fig. 2: Parts comprised in a building and failure expectancy period

Tents, wooden houses and office buildings serve the same functions in terms of weatherproofness. Each building has its own life expectancy period, varying with time depending on the housing types.

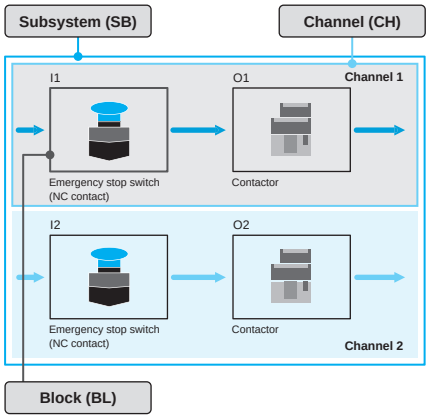
Each element of the parts comprised in the building (see Fig. 2) (e.g., tent support, wooden house beam, building steel frame) has its own inherent failure rate of the materials. Even if a periodical replacement period is observed, the weatherproof durability time varies depending on the frequency of use. The same is true with the safety-related parts control devices.

MTTFd is an expectancy time before dangerous failure, not the durable years of the parts.

2) Layers of MTTFd

Take, for example, the block diagram used in 5. Safety-related Parts PL Evaluation Procedure in Chapter 5. If the device itself is already evaluated as PL in the subsystem, it will be excluded from consideration. For further details, see 8. PL Evaluation in Chapter 5.

Each box in the block diagram represents a singular part (block) featured with its own MTTFd. If some blocks are found in the same channel, an average is taken as MTTFd for the channel. If two channels are used (category 3 and category 4), take further average to yield MTTFd for the total subsystem comprised of singular parts.



3) Discrete component (block) MTTFd

Assign the MTTFd data to each box in the expanded block diagram.

MTTFd in a block (BL) is provided with the following options.

1. Use the data prepared by the parts manufacturers.
2. If manufacturer data are not available, use the data referred to in Annex in ISO 13849-1: 2006.
3. If no data is available, MTTFd is assumed to be 10 years.

If the parts function only when the operation is demanded as a switch or a relay or when the consumption is caused to the parts, the dangerous failure rate is relevant to the count of the operations. The data referred to as B10d are provided to such types of the parts.

B10d: Count of operations until 10% of the parts encounter the dangerous failure

MTTFd for a discrete component is obtained from B10d and the part's mean number of annual operations (nop) per year.

$$MTTFd = \frac{B10d}{0.1 \times nop} \quad \text{(Formula 1)}$$

nop: Total count of operations per year for the target application (Units: cycle/year)

The nop can be obtained from the following formula.

$$nop = \frac{dop \times hop \times 3{,}600}{t_{cycle}} \quad \text{(Formula 2)}$$

tcycle: Average time interval per operation cycle (Units: second/cycle)

hop: Operation time per day (Units: hour/day)

dop: Operating days per year (Units: day/year)

A device designer in this case is required to know how frequently the safety function is requested to operate.

4) MTTFd of channel

On completing the assignment of MTTFd to all blocks, MTTFd is calculated by channel (CH) based on the assignment. Harmonic mean of the MTTFd in all the blocks in the same channel is taken using the following formula.

$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}} \quad \text{(Formula 3)}$$

Two channels are available in the designated architecture in category 3 and category 4 and the calculation is required for both channels.

5) MTTFd of subsystem

If MTTFd is different with channel 1 and channel 2, MTTFd is further averaged in the subsystem (SB) level.

$$MTTFd_{SB} = \frac{2}{3}\left[MTTFd_{CH1} + MTTFd_{CH2} - \frac{1}{\frac{1}{MTTFd_{CH1}} + \frac{1}{MTTFd_{CH2}}}\right] \quad \text{(Formula 4)}$$

If, however, MTTFd is identical in both channel 1 and channel 2, the calculation result in the Eq. 3 is straightforwardly applied to the MTTFd in the subsystem.

Reference

What is Mission Time?

The parts have their own inherent failure rate and the mechanical parts failure increases steeply at a certain time due to the fatigue or aging. The same is true with the dangerous failure rate. The characteristics during the rapidly changing period cannot be used for the evaluation of MTTFd. The dangerous failure rate is assumed to be constant based on the premise that the parts are replaced with the identical parts periodically by the designated usage period for determination of MTTFd of the part. This period of time is called Mission Time.

The designer of the machinery shall consider the following in terms of mission time.

(1) The designer shall define the control system of a machine or the mission time (operating years of an intended machine) of a machine in total.
(2) If T10d for each part used in the control system is shorter than the mission time of the machinery, notify the users of the necessity of the replacement of the part in T10d period.

T10d represents time taken by 10% samples to reach the dangerous failure, to be obtained by the following equation.

$$T10d = \frac{B10d}{nop} \quad \text{(Formula 5)}$$

Reference: MTTFd or B10d for parts referred to in International Standards and their typical values (Source: ISO 13849-1: 2006 Annex C)

	Well-tried basic safety principles in compliance with ISO 13849-2: 2003	Other related Standards	Typical values MTTFd (year) B_{10d} (cycle)
Mechanical components	Tables A.1 and A.2	–	$MTTF_d$ =150
Hydraulic components	Tables C.1 and C.2	EN 982	$MTTF_d$ =150
Pneumatic components	Tables B.1 and B.2	EN 983	B_{10d} =20,000,000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} =20,000,000
Relays and contactor relays with maximum load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} =400,000
Proximity switches with small load (machanical load)	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} =20,000,000
Proximity switches with maximum load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} =400,000
Contactors with small load (mechanical load)	Tables D.1 and D.2	IEC 60947	B_{10d} =20,000,000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B_{10d} =2,000,000
Position switches independent of load *	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} =20,000,000
Position switches (with separate actuator, guard-locking) independent of load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} =2,000,000
Emergency stop devices independent of the load	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} =100,000
Emergency stop devices with maximum operational demands	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} =6,050
Push buttons (e.g. enabling switches) independent of the load)	Tables D.1 and D.2	IEC 60947	B_{10d} =100,000

* Fault exclusion in the direct opening action is only applied to the contact welding failure. If that is a case, that means the relevant B_{10d} is applicable to the switch actuator mechanical failure.

Note:1. For definition and usage of B_{10d}, see Table C. 4 in Annex C in ISO 13849-1: 2006.
Note:2. B_{10d} is estimated as two times B_{10} (50 % dangerous failure).
Note:3. "Small-load" indicates, for example, 20% of the rated value. (See ISO 13849-2 for details)

(3) DC (Diagnostic Coverage) and DCavg

Diagnostic coverage (DC) represents the effectiveness of dangerous failure monitoring of the safety-related parts and the DCavg the averaged values for the safety-related parts or the whole subsystem.

1) Concept of DC

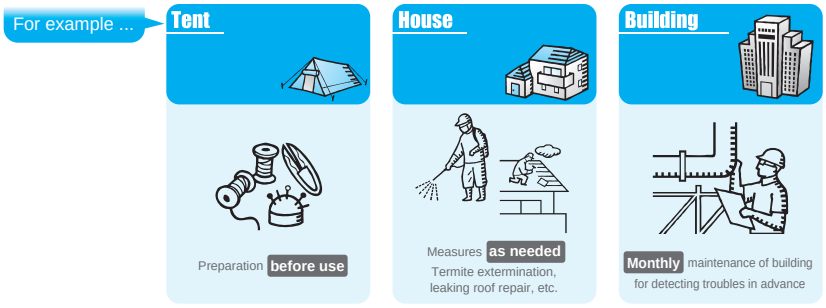


Fig. 3: Effective measures for maintaining building

There are two cases of safety-related parts failures: safety failure and dangerous failure. If the safety-related parts functionalities are met and the usage is appropriate, safety failure is not a problem. If, however, a dangerous failure occurs, there could be two different situations of whether effective measures are taken (see Fig. 3) or not depending on the detectability (diagnostic function). Feasibility (%) to detect the failure and take an effective measure against the dangerous failure is represented by the DC.

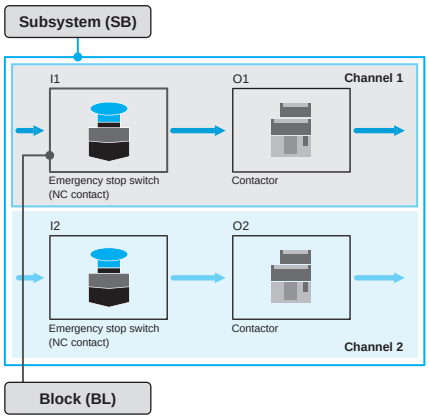
A certain level of DC is required for the category for achievement of the PLr needed for the safety functions. In association with the building in a preceding example, as far as a tent is concerned, repairing once a year before use would be quite OK. If, on the other hand, in case of a wooden housing for daily life, immediate action is required for termite or leaky roof being found. With the office buildings, unless proactive actions are taken in anticipation of the possible troubles through the periodical maintenance, a large disaster may be encountered. So, the required level of diagnostics shall be complied with the relevant structure.

For further details, see (1) Category in 6. Subsystem Configured in Discrete Components in Chapter 5.

2) Layers of DC

Take, for example, the block diagram used in Section 5. Safety-Related Parts PL Evaluation Procedure in Chapter 5. If the device itself is already evaluated as PL in the subsystem, it will be excluded from consideration.

For further details, see 8. PL Evaluation in Chapter 5.



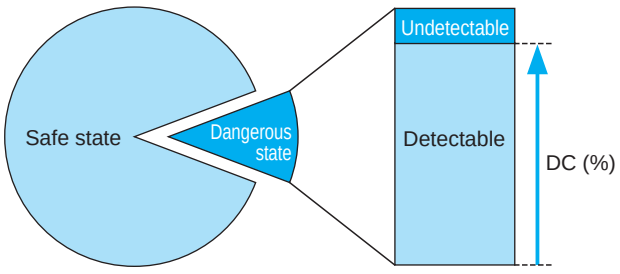
Each block in the block diagram box is provided with the individual DC. DCs in all the blocks averaged out by the subsystem levels are called DCavg (DC Average).

Note: Architecture which requires the evaluation of the DC and DCavg is the designated structure of category 2 or more having the monitoring capability. The evaluation is not needed for the designated architecture of category B or category 1.

3) DC for a block

Discrete parts (such as switches or contactors) are not usually provided with the diagnostic functions by themselves. The state of those devices, however, are mostly monitored by the diagnostics of other devices (such as safety controllers). So, it is necessary for the device designers to determine what constitutes the failure diagnostics with the comparison with the controller function.

Select the relevant DC from Table 1 in Annex E in ISO 13849-1 by considering what safety design principles are used in the failure diagnostics and asign their values into each block.



Safety-related parts failure: safe or dangerous?

Dangerous failure: Detectable (effective measures taken?) or undetectable

Reference: Evaluating the diagnostic coverage (DC) (Source: ISO 13849-1: 2006 Annex E)

Input device	
Measure	DC
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input 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 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

Logic	
Measure	DC
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %
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)
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 %
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 %
Invariable memory: signature of one word (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	99 %
Variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timers and cross comparison of these data	60 %
Variable memory: check for readability and write ability of used data memory cells	60 %
Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!

Output device	
Measure	DC
Monitoring of outputs by one channel without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
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 %
Redundant shut-off path with no monitoring of the actuator	0 %
Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depnding on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %

Note:1. For additional evaluation of the DC, see Table A.2 to A.15 in IEC 61508-2: 2000.
Note:2. If Medium or High DC is required for the logical operation devices, it is needed to apply a measure having a minimum 60% DC for variable memory, invariable memory and process devices. There are other measures than those described in this table.

4) Examples of DC application to discrete parts

Following is a table showing the discrete components of the typical safety-related parts to which the Table 1 in the Annex E is applied.

Parts	DC (%)	Annex E relevant items	Preconditions
Combination of two switches	99	Validation check (input device)	• At least one of the switches is provided with the direct opening action. • Interchannel cross-monitoring being performed by the safety controller where two switches are hazardously connected (via a guard)* • Separately conformed with the requirements of ISO 14119 (guard-linked interlocking device)
Relays	99	Direct monitoring (logical operation device) -Electromechanical device monitoring by mechanically linked contact	• Provided with enforced guide contact mechanism • Fed back to the safety controller and being monitored
Contactor	99	Direct monitoring (output device) -Electromechanical device monitoring by mechanically linked contact	• Provided with a mirror contact • Fed back to the safety controller and being monitored

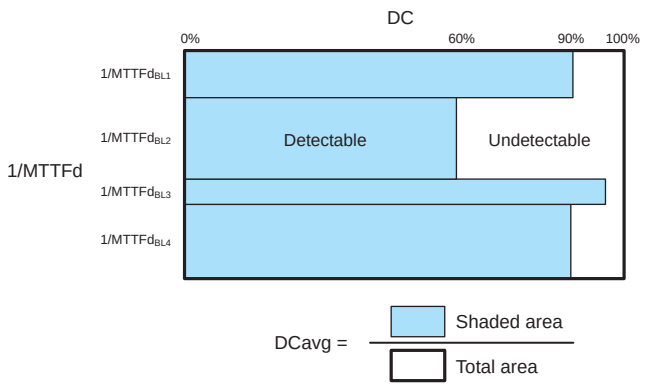
* Since a diagnostic function is different with controllers, DC being given could also be different. For further detail, contact a respective control device manufacturer.

5) DCavg in subsystem

Average out the DC values for all the blocks (BL) comprising the subsystem (SB) for DCavg.

$$DCavg = \frac{\sum_{i=1}^{n} \frac{DC_{BLi}}{MTTFd_{BLi}}}{\sum_{i=1}^{n} \frac{1}{MTTFd_{BLi}}}$$ (Formula 6)

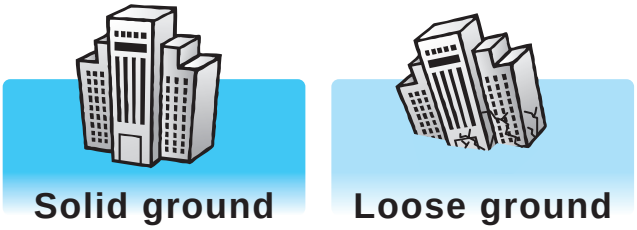
DCavg is weighted by MTTFd in each block. This is shown in the Figure on the right. This means that a block of the smaller MTTFd (less reliable) in the subsystem gives a larger impact to DCavg.



(4) CCF (Common Cause Failure)

Common cause failure (CCF) is a tolerance to the simultaneous failure in channels in the designated architecture (including category 2) of two or more channels.

Concept of CCF



Common cause failure (CCF) is generally a term to describe the failure mode in which multiple systems are impaired by a common cause, but as PL parameters, it is used to represent the level of tolerance against the simultaneous failure of channels.
CCF is, as it were, a reliability index in terms of engineering management for the safety-related parts design and construction. This is similar to the ground on which a building is established; even a strong building erected on the weak ground is susceptible to collapse.

CCF is to be evaluated by the device designers using scores based on the design specifications margins, parts positioning on the actual devices or wiring states, not the evaluation on the block diagrams. Evaluation score may vary depending on how much effective safety principles are used for eliminating the common causes. Items for consideration on design are standardized in Table F.1 in Annex F.1 in ISO 13849-1 in check sheet form. Select check boxes for the relevant items and add together the score. Make a decision whether the total score exceeds 65 points. CCF score of 65 points or more is required for the designated architecture of redundancy of category 2 or more. For details of category, see (1) Category in 6. Subsystem Configured in Discrete Components in Singular Parts in Chapter 5.

Table F.1 in Annex F in ISO 13849-1

(Source: Annex F in ISO 13849-1: 2006)

No.	Measures against Common Cause Failures (CCF)	Score
1	**Separation/segregation**	
	Physical separation between the signal paths for example separation of wiring/piping for example sufficient creepage and clearance on printed circuit boards	15
2	**Diversity**	
	Using different technologies/design or physical principles for example first channel in programmable electronic and second channel hardwired for example type of initiation for example pressure and temperature Measuring distance and pressure for example digital and analog Components supplied from different manufacturers.	20
3	**Design/application/experience**	
3.1	Protection against overvoltage, overpressure, overcurrent etc.	15
3.2	Using well-tried components	5
4	**Assessment/analysis**	
	Have the results of the analysis of failure types and effects been considered in order to avoid common causes failures in future design	5
5	**Competence/training**	
	Have designers/mechanics been trained in understanding the causes and consequences of failures with a common cause	5
6	**Environment**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in compliance with the respective standards Fluid systems: Filtering of the pressure medium, prevention of dirt intake, drainage of compressed air, for example in compliance with the requirements of the manufacturer responsible for the purity of the media, Electric systems: Has the system been tested for electromagnetic compatibility, for example as specified against CCF in the respective standards. For combined fluid and electric systems, both requirements should be considered.	25
6.2	Other influences Have all requirements for immunity against all relevant environmental factors such as temperature, shock, vibration, humidity (for example as stipulated in the respective standards) been considered	10
	Total	**[maximum 100]**

Total score	Measures to prevent Common Cause Failures
65 or more	Requirements fulfilled
Less than 65	Process failed ⇒Choose additional measures

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

1) What is PFHd ?

PFHd is a parameter derived from the conceptual view of the functional safety. That represents a very tiny figure, meaning a count of the latent hazardous failure (probability of dangerous failure) per hour with a certain device.
Reliability (dangerous failure rate) in the safety-related parts can be obtained by the sum of PFHd of all the subsystems comprised. Technical file ISO/TR 23849 as a guidance of ISO 13849-1 authenticates the reliability data for safety of machinery for the dangerous failure evaluated in IEC 62061 based on the functional safety to be used as the PL assessment parameters and PFHd for the subsystem comprised of the discrete parts can be obtained by the conversion from the four parameters of category, MTTFd, DCavg and CCF.

2) Conversion into PFHd

For conversion from the category, MTTFd, DCavg and CCF into PFHd, the Table K.1 in the Annex K in ISO 13849-1 is used.
As shown in the table below, PFHd is represented by a decimal number of mantissa and exponent.
Source: ISO 13849-1: 2006, Annex K, Table K.1

Category		B	1	2		3		4
DCavg		None		Low 60≤DCavg	Medium 90≤DCavg	Low 60≤DCavg	Medium 90≤DCavg	High 99≤DCavg
CCF		Not relevant		65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF
Low	3≤MTTFd	3.80×10^{-5}		2.58×10^{-5}	1.99×10^{-5}	1.26×10^{-5}	6.09×10^{-6}	
	3.3≤MTTFd	3.46×10^{-5}		2.33×10^{-5}	1.79×10^{-5}	1.13×10^{-5}	5.41×10^{-6}	
	3.6≤MTTFd	3.17×10^{-5}		2.13×10^{-5}	1.62×10^{-5}	1.03×10^{-5}	4.86×10^{-6}	
	3.9≤MTTFd	2.93×10^{-5}		1.95×10^{-5}	1.48×10^{-5}	9.37×10^{-6}	4.40×10^{-6}	
	4.3≤MTTFd	2.65×10^{-5}		1.76×10^{-5}	1.33×10^{-5}	8.39×10^{-6}	3.89×10^{-6}	
	4.7≤MTTFd	2.43×10^{-5}		1.60×10^{-5}	1.20×10^{-5}	7.58×10^{-6}	3.48×10^{-6}	
	5.1≤MTTFd	2.24×10^{-5}		1.47×10^{-5}	1.10×10^{-5}	6.91×10^{-6}	3.15×10^{-6}	
	5.6≤MTTFd	2.04×10^{-5}		1.33×10^{-5}	9.87×10^{-6}	6.21×10^{-6}	2.80×10^{-6}	
	6.2≤MTTFd	1.84×10^{-5}		1.19×10^{-5}	8.80×10^{-6}	5.53×10^{-6}	2.47×10^{-6}	
	6.8≤MTTFd	1.68×10^{-5}		1.08×10^{-5}	7.93×10^{-6}	4.98×10^{-6}	2.20×10^{-6}	
	7.5≤MTTFd	1.52×10^{-5}		9.75×10^{-6}	7.10×10^{-6}	4.45×10^{-6}	1.95×10^{-6}	
	8.2≤MTTFd	1.39×10^{-5}		8.87×10^{-6}	6.43×10^{-6}	4.02×10^{-6}	1.74×10^{-6}	
	9.1≤MTTFd	1.25×10^{-5}		7.94×10^{-6}	5.71×10^{-6}	3.57×10^{-6}	1.53×10^{-6}	
Medium	10≤MTTFd	1.14×10^{-5}		7.18×10^{-6}	5.14×10^{-6}	3.21×10^{-6}	1.36×10^{-6}	
	11≤MTTFd	1.04×10^{-5}		6.44×10^{-6}	4.53×10^{-6}	2.81×10^{-6}	1.18×10^{-6}	
	12≤MTTFd	9.51×10^{-6}		5.84×10^{-6}	4.04×10^{-6}	2.49×10^{-6}	1.04×10^{-6}	
	13≤MTTFd	8.78×10^{-6}		5.33×10^{-6}	3.64×10^{-6}	2.23×10^{-6}	9.21×10^{-7}	
	15≤MTTFd	7.61×10^{-6}		4.53×10^{-6}	3.01×10^{-6}	1.82×10^{-6}	7.44×10^{-7}	
	16≤MTTFd	7.13×10^{-6}		4.21×10^{-6}	2.77×10^{-6}	1.67×10^{-6}	6.76×10^{-7}	
	18≤MTTFd	6.34×10^{-6}		3.68×10^{-6}	2.37×10^{-6}	1.41×10^{-6}	5.67×10^{-7}	
	20≤MTTFd	5.71×10^{-6}		3.26×10^{-6}	2.06×10^{-6}	1.22×10^{-6}	4.85×10^{-7}	
	22≤MTTFd	5.19×10^{-6}		2.93×10^{-6}	1.82×10^{-6}	1.07×10^{-6}	4.21×10^{-7}	
	24≤MTTFd	4.76×10^{-6}		2.65×10^{-6}	1.62×10^{-6}	9.47×10^{-7}	3.70×10^{-7}	
	27≤MTTFd	4.23×10^{-6}		2.32×10^{-6}	1.39×10^{-6}	8.04×10^{-7}	3.10×10^{-7}	
High	30≤MTTFd		3.80×10^{-6}	2.06×10^{-6}	1.21×10^{-6}	6.94×10^{-7}	2.65×10^{-7}	9.54×10^{-8}
	33≤MTTFd		3.46×10^{-6}	1.85×10^{-6}	1.06×10^{-6}	5.94×10^{-7}	2.30×10^{-7}	8.57×10^{-8}
	36≤MTTFd		3.17×10^{-6}	1.67×10^{-6}	9.39×10^{-7}	5.16×10^{-7}	2.01×10^{-7}	7.77×10^{-8}
	39≤MTTFd		2.93×10^{-6}	1.53×10^{-6}	8.40×10^{-7}	4.53×10^{-7}	1.78×10^{-7}	7.11×10^{-8}
	43≤MTTFd		2.65×10^{-6}	1.37×10^{-6}	7.34×10^{-7}	3.87×10^{-7}	1.54×10^{-7}	6.37×10^{-8}
	47≤MTTFd		2.43×10^{-6}	1.24×10^{-6}	6.49×10^{-7}	3.35×10^{-7}	1.34×10^{-7}	5.76×10^{-8}
	51≤MTTFd		2.24×10^{-6}	1.13×10^{-6}	5.80×10^{-7}	2.93×10^{-7}	1.19×10^{-7}	5.26×10^{-8}
	56≤MTTFd		2.04×10^{-6}	1.02×10^{-6}	5.10×10^{-7}	2.52×10^{-7}	1.03×10^{-7}	4.73×10^{-8}
	62≤MTTFd		1.84×10^{-6}	9.06×10^{-7}	4.43×10^{-7}	2.13×10^{-7}	8.84×10^{-8}	4.22×10^{-8}
	68≤MTTFd		1.68×10^{-6}	8.17×10^{-7}	3.90×10^{-7}	1.84×10^{-7}	7.68×10^{-8}	3.80×10^{-8}
	75≤MTTFd		1.52×10^{-6}	7.31×10^{-7}	3.40×10^{-7}	1.57×10^{-7}	6.62×10^{-8}	3.41×10^{-8}
	82≤MTTFd		1.39×10^{-6}	6.61×10^{-7}	3.01×10^{-7}	1.35×10^{-7}	5.79×10^{-8}	3.08×10^{-8}
	91≤MTTFd		1.25×10^{-6}	5.88×10^{-7}	2.61×10^{-7}	1.14×10^{-7}	4.94×10^{-8}	2.74×10^{-8}
	100≤MTTFd		1.14×10^{-6}	5.28×10^{-7}	2.29×10^{-7}	1.01×10^{-7}	4.29×10^{-8}	2.47×10^{-8}

How to use Table K.1 in Annex K in ISO 13849-1

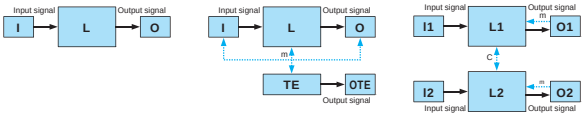
Conversion example into PFHd is shown below.

PL parameter

Usage (example)

Category

Designated architecture (configuration of I. L and O)



Designated architecture corresponds to Cat 3.

MTTFd

- B10d
- nop*

* The machine designer him/herself needs to know nop.

(1) Component block

* The machine designer him/herself needs to know Nop.

1. Use MTTFd provided by the manufacturer
2. Use MTTFd specified in Annex C
3. When B10d is provided, convert into MTTFd from the formula on the right

$$MTTFd = \frac{B10d}{0.1 \times N_{OP}}$$

(2) Channel

$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

(3) Entire subsystem

If Channel 1 and Channel 2 MTTFd are equivalent, assume the equation 2 result as MTTFd for the subsystem. MTTFd for the subsystem, however, is limited up to 100 years.

$$MTTFd = \frac{2}{3}\left[MTTFdc1 + MTTFdc2 - \frac{1}{\frac{1}{MTTFdc1} + \frac{1}{MTTFdc2}}\right]$$

Subsystem MTTFd calculation result is 40 years.

DCavg

- DC
- MTTFd

(1) Component block ⇨ Select the relevant DC from Table 1 in Annex E

(3) Entire subsystem

$$DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

Subsystem DCavg calculation result is 80%.

CCF

The score in the checklist in Annex F must be 65 or over

Check list score is 75.

Category		B	1	2		3		4
DCavg		None		Low 60≤DC	Medium g	Low 60≤DCavg	Medium 90≤DCavg	High 99≤DCavg
CCF		Not relevant		65 ≤ C	F	65 ≤ CCF		
Low	3≤MTTFd	a 3.80×10^{-5}		a 2.5		a 1.26×10^{-5}	b	
	3.3≤MTTFd	a 3.46×10^{-5}		a 2.3		a 1.13×10^{-5}	b 5.41×10	
	3.6≤MTTFd	a 3.17×10^{-5}		a 2.1	a 1.62×10	a 1.03×10^{-5}	b 4.86×10^{-6}	
	3.9≤MTTFd	a 2.93×10^{-5}		a 1.95×10^{-5}	a 1.48×10^{-5}	b 9.37×10^{-6}	b 4.40×10^{-6}	
	4.3≤MTTFd	a 2.65×10^{-5}		a 1.76×10^{-5}	a 1.33×10^{-5}	b 8.39×10^{-6}	b 3.89×10^{-6}	
	4.7≤MTTFd	a 2.43×10^{-5}		a 1.60×10^{-5}	a 1.20×10^{-5}	b 7.58×10^{-6}	b 3.48×10^{-6}	
	5.1≤MTTFd	a 2.24×10^{-5}		a 1.47×10^{-5}	a 1.10×10^{-5}	b 6.91×10^{-6}	b 3.15×10^{-6}	
	5.6≤MTTFd	a 2.04×10^{-5}		a 1.33×10^{-5}	b 9.87×10^{-6}	b 6.21×10^{-6}	c 2.80×10^{-6}	
	6.2≤MTTFd	a 1.84×10^{-5}		a 1.19×10^{-5}	b 8.80×10^{-6}	b 5.53×10^{-6}	c 2.47×10^{-6}	
	6.8≤MTTFd	a 1.68×10^{-5}		a 1.08×10^{-5}	b 7.93×10^{-6}	b 4.98×10^{-6}	c 2.20×10^{-6}	
	7.5≤MTTFd	a 1.52×10^{-5}		b 9.75×10^{-6}	b 7.10×10^{-6}	b 4.45×10^{-6}	c 1.95×10^{-6}	
	8.2≤MTTFd	a 1.39×10^{-5}		b 8.87×10^{-6}	b 6.43×10^{-6}	b 4.02×10^{-6}	c 1.74×10^{-6}	
	9.1≤MTTFd	a 1.25×10^{-5}		b 7.94×10^{-6}	b 5.71×10^{-6}	b 3.57×10^{-6}	c 1.53×10^{-6}	
Medium	10≤MTTFd	a 1.14×10^{-5}		b 7.18×10^{-6}	b 5.14×10^{-6}	b 3.21×10^{-6}	c 1.36×10^{-6}	
	11≤MTTFd	a 1.04×10^{-5}		b 6.44×10^{-6}	b 4.53×10^{-6}	c 2.81×10^{-6}	c 1.18×10^{-6}	
	12≤MTTFd	b 9.51×10^{-6}		b 5.84×10^{-6}	b 4.04×10^{-6}	c 2.49×10^{-6}	c 1.04×10^{-6}	
	13≤MTTFd	b 8.78×10^{-6}		b 5.33×10^{-6}	b 3.64×10^{-6}	c 2.23×10^{-6}	d 9.21×10^{-7}	
	15≤MTTFd	b 7.61×10^{-6}		b 4.53×10^{-6}	b 3.01×10^{-6}	c 1.82×10^{-6}	d 7.44×10^{-7}	
	16≤MTTFd	b 7.13×10^{-6}		b 4.21×10^{-6}	c 2.77×10^{-6}	c 1.67×10^{-6}	d 6.76×10^{-7}	
	18≤MTTFd	b 6.34×10^{-6}		b 3.68×10^{-6}	c 2.37×10^{-6}	c 1.41×10^{-6}	d 5.67×10^{-7}	
	20≤MTTFd	b 5.71×10^{-6}		b 3.26×10^{-6}	c 2.06×10^{-6}	c 1.22×10^{-6}	d 4.85×10^{-7}	
	22≤MTTFd	b 5.19×10^{-6}		c 2.93×10^{-6}	c 1.82×10^{-6}	c 1.07×10^{-6}	d 4.21×10^{-7}	
	24≤MTTFd	b 4.76×10^{-6}		c 2.65×10^{-6}	c 1.62×10^{-6}	d 9.47×10^{-7}	d 3.70×10^{-7}	
	27≤MTTFd	b 4.23×10^{-6}		c 2.32×10^{-6}	c 1.39×10^{-6}	d 8.04×10^{-7}	d 3.10×10^{-7}	
High	30≤MTTFd		b 3.80×10^{-6}	c 2.06×10^{-6}	c 1.21×10^{-6}	d 6.94×10^{-7}	d 2.65×10^{-7}	e 9.54×10^{-8}
	33≤MTTFd		b 3.46×10^{-6}	c 1.85×10^{-6}	c 1.06×10^{-6}	d 5.94×10^{-7}	d 2.30×10^{-7}	e 8.57×10^{-8}
	36≤MTTFd		b 3.17×10^{-6}	c 1.67×10^{-6}	d 9.39×10^{-7}	d 5.16×10^{-7}	d 2.01×10^{-7}	e 7.77×10^{-8}
	39≤MTTFd		c 2.93×10^{-6}	c 1.53×10^{-6}	d 8.40×10^{-7}	d 4.53×10^{-7}	d 1.78×10^{-7}	e 7.11×10^{-8}
	43≤MTTFd		c 2.65×10^{-6}	c 1.37×10^{-6}	d 7.34×10^{-7}	d 3.87×10^{-7}	d 1.54×10^{-7}	e 6.37×10^{-8}
	47≤MTTFd		c 2.43×10^{-6}	c 1.24×10^{-6}	d 6.49×10^{-7}	d 3.35×10^{-7}		
	51≤MTTFd			10⁻⁶	d 5.80×10^{-7}	d 2.93×10^{-7}		
	56≤MTTFd			10⁻⁶	d 5.10×10^{-7}	d 2.52×10^{-7}		
	62≤MTTFd			10⁻⁷	d 4.43×10^{-7}	d 2.13×10^{-7}		
	68≤MTTFd		c 1.68×10^{-6}	d 8.17×10^{-7}	d 3.90×10^{-7}	d 1.84×10^{-7}		
	75≤MTTFd		c 1.52×10^{-6}	d 7.31×10^{-7}	d 3.40×10^{-7}	d 1.57×10^{-7}		
	82≤MTTFd		c 1.39×10^{-6}	d 6.61×10^{-7}	d 3.01×10^{-7}	d 1.35×10^{-7}	e 5.79×10^{-8}	e 3.08×10^{-8}
	91≤MTTFd		c 1.25×10^{-6}	d 5.88×10^{-7}	d 2.61×10^{-7}	d 1.14×10^{-7}	e 4.94×10^{-8}	e 2.74×10^{-8}
	100≤MTTFd		c 1.14×10^{-6}	d 5.28×10^{-7}	d 2.29×10^{-7}	d 1.01×10^{-7}	e 4.29×10^{-8}	e 2.47×10^{-8}

Cat3 domain selected

Confirm the range 65 ≤ CCF

Focused to domain equivalent to 60 ≤ Dcavg < 90

Domain equivalent to 39 ≤ MTTFd < 43 selected

Crossed portion represents PL and PFHd for this channel

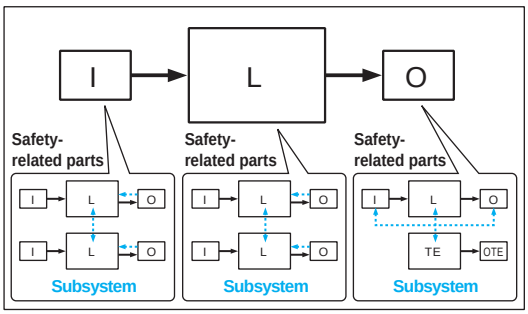
7. Complex Subsystem

The individual subsystem corresponds to the devices cited in 5. Safety-related Parts PL Evaluation Procedure in Chapter 5. Safety-Related Parts PL Evaluation Procedure in Chapter 5. The internal hardware structure is represented in the designated architecture. If the reliability of the devices themselves is already evaluated by ISO 13849-1 and the subsystem categories, MTTFd and DCavg data are provided by the control device manufacturers, they are converted into PFHd using the Table K.1 in Annex K in ISO 13849-1.

There are some safety devices having the complex electronic circuits which are evaluated based on IEC 62061 or IEC 61508. If that is a case, the performance of the safety devices is evaluated by Safety Integrity Level (SIL). PFHd is also used for SIL evaluation, and the level is subdivided as with PL evaluation by PFHd exponents. There is an equivalency relation between PL and SIL via PFHd. That indicates that the PFHd value data for the safety devices certified by IEC 62061 or IEC 61508 can be straightforwardly used for PL evaluation once the data are supplied by the manufacturers.

It is, however, needed to have met the overall requirements of ISO 13849-1 in addition to those of PFHd. Note that there are some cases where SIL is not compatible with the size of PFHd, depending on the hardware structure because of the restrictions called SIL claim limit.

Safety-related parts (entire system)



PL	PFHd		SIL*
	Mantissa	Exponent	
a	10 > n ≥ 1	x10^{-5}	Not supported
b	10 > n ≥ 3	x10^{-6}	1
c	3 > n ≥ 1	x10^{-6}	1
d	10 > n ≥ 1	x10^{-7}	2
e	10 > n ≥ 1	x10^{-8}	3

*(IEC 61508-1, Evaluation by high-frequency operation mode)

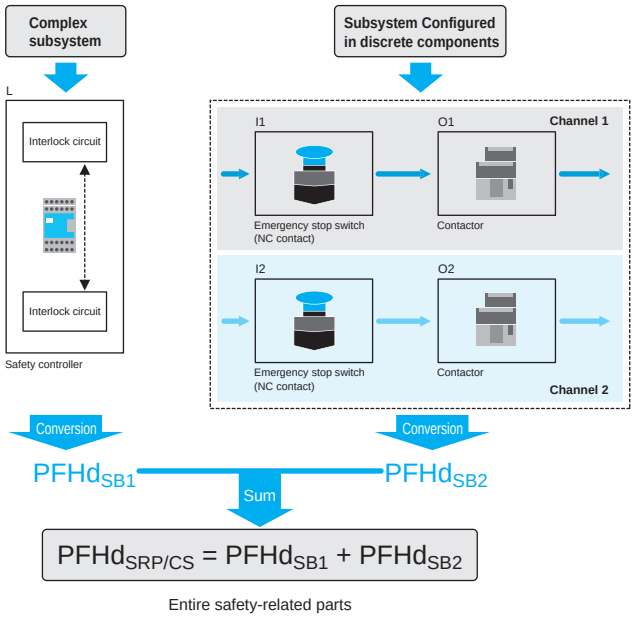
8. PL Evaluation

This section describes the final determination of PL for the safety-related parts by concatenating multiple subsystems.

1) Combination of Subsystems

PL for the entire safety-related parts is evaluated by the summation of the dangerous failure rate in all the subsystems.
Add PFHd of the subsystems configured in discrete components and PFHd of all other complex subsystems.

$$PFHd_{SRP/CS} = \sum_{i=1}^{n} PFHd_{SBn}$$



2) PL Estimation

PL for the overall safety-related parts is determined by the exponent size of the floating point as a result of summation of the PFHd in the subsystem.

If the sum of the PFHd is 1.50 x 10^{-7}, the exponential portion is -7th power of 10, indicating the PL for the entire safety-related parts is d according to the Table below.
This completes the PL determination for one safety function system. Return to 3. Organizing Safety Functions and Hazards in Chapter 5 and repeat the procedure of PL determination for all other safety function systems.

However, if SIL (and corresponding PL) is found restricted by SIL claim limit in a series of subsystems, there could be cases where PL for the overall safety-related parts cannot be determined by PFHd alone.

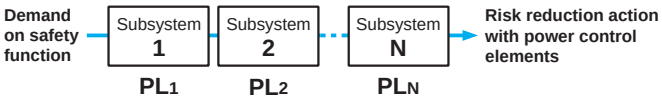
(Source: ISO 13849-1: 2006)

PFHd		PL
Mantissa	Exponent	
10 > n ≥ 1	10^{-5}	a
10 > n ≥ 3	10^{-6}	b
3 > n ≥ 1	10^{-6}	c
10 > n ≥ 1	10^{-7}	d
10 > n ≥ 1	10^{-8}	e

Remark:
To achieve the PL determination, the dangerous failure average rate per hour and other measures are needed.

3) Simplified estimation

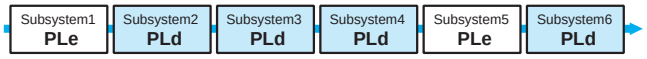
If PL as a subsystem only is declared by a control device manufacturer and the detailed data of PFHd is not available, the following procedure allows a simplified evaluation of PL for the entire safety-related parts with the subsystem PL alone.
This method allows the PL of the safety-related parts to be evaluated when there is nonconformity between PL and PFHd values because of the SIL claim limit in the subsystems.



1. Identify the lowest PL (PLlow) in each subsystem.
2. Identify the number of subsystems (Nlow) having the same PLow.
3. Estimate according to the Table on the right.

PL low	N low	PL
a	4 or more	None
	Up to 3	a
b	3 or more	a
	Up to 2	b
c	3 or more	b
	Up to 2	c
d	4 or more	c
	Up to 3	d
e	4 or more	d
	Up to 3	e

With the combination of the following subsystems, for example:



PL	Count (N)
e	2
d	4

PL for the safety-related parts as a whole is PLc.

Note: Calculation method used
(1) Derive overall PL from the summation of PFHd for the subsystems.
(2) Derive overall PL from the count of PLlow for the subsystems.
The above method does not show the compatibility between ISO 13849-1: 2006 and IEC 62061.
The values of PFHd alone do not testify to the conformity with ISO 13849-1: 2006.
Moreover, PL determination achieved does not validate the conformity with IEC 62061 or IEC 61508.
In addition to PFHd or MTTFd values, confirmation or certification that the parts meet the ISO 13849-1: 2006 requirements such as category or CCF.

9. Basic Safety Principles for Risk Reduction in the Failure

If the electric device failures or disturbances cause the hazardous situation and the machines or works during process are threatened to be impaired, necessary actions shall be taken to minimize the jeopardy. This section describes the typical means for minimizing the failure risks based on the IEC 60204-1.

• Applying the ISO 13849-1 or IEC 62061 requirements

The control circuit should maintain the appropriate safety performance level determined by the risk assessment.
See 2. Relationship between Risk Assessment and PL in Chapter 5.

(1) Description in IEC 60204-1

1) Use of well-tried circuit principles and components

1. Basic circuit configuration in consideration of earth failure

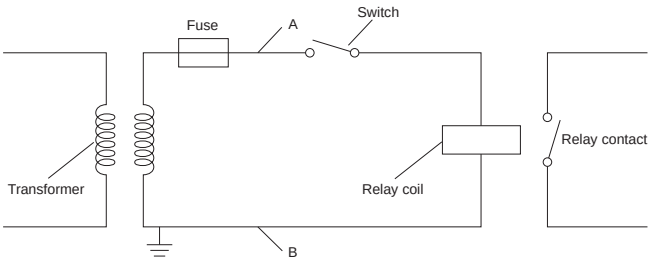
Typical actions taken are shown below.

• Basic circuit configuration

Precautions on configuration are shown below on designing the safety circuit for the control system.

(1) Relay contact in the safety circuit is to be opened by non-exciting coil.
(2) Connect one line of the safety circuit in the secondary winding of the isolation transformer to the earth.
(3) Place all the coils in the safety circuit as closest to the earth line as possible for direct connection.
(4) Be sure to attach the fuse to the safety circuit.

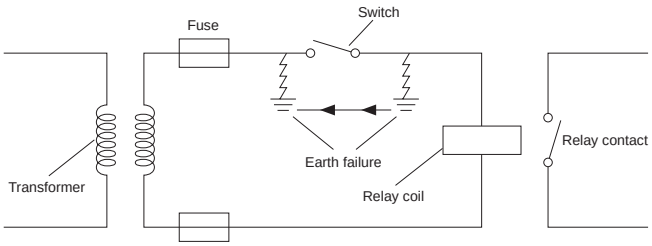
Shown below is a basic configuration of the safety circuit with the items (1) to (4) included in the above.



If the earth failure occurs on the switch line A, a fuse is blown with the path shut off.
Because a coil line B is earthed, there is no earth failure.

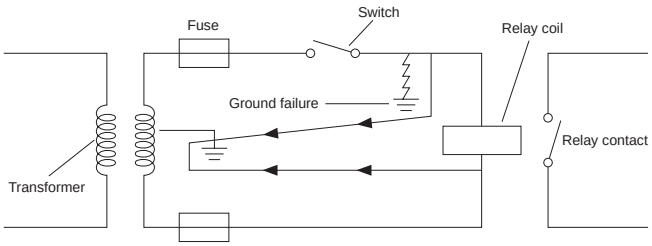
• Earth failure example

The safety circuit is not earthed



A switch is bypassed by two earth failures, causing a sudden start or stop of a machine.

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



A single earth failure causes the relay coil to keep 50% of voltage applied, subject to the inability to stop the machine.

2. Measures provided ready to shut off or stop the hazards based on the stoppage principle.

For details, see Chapter 1. Safety Secured by De-energizing.

3. Safety regulation certified parts used.

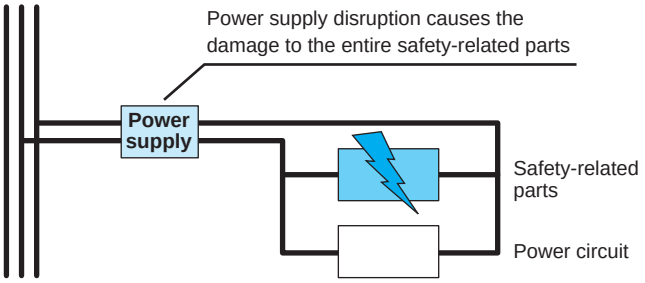
Safety regulation certification is one issued by the third-party certificate authority such as TÜV.

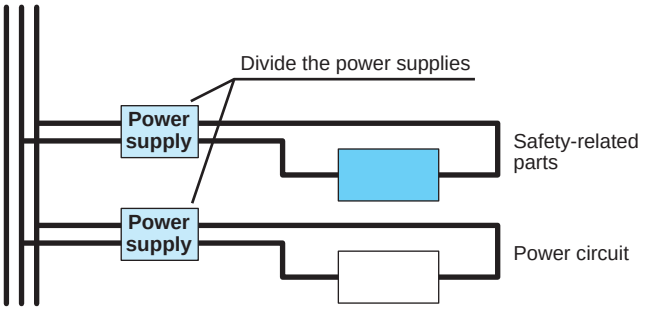
4. Safety switch to be used for reliable opening operation

The certified product is labeled as ⊣ mark.

5. Safety-related parts function shall not be impaired by a single power failure.

Isolate the power supplies of the power systems from the safety-related parts.





2) Periodical functional test

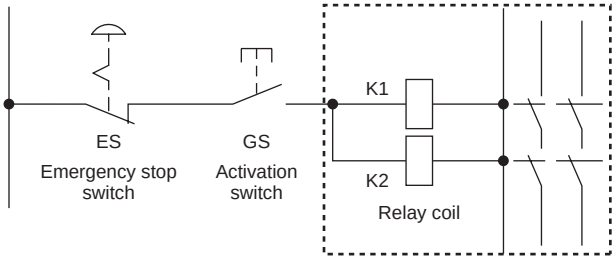
Perform the safety-related functional test either automatically via the control system or manually.
Start the test at the beginning of the business hours and for a certain period of days. If a failure is detected, be sure not to restart the machine until the cause is clarified.

3) Having the redundancy

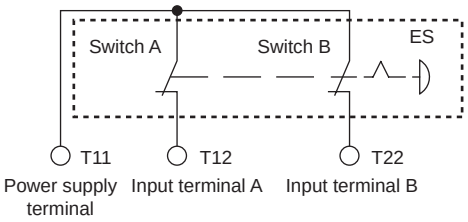
Providing a partial or overall redundancy would minimize the risk caused by a single failure by the electric circuit.

For example, by combining two or more relays or switches, a circuit function is kept even if a single part is encountered with a failure as shown below.

- **Example of redundant outputs by using two relays**



- **Example of redundant inputs by using two contacts**



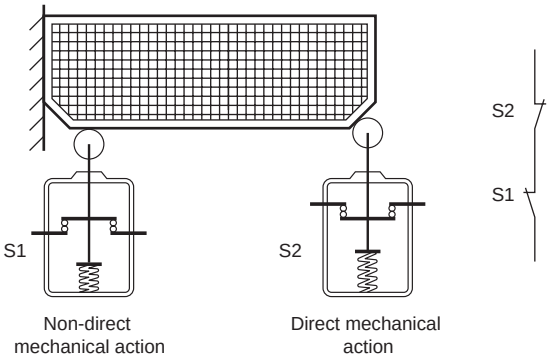
4) Use of diversity

Same type of devices under the redundant configuration could be failed at the same time under the same conditions. Using the control circuits of the diversified principles or various types of devices or parts could reduce the failure rate due to the identical, common causes.
Examples of diverse parts or devices in usage are as follows.

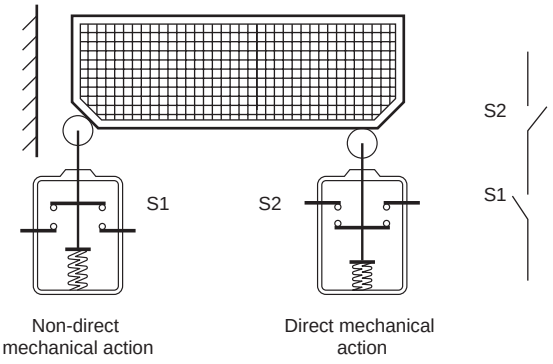
1. Operating the movable guard with a combination of NC contact and NO contact

- **Example of operating the movable guard with a combination of negative and positive operation switches**

<contacts closed> (guard closed)



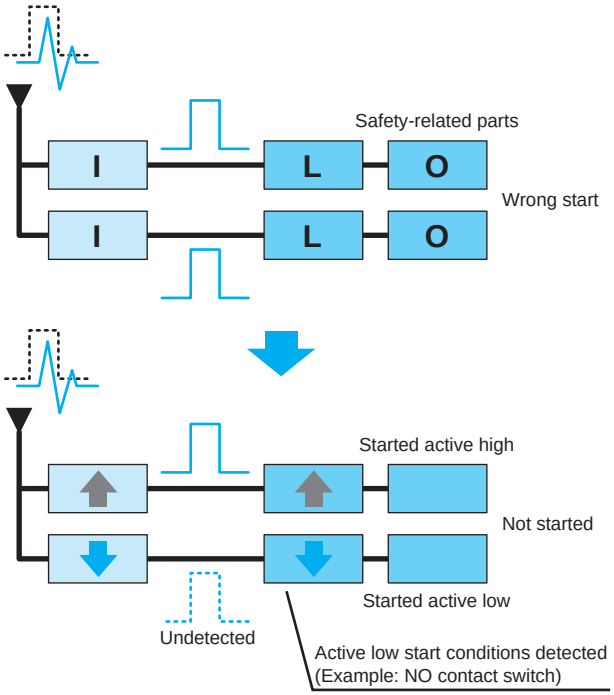
<contacts open> (guard open)



2. Using different types of control parts in a circuit

- **Combination example of active high and active low operation sensors**

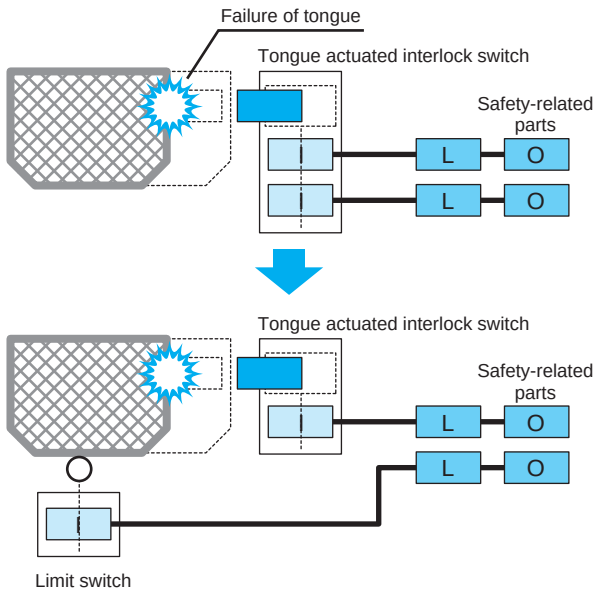
Erroneous signals could be input into channel 1 and channel 2 by noise on the occasion of surge.
By reversing the logic and phase of the signals into channel 1 and channel 2, the noise of the same phase can be eliminated.



3. Redundant configuration by combining electric-mechanical circuits and electronic circuits.

- **Example of sharing different types of switches**

Open/closed guard is detected by two different detection means. A single door switch of key-in type alone could cause an unlocked key to be a common cause failure. If this risk cannot be eliminated, a different type of a switch such as a limit switch should be additionally used.

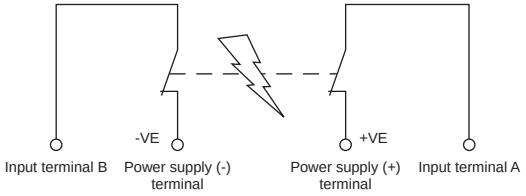


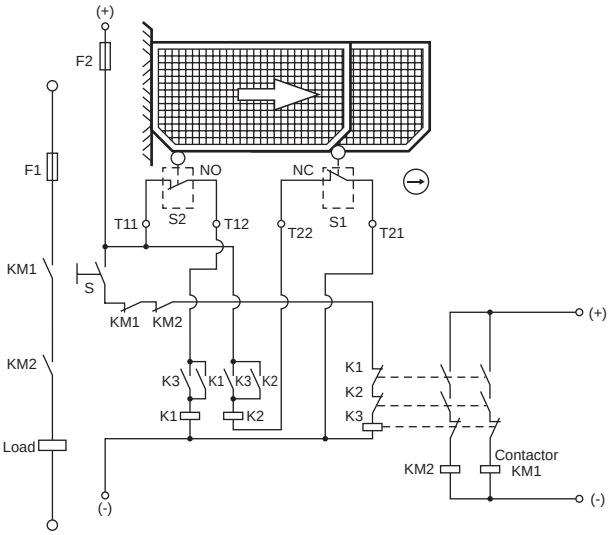
Note: It is necessary to determine the type of switches or its usage based on the risk assessment results or Type C standard request.

5) Short circuit protection or its detection

Damages to the wires by the squash, heat, hitting or acid could cause the branches or short circuit to the wiring.
Providing the safety control circuit with the short circuit protection allows these impacts to be detected. Short circuit protection can be achieved with the following conditions.
(1) The safety control circuit shall be provided with the two-channel inputs with NC contacts respectively.
(2) There shall be potential difference between channels.
A short-circuit detection circuit example is shown below.

- **Example of Short-circuit detection in the 2-channel switch inputs**



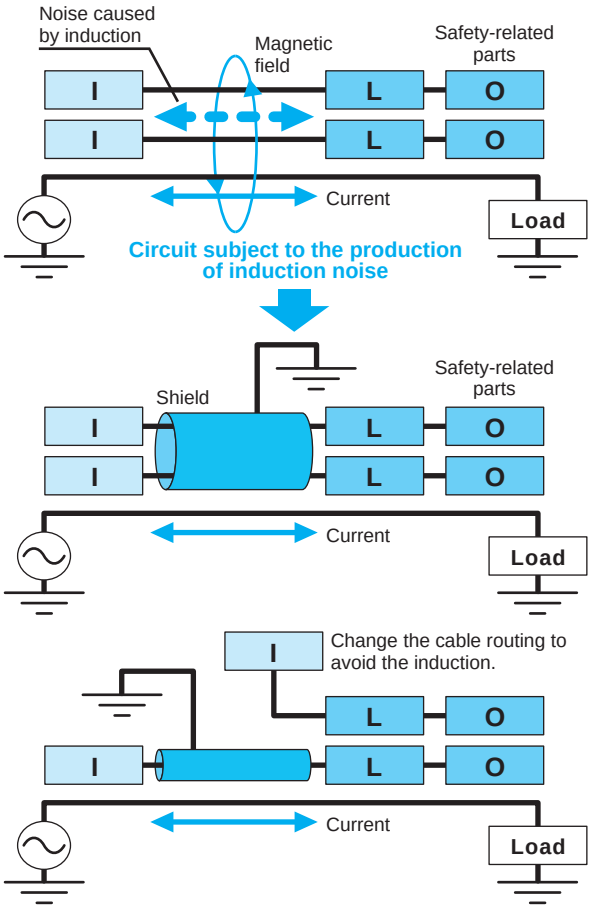


Note: Operation is not verified with the circuit example for safety standard certification.

6) Electromagnetic compatibility (EMC)

The circuitry shall have an appropriate immunity against the electromagnetic interference for proper operation in an intended environment.

- **Example for enhancing the EMC**
  - Provide an appropriate shield to the path whose impedance is likely to be high (e.g., a cable connecting an external sensor and the controller in the control panel).
  - Change the cable routing to avoid the induction. Change the two-channel cable routing to avoid the interference of the same noise source.
  - Check the electromagnetic immunity with the EMC test based on the IEC 62061 Annex E.



7) Operation in other intended environments

• Example of consideration to the heat

For installing the input devices such as switches into the designated area, the devices are designed in consideration against the parts impairment or malfunction due to the heat (high or low) or chemicals to prevent the dangerous failure on installation or usage in the environment exceeding the parts rating.

• Example of consideration to the vibration

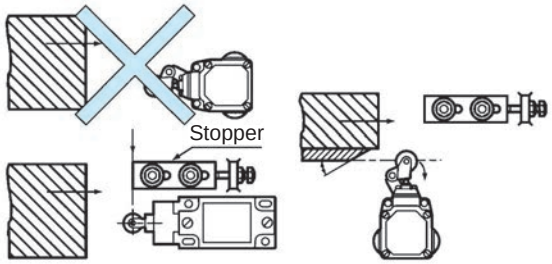
Do not install the mechanical contact parts such as relays to the vibrating location.

• Example of consideration to the mechanical stress

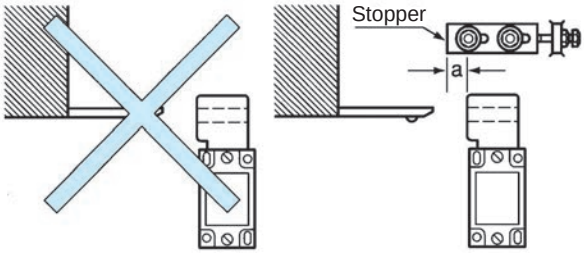
Avoid mounting the switches in a way that reduces the expected effectiveness due to the mechanical stress.
For example:

- Design and mount the limit switch dogs not to produce the overtravel.
- Provide a stopper to prevent the impact from the guard against the head of the key-in type door switch.
- Observe the design value of the key insertion radius for the key-in type door switch.

●Protection against switches



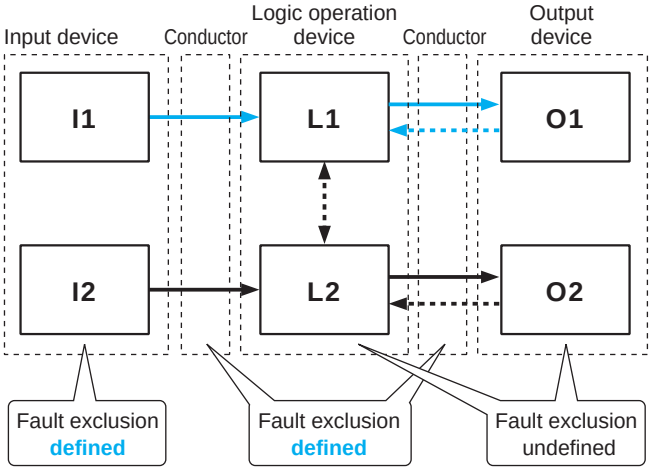
(For safety limit switches)
Mount a stopper to protect the switches from damage on operating an actuator or on overtravel.



(For safety door switches)
Do not use the switch itself as a stopper. Mount a stopper to prevent the switch body and tongues. Adjust the setting position (a) so that it is within the tongue setup zone.

Fault exclusion

In an fault exclusion state, there is no dangerous failure because in a certain condition the parts are not broken dangerously or the way of the failure is defined. Fault exclusion conditions are defined in the series standard of ISO 13849-2.



Applicability of the fault exclusion in ISO 13849-1: 2006 means that the MTTFd or DCavg in the relevant safety-related parts can be placed outside the scope of consideration.

Take a circuit composed of typical electric parts as an example. Of the designated architecture of input devices (I), logic operation devices (L), output devices (O) and the conductors as an interface, what are defined in ISO 13849-2 are the switches and the conductors alone. For example, for a switch of a direct opening action mechanism, which is in conformity with Annex K in IEC 60947-5-1, the failure mode of "Not able to open the contact" can be applied to the failure exception. Short circuits between the terminals in the IEC 60947-5-1 conformed switches can be excluded from failure. But it does not means that they are not broken dangerously in all the conditions. Failure exception cannot be applied in some use cases. For example, a failure exception is not defined for the failure in which a switch is not closed. That is, a failure exception cannot be applied if the safety function is made to work by closing the switch.
If the cables are appropriately protected and structured to be in conformity with the IEC 60204-1, the failure exception can be applied to the conductors such as cables.

The failure exception is not necessarily applied to all the safety components. And it is important to recognize in some conditions that there could be possibilities that the parts may be broken dangerously.

Failure to be considered	Fault exclusion	Remarks
Contact does not close	None	—
Contact does not open	A contact conformed with IEC 60947-5-1 Annex K is considered to be opened.	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 from the failure.
Short circuit between the adjacent, mutually isolated contacts	Short circuit of the contacts conformed with IEC 60947-5-1 can be excluded from failure.	Loosened conductor should not bridge the isolation between the contacts.
Simultaneous shorting between three terminals of the switching contacts	Simultaneous short circuit of the contacts conformed with IEC 60947-5-1 can be excluded from failure.	Loosened conductor should not bridge the isolation between the contacts.

Failure exceptions of the position switches (limit switches) and operating switches (ISO 13849-2 Annex D)

Failure to be considered	Fault exclusion	Remarks
Short circuit of lines	A cable is properly protected and the structure in conformity with IEC 60204-1	—

Cable failure exception (ISO 13849-2 Annex D)

• Switches

Mechanical impairment to the door switches or interlock switches such as limit switches cannot be ignored because of the nature of switch operation by opening/closing of the guard. If two NC contacts (conformed with IEC 60947-5-1 Annex K) having the direct opening action built in a switch are used for the redundant input for the safety-related parts, this could involve the common cause failure (CCF) such as coming off of an actuator (e.g., a key) or the damage, the fault exclusion is not applied. (See (3) DC (Diagnostic Coverage) and DCavg in 6. Subsystem Configured in Discrete Components in Chapter 5)
Fault exclusion can be applied to the emergency stop switches and enable switches. Because they are manually operable switches and the damage to the switch itself can be usually ignored.

10. Validation for Programmable Devices

Before designing the safety-related parts for the facilities or equipment using the programmable safety devices, it is needed to check the safety of not only the hardware and software.
There are two types of software: application software (SRASW) created by the device designer and the firmware (SRESW) embedded in the programmable device. This section describes the application software. (See Figure 1).

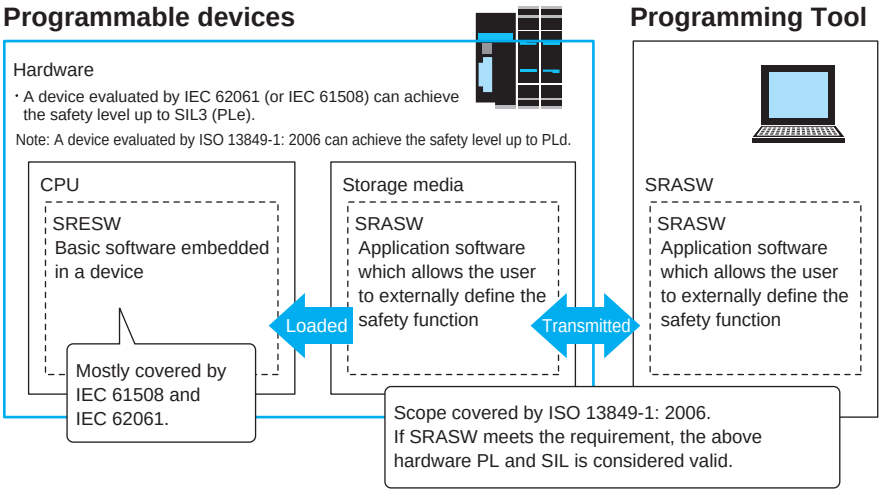


Fig. 1

Design process for the safety-related parts software

V model is referred to in ISO 13849-1 as the design process scheme for the safety-related parts software (SRASW). This is based on the quality management system ISO 9000 series concept as the background and generally used not only in the safety-related design but in the software development as well. Software design procedure assumes what is called Plan-Do-Check-Action flow in the quality control management.
Prepare the documents required at each phase of design and show the third party that the safety functions are appropriately configured by software. To configure the safety-related parts by software, it is recommended to streamline the procedure in advance of design, modification and documentation.
This section describes what is to be done in each phase based on the flow in Figure 2.

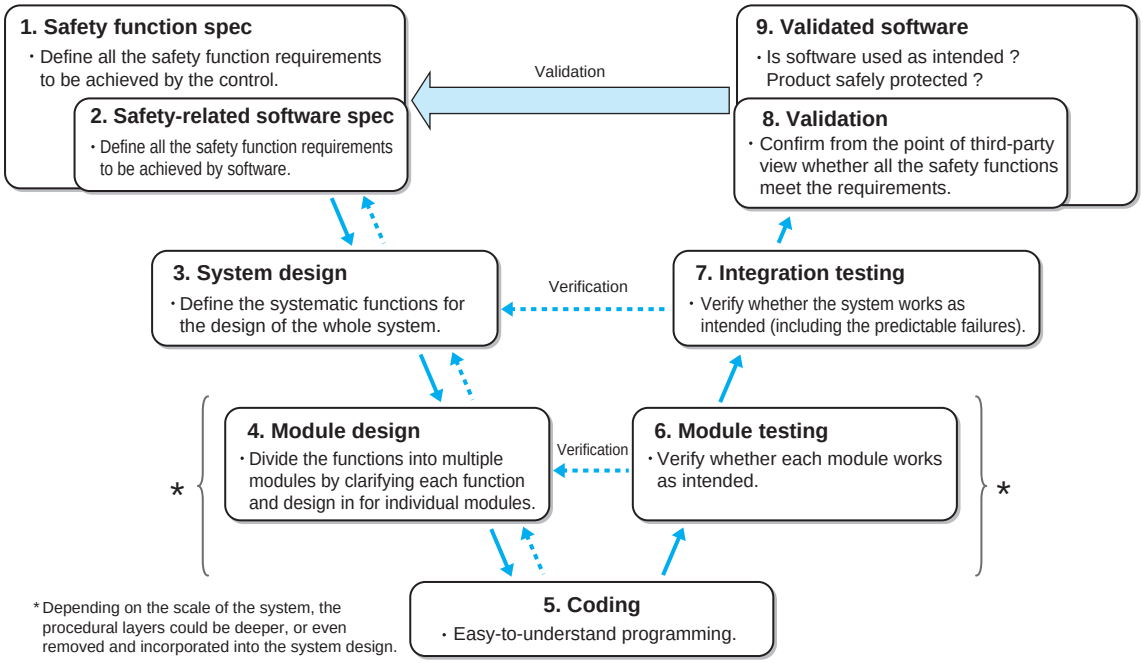
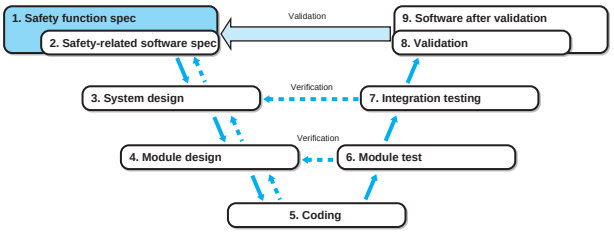


Fig. 2

1. Safety function specification

Extract all the safety functions (described in ISO 13849-1) achievable with the control from the risk assessment sheet and define the operations, performance level (PLr), frequency of operations (nop) as the requirements in the safety function specifications.
Create a list of the parts comprising the control circuits and safety functions based on the safety function specifications. Parts specifications and mechanical safety reliability data for the dangerous failure are obtained from the device manufacturers. Analyze the control circuits (such as FMEA) and define the predictable failure or abuses of the parts.

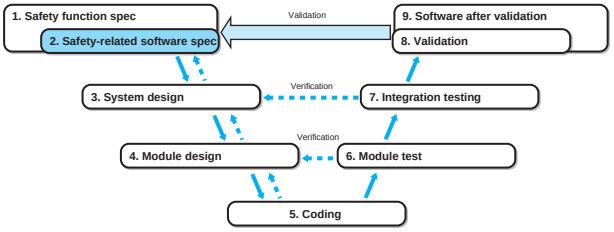
<Documents example>
• Safety function specification
• Control circuits
• Operation list
• Parts list
• Parts specifications
• Mechanical safety reliability data for the dangerous failure, etc.



2. Safety-related software specification

Of the safety functions, define the requirements achieved by software.
From the operation list created based on the "1. Safety function specifications," extract the safety functions alone which are 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 for determination of the interface specifications.
Determine the safety function logic and operation specifications from the operation list.

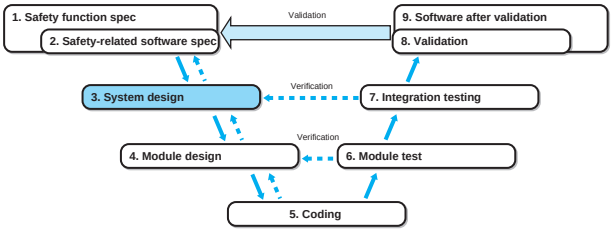
<Documents example>
• Interface specifications
• Operating specifications, etc.



3. System design

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

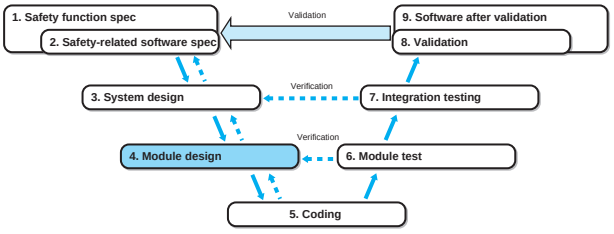
<Documents example>
• System test procedure, etc.



4. Module design

Depending on the scale of the system, multiple hardware modules, that is, combination of multiple programmable safety controllers, are used to achieve the safety function. In that case, each software is also divided into functional blocks for design. The functional blocks includes the blocks of function which are created specifically by a designer.
For ease of verification in the later phase of the module tests, create the test procedure for each module.

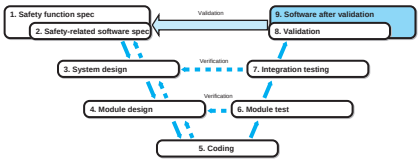
<Documents example>
• Test procedure for each module, etc.



9. Validated software

On completing the software validation, incorporate with the safety-related parts hardware in the control circuit for validation. With the software embedded in the device incorporated with the parts in mechanism, confirmation is proceeded with that of the risk reduction. Validated program is handled as part of the hardware and is used for simplified management of the following items. If a program is required to be modified in a lifecycle of the device, security is provided so that authorized personnel only can change the program.

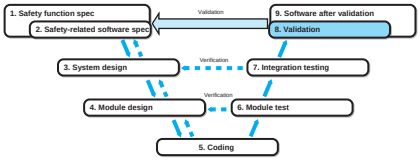
<Example of items for management>
- Device type or revision
- User (customer) of a device
- Control circuit design version
- Target module
- Device format and revision where a program is transferred
- Version of a program itself, etc.



8. Validation

Confirm whether the program is designed according to the safety function specifications, based on the variation of the output, including the response performance, in compliance with the external specifications, with the input conditions created by implementing the program into the safety-related parts. Since this scheme of validation is focused on the external specifications, you do not need to have the insight into the detailed structure of the software.
Record the result into the validation test confirmation. If any trouble is found, this could be derived from the software specification itself, regress to the safety-related software specification process for correction (see "Validation" in the Figure).

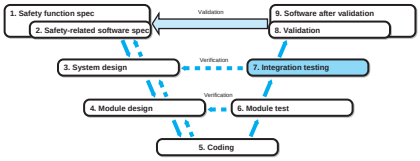
<Documents example>
- Validation record, etc.



7. Integration testing

Verify whether the total software operation is as intended including the incorporated modules based on the system test procedure. Execute all the operations of the program once on the development tool simulator, in some cases with the program loaded in the safety-related parts, to verify the response performance from the input given until output as a reaction or the operation of the predictable parts failure or abuse as defined in the safety function specification. Record the result into the integration testing result document. If any trouble is found, this could be derived from the design, regress to the system design process for correction (see "Verification" in the Figure). Reverify whether there is another trouble due to the modification work.

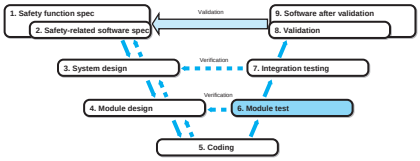
<Documents example>
- Integration testing result documents, etc.



6. Module testing

Verify whether a module works as intended based on the test procedure per module. Verify either on the development tool simulator or in some case on the actual device by feeding the simulated input.
Record the result into the module test result document. If any trouble is found, this could be derived from the design, regress to the module design process for correction. (See "Verification" in the Figure) Reverify whether there is another trouble due to the modification work.

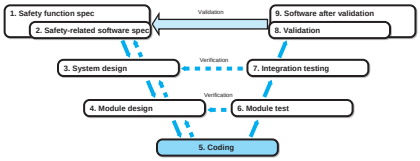
<Documents example>
Module test result document
Software correction procedure, etc.



5. Coding

Embody the system worked out by the module design via the program. Create the program by adding the comment statement understandable by the third party.
If any bugs are found in the later phase of the module test or integration testing, a couple of regressions could be encountered in coding for correction. Program version management will tell you what type of bugs are corrected and reflected to the later phase of processing.

<Documents example>
Program version management, etc.



11. Safety-related Parts PL Evaluation in the Devices

(1) Sorting out safety functions

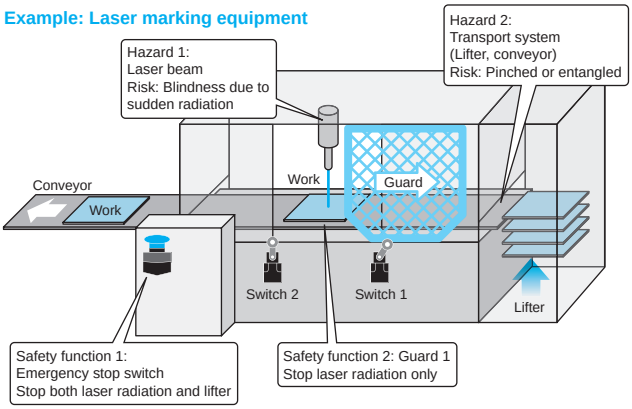
This section explains how to sort out the hazards or safety functions in a system.

Note: The description is for the sake of explanatory example. Different calculation is necessary to suit to the device of the actual circuit.

It is often the cases that a safety function is not alone in the actual device control system. There are some cases when more than one safety functions are provided against the risks derived from hazards in a machine. There are still other cases where different safety functions are provided against each risk for multiple hazards in a machine. Also in such a case, PL is evaluated for each safety function.

But this does not mean that not all safety functions have their own independent control circuits; they often share the same control circuit.

Example: Laser marking equipment

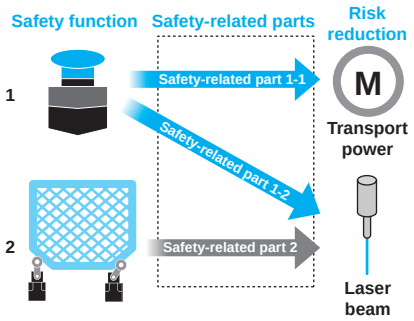


Above devices are assumed as an example.

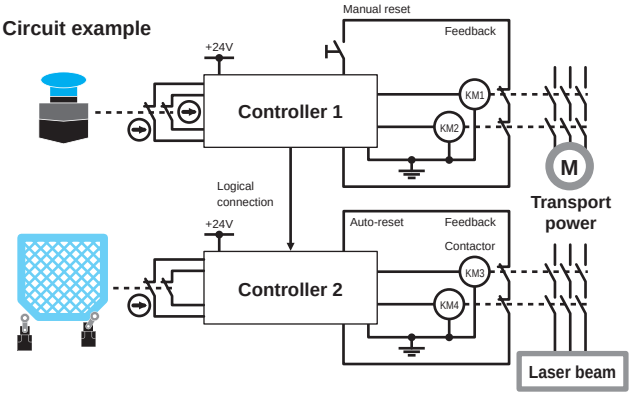
This equipment has two hazards. One is the laser beam, which would cause, if the beam is penetrated into an eye, the worst case of loss of eyesight, equivalent to PLr = d; and the other is the transport system (lifter and conveyor) which would cause a relatively light hazard such as bruises or scraping, equivalent to PLr = b.

Against the laser beam, movable guard is set up and interlock system is provided. If a work is stuck in an equipment, an operator manually handles, but if the transport system is stopped, there could be an inconvenience to work, so the laser beam radiation only is stopped. In an emergency, press the emergency stop switch to shut down both the laser beam and transport power.

Relationship between the safety function and the risk reduction action in simplified form is as shown below; this equipment has three lines of safety functions and each is required to evaluate PL.



Circuit example



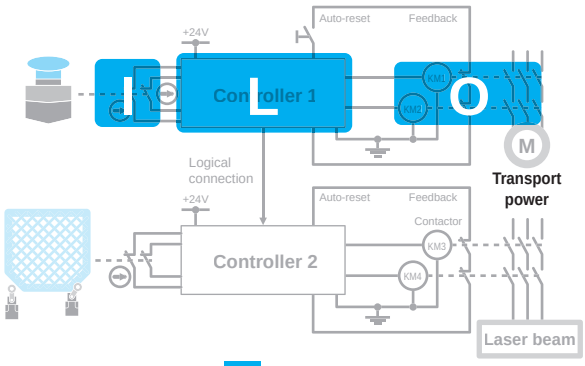
These safety functions are achieved with the circuit in the above. Transport power is shut down by the logical operation device of controller 1 while the laser beam is shut down by the controller 2.

Controller 1 and Controller 2 are logically connected by the redundantly configured interface and the logical input of Controller 2 is ANDed together with the physical input system (safety function 1 and safety function 2). Demand for operation for emergency stop switch leads to the shut down of both of the transport power and the laser beam, and demand for operation for guard 1 leads to the shut down of the laser beam alone.

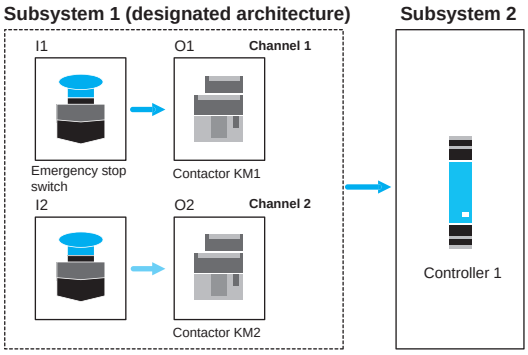
Controller 1 and Controller 2 are assumed to be individually evaluated in terms of PFHd.

(2) Drawing up block diagram

Safety-related part 1-1

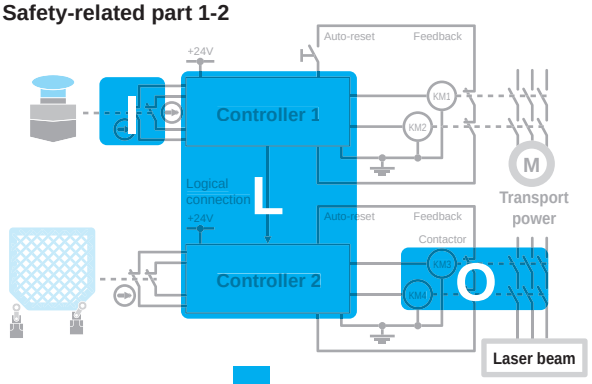


Block diagram

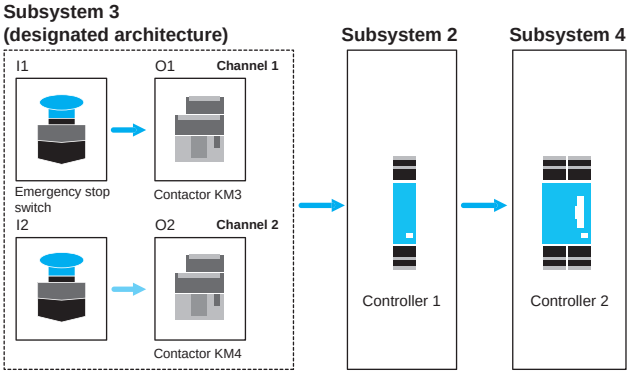


Safety related part 1-1 is comprised of the emergency stop switch NC contacts 1 and 2, the designated architecture (subsystem 1) of contactors KM 1 and KM 2 and controller 1 (subsystem 2) where PL and PFHd are individually evaluated.
PFHd for subsystem 1 is evaluated using the parameters (category, MTTFd, DCavg and CCF).

Safety-related part 1-2



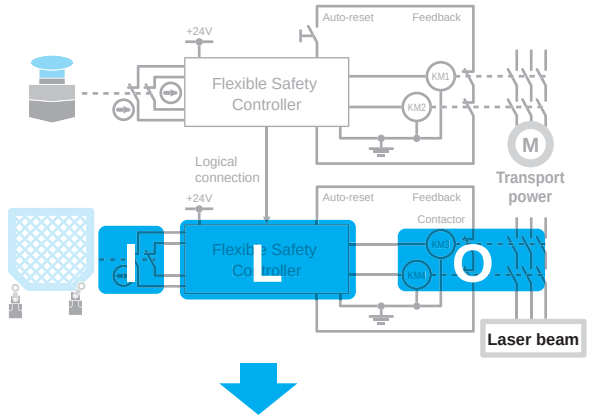
Block diagram



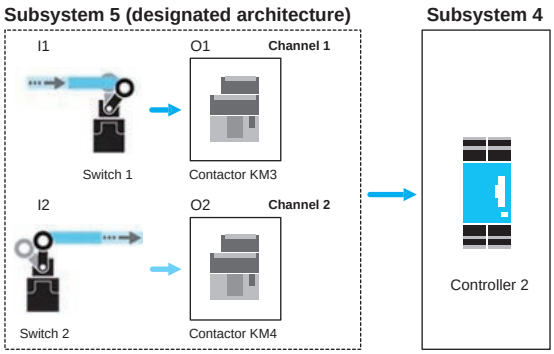
Safety related part 1-2 is comprised of the emergency stop switch NC contacts 1 and 2, the designated architecture (subsystem 3) of contactors KM 3 and KM 4 and controller 1 (subsystem 2) and controller 2 (subsystem 4) where PL and PFHd are individually evaluated.
PFHd for subsystem 3 is evaluated using the parameters (category, MTTFd, DCavg and CCF).

Note: Since contactors KM 3 and KM 4 are shared components with the safety-related parts 2, MTTFd is calculated by the summation of nop in each safety function.
If, however, the operation demand to one block is extremely low and the impact to the other block is almost nil, this can be considered a margin of error and this calculation is not applied. (Example: A guard is often operated daily while the emergency stop is so few as once a year)

Safety-related part 2



Block diagram

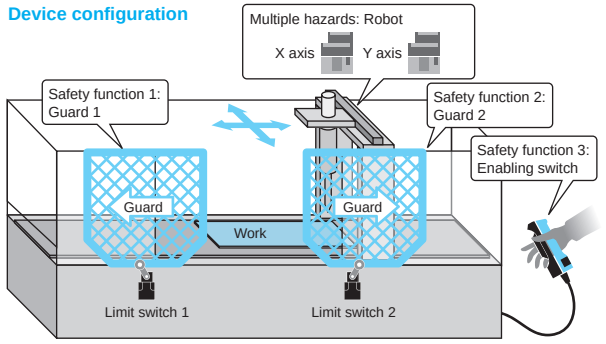


Safety related parts 2 is comprised of the designated architecture (subsystem 5) of contactors KM 3 and KM 4 and the controller 2 (subsystem 4) where PL and PFHd are individually evaluated. PFHd for subsystem 5 is evaluated using the parameters (category, MTTFd, DCavg and CCF).

Note: Note: Since contactors KM 3 and KM 4 are shared components with the safety-related parts 1-2, MTTFd is calculated by the summation of nop in each safety function.
If, however, the operation demand to one block is extremely low and the impact to the other block is almost nil, this can be considered a margin of error and this calculation is not applied.
(Example: A guard is often operated daily while the emergency stop is so few as once a year)

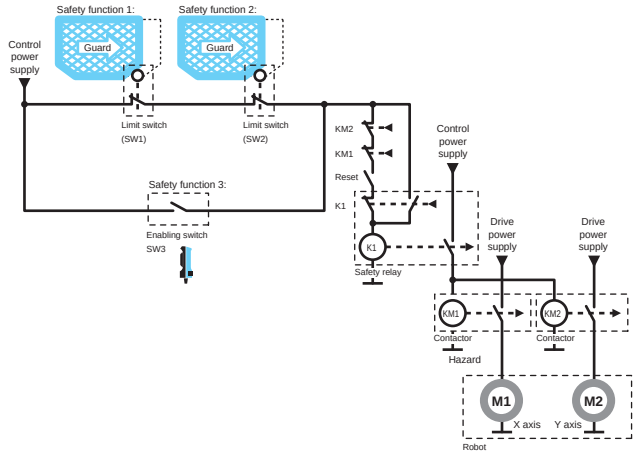
(3) Points in compositive hazard schematisation

Device configuration



Block diagram is a logical conceptual diagram to represent the sum of the dangerous failure rates. This does not necessarily correspond to the electrical control circuit diagram.
Consider the machine as in the diagram above for example. The hazard for this machine is a robot operating along the X and Y axes. Contradiction with this movement is assumed to be the hazardous event, against which a safety measure is to be set up based on the risk assessment. The risk reduction shall be assumed to be achieved without stopping both X and Y axes simultaneously. Use a measure, for example, for configuring an interlock circuit with two limit switches, with movable guards installed opening right and left. Each guard is assigned as safety functions 1 and 2. If one guard is opened, a hazard is shut down by activating the interlock. There are some cases, however, where a robot is required to operate with the guards open for the maintenance or adjustment purposes of a machine. The enabling switch is used as alternative of the guard and this works as the safety function 3.
And the request PL for these safety functions is assumed to be equivalent to PLr = c.

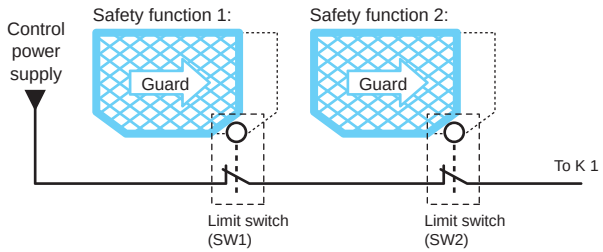
Example of the electric circuit diagram in the safety-related parts

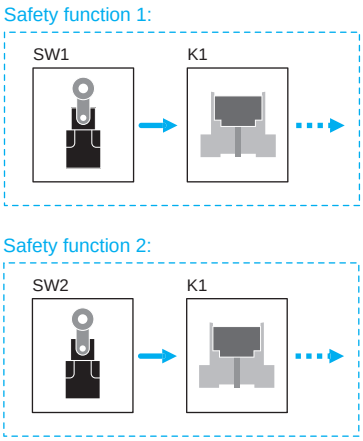


Suppose the safety-related parts for achieving the safety functions 1, 2 and 3 are configured in a single system as the diagram above. Assume that the designated architecture category 1 is selected for meeting PLr = c or its equivalent.

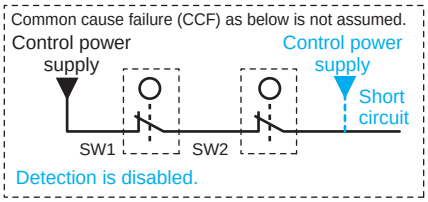
Note: Note: This circuit diagram is intended for the simplified explanation only for the block diagram expansion and not a recommended circuit for this application. (For example, on enabling, other safety functions are required including the mode switching by key switches and accompanied restriction of the power engine, but these are skipped in this description)If further information is needed, see the relevant standards.

Series connection of input devices

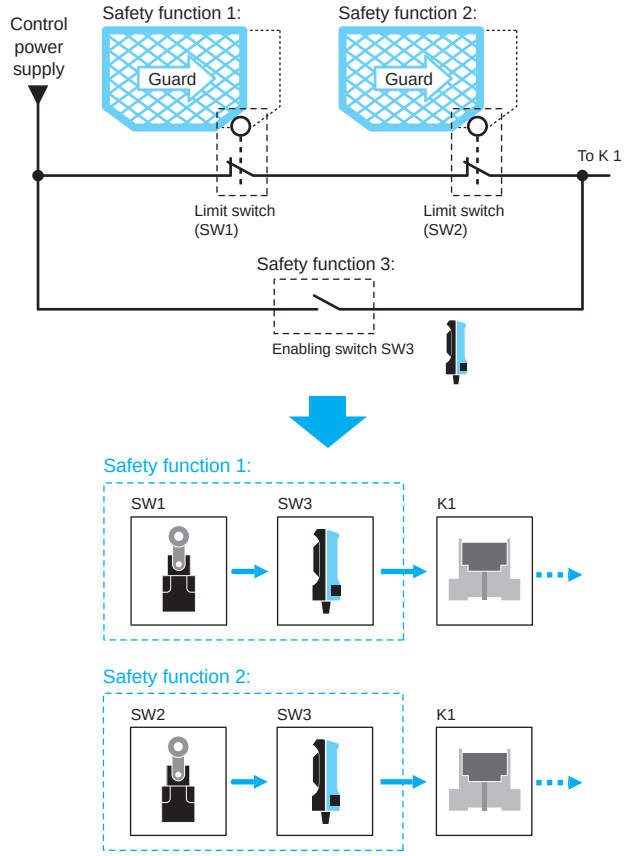




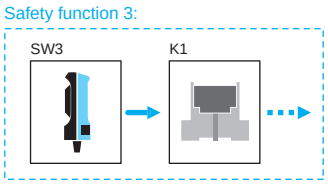
Two limit switches (SW1 and SW2) for guard 1 and guard 2 in the input section of this circuit are electrically connected in series. The safety function 1 and safety function 2, however, are not affected by each other. When the safety function 1 demands operation (that is, when guard 1 is opened), interlock works regardless of the state of the guard 2 to shut off the hazard. Even if SW2 is in a state of dangerous failure due to the contact welding, the safety function 1 is not affected by this. The opposite is also true.
That is, the two safety functions are independent of each other. PL is used to evaluate each safety function, so the block diagram is divided into two for each PL evaluation.
It is assumed, however, there is no such a case where both safety functions are damaged at the same time due to the short circuit of the conductors.



Input devices in parallel connection

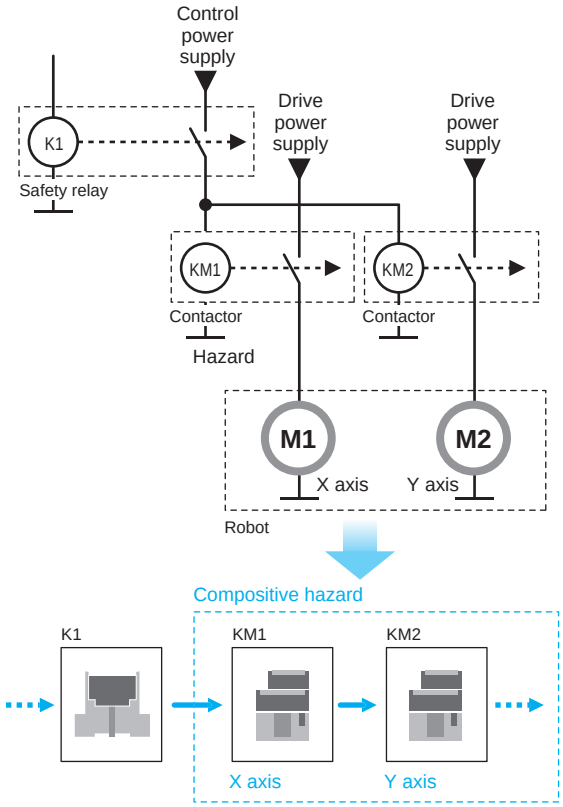


In parallel with the limit switches (SW1 and SW2) for guard 1 and guard 2, the enabling switch is connected with the hardware wire. It could be possible that the enabling switch dangerous failure may affect safety functions 1 and 2. For examle, even if the detection of the open state of the guard is assumed to cause the driving engine of the hazard to shut down, the dangerous failure of the output contact welding in the enabling switch would fail to detect the open state of the guard, resulting in the impairment of the guard safety function.
If the dangerous failure in a part may impact the safety function of other parts, those dangerous failure rates are summed together, represented in a block diagram as a series connection.



From a reverse point of view on the other hand, the enabling switch in safety function 3 is not subject to hazardous state as far as the simultaneous dangerous failure is not encountered such as the simultaneous welding of the limit switches (SW1 and SW2) in guards 1 and 2. With the due considerations given to the common cause failure, the probability of such a failure could be assumed to be infinitely small. Therefore, an input device attributable to the cause of the dangerous failure in safety function 3 is considered to be the enabling switch (SW3) only and the resulting block diagram is as shown in the above.

Output devices in parallel connection



In the output of the circuit of interest, two contactors (KM1 and KM2) are connected in parallel for controlling the X and Y axes of the robot. It is premised here that only one axis cannot reduce the risk. If, for example, the robot X-axis movement is controlled into stop, the Y-axis movement could cause an accident, resulting in the impairment of safety function. If a real reduction of the risk can only be achieved by the simultaneous stop of the X and Y axes, the dangerous failure rates for two contactors are required to be summed together, resulting in the series connection in the block diagram.

Note: If, however, risk assessment reveals that X and Y axes are separate hazards and the consideration of the composite risks is not needed and each PLr is different, the block diagram can also be separated.

PL Decision Table/PFHd Conversion Table (Source: ISO 13849-1, Annex K, Table K.1)

Category		B	1	2		3		4
DCavg		None		Low 60≤DC	Medium g	Low 60≤DCavg	Medium 90≤DCavg	High 99≤DCavg
CCF		Not relevant		65 ≤ C	F	65 ≤ CCF		
Low	3≤MTTFd	a 3.80×10^{-5}		a		a 1.26×10^{-5}	b	
	3.3≤MTTFd	a 3.46×10^{-5}		a		a 1.13×10^{-5}	b 5.41×10^{-6}	
	3.6≤MTTFd	a 3.17×10^{-5}		a		a 1.03×10^{-5}	b 4.86×10^{-6}	
	3.9≤MTTFd	a 2.93×10^{-5}		a 1.95×10^{-5}	a 1.48×10^{-5}	b 9.37×10^{-6}	b 4.40×10^{-6}	
	4.3≤MTTFd	a 2.65×10^{-5}		a 1.76×10^{-5}	a 1.33×10^{-5}	b 8.39×10^{-6}	b 3.89×10^{-6}	
	4.7≤MTTFd	a 2.43×10^{-5}		a 1.60×10^{-5}	a 1.20×10^{-5}	b 7.58×10^{-6}	b 3.48×10^{-6}	
	5.1≤MTTFd	a 2.24×10^{-5}		a 1.47×10^{-5}	a 1.10×10^{-5}	b 6.91×10^{-6}	b 3.15×10^{-6}	
	5.6≤MTTFd	a 2.04×10^{-5}		a 1.33×10^{-5}	b 9.87×10^{-6}	b 6.21×10^{-6}	c 2.80×10^{-6}	
	6.2≤MTTFd	a 1.84×10^{-5}		a 1.19×10^{-5}	b 8.80×10^{-6}	b 5.53×10^{-6}	c 2.47×10^{-6}	
	6.8≤MTTFd	a 1.68×10^{-5}		a 1.08×10^{-5}	b 7.93×10^{-6}	b 4.98×10^{-6}	c 2.20×10^{-6}	
	7.5≤MTTFd	a 1.52×10^{-5}		b 9.75×10^{-6}	b 7.10×10^{-6}	b 4.45×10^{-6}	c 1.95×10^{-6}	
	8.2≤MTTFd	a 1.39×10^{-5}		b 8.87×10^{-6}	b 6.43×10^{-6}	b 4.02×10^{-6}	c 1.74×10^{-6}	
	9.1≤MTTFd	a 1.25×10^{-5}		b 7.94×10^{-6}	b 5.71×10^{-6}	b 3.57×10^{-6}	c 1.53×10^{-6}	
Medium	10≤MTTFd	a 1.14×10^{-5}		b 7.18×10^{-6}	b 5.14×10^{-6}	b 3.21×10^{-6}	c 1.36×10^{-6}	
	11≤MTTFd	a 1.04×10^{-5}		b 6.44×10^{-6}	b 4.53×10^{-6}	c 2.81×10^{-6}	c 1.18×10^{-6}	
	12≤MTTFd	b 9.51×10^{-6}		b 5.84×10^{-6}	b 4.04×10^{-6}	c 2.49×10^{-6}	c 1.04×10^{-6}	
	13≤MTTFd	b 8.78×10^{-6}		b 5.33×10^{-6}	b 3.64×10^{-6}	c 2.23×10^{-6}	d 9.21×10^{-7}	
	15≤MTTFd	b 7.61×10^{-6}		b 4.53×10^{-6}	b 3.01×10^{-6}	c 1.82×10^{-6}	d 7.44×10^{-7}	
	16≤MTTFd	b 7.13×10^{-6}		b 4.21×10^{-6}	c 2.77×10^{-6}	c 1.67×10^{-6}	d 6.76×10^{-7}	
	18≤MTTFd	b 6.34×10^{-6}		b 3.68×10^{-6}	c 2.37×10^{-6}	c 1.41×10^{-6}	d 5.67×10^{-7}	
	20≤MTTFd	b 5.71×10^{-6}		b 3.26×10^{-6}	c 2.06×10^{-6}	c 1.22×10^{-6}	d 4.85×10^{-7}	
	22≤MTTFd	b 5.19×10^{-6}		c 2.93×10^{-6}	c 1.82×10^{-6}	c 1.07×10^{-6}	d 4.21×10^{-7}	
	24≤MTTFd	b 4.76×10^{-6}		c 2.65×10^{-6}	c 1.62×10^{-6}	d 9.47×10^{-7}	d 3.70×10^{-7}	
	27≤MTTFd	b 4.23×10^{-6}		c 2.32×10^{-6}	c 1.39×10^{-6}	d 8.04×10^{-7}	d 3.10×10^{-7}	
High	30≤MTTFd		b 3.80×10^{-6}	c 2.06×10^{-6}	c 1.21×10^{-6}	d 6.94×10^{-7}	d 2.65×10^{-7}	e 9.54×10^{-8}
	33≤MTTFd		b 3.46×10^{-6}	c 1.85×10^{-6}	c 1.06×10^{-6}	d 5.94×10^{-7}	d 2.30×10^{-7}	e 8.57×10^{-8}
	36≤MTTFd		b 3.17×10^{-6}	c 1.67×10^{-6}	d 9.39×10^{-7}	d 5.16×10^{-7}	d 2.01×10^{-7}	e 7.77×10^{-8}
	39≤MTTFd		c 2.93×10^{-6}	c 1.53×10^{-6}	d 8.40×10^{-7}	d 4.53×10^{-7}	d 1.78×10^{-7}	e 7.11×10^{-8}
	43≤MTTFd		c 2.65×10^{-6}	c 1.37×10^{-6}	d 7.34×10^{-7}	d 3.87×10^{-7}	d 1.54×10^{-7}	e 6.37×10^{-8}
	47≤MTTFd		c 2.43×10^{-6}	c 1.24×10^{-6}	d 6.49×10^{-7}	d 3.35×10^{-7}		
	51≤MTTFd				d 5.80×10^{-7}	d 2.93×10^{-7}		
	56≤MTTFd				d 5.10×10^{-7}	d 2.52×10^{-7}		
	62≤MTTFd		c 1.84×10^{-6}	d 9.06×10^{-7}	d 4.43×10^{-7}	d 2.13×10^{-7}		
	68≤MTTFd		c 1.68×10^{-6}	d 8.17×10^{-7}	d 3.90×10^{-7}	d 1.84×10^{-7}		
	75≤MTTFd		c 1.52×10^{-6}	d 7.31×10^{-7}	d 3.40×10^{-7}	d 1.57×10^{-7}		
	82≤MTTFd		c 1.39×10^{-6}	d 6.61×10^{-7}	d 3.01×10^{-7}	d 1.35×10^{-7}	e 5.79×10^{-8}	e 3.08×10^{-8}
	91≤MTTFd		c 1.25×10^{-6}	d 5.88×10^{-7}	d 2.61×10^{-7}	d 1.14×10^{-7}	e 4.94×10^{-8}	e 2.74×10^{-8}
	100≤MTTFd		c 1.14×10^{-6}	d 5.28×10^{-7}	d 2.29×10^{-7}	d 1.01×10^{-7}	e 4.29×10^{-8}	e 2.47×10^{-8}

Cat3 domain selected

Confirm the range 65 ≤ CCF

Focused to domain equivalent to 60 ≤ DCavg < 90

Domain equivalent to 39 ≤ MTTFd < 43 selected

Crossed portion represents PL and PFHd for this channel

PL Decision Table (Source: ISO 13849-1, Annex K, Table K.1)

Category		B	1	2		3		4
DCavg		None		Low 60≤DCavg	Medium 90≤DCavg	Low 60≤DCavg	Medium 90≤DCavg	High 99≤DCavg
CCF		Not relevant		65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF
Low	3≤MTTFd	a		a	a	a	b	
	3.3≤MTTFd	a		a	a	a	b	
	3.6≤MTTFd	a		a	a	a	b	
	3.9≤MTTFd	a		a	a	b	b	
	4.3≤MTTFd	a		a	a	b	b	
	4.7≤MTTFd	a		a	a	b	b	
	5.1≤MTTFd	a		a	a	b	b	
	5.6≤MTTFd	a		a	b	b	c	
	6.2≤MTTFd	a		a	b	b	c	
	6.8≤MTTFd	a		a	b	b	c	
	7.5≤MTTFd	a		b	b	b	c	
	8.2≤MTTFd	a		b	b	b	c	
	9.1≤MTTFd	a		b	b	b	c	
Medium	10≤MTTFd	a		b	b	b	c	
	11≤MTTFd	a		b	b	c	c	
	12≤MTTFd	b		b	b	c	c	
	13≤MTTFd	b		b	b	c	d	
	15≤MTTFd	b		b	b	c	d	
	16≤MTTFd	b		b	c	c	d	
	18≤MTTFd	b		b	c	c	d	
	20≤MTTFd	b		b	c	c	d	
	22≤MTTFd	b		c	c	c	d	
	24≤MTTFd	b		c	c	d	d	
	27≤MTTFd	b		c	c	d	d	
High	30≤MTTFd		b	c	c	d	d	e
	33≤MTTFd		b	c	c	d	d	e
	36≤MTTFd		b	c	d	d	d	e
	39≤MTTFd		c	c	d	d	d	e
	43≤MTTFd		c	c	d	d	d	e
	47≤MTTFd		c	c	d	d	d	e
	51≤MTTFd		c	c	d	d	d	e
	56≤MTTFd		c	c	d	d	d	e
	62≤MTTFd		c	d	d	d	e	e
	68≤MTTFd		c	d	d	d	e	e
	75≤MTTFd		c	d	d	d	e	e
	82≤MTTFd		c	d	d	d	e	e
	91≤MTTFd		c	d	d	d	e	e
	100≤MTTFd		c	d	d	d	e	e

Category		B	1	2		3		4
DCavg		None		Low 60≤DCavg	Medium 90≤DCavg	Low 60≤DCavg	Medium 90≤DCavg	High 99≤DCavg
CCF		Not relevant		65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF	65 ≤ CCF
Low	3≤MTTFd	3.80×10^{-5}		2.58×10^{-5}	1.99×10^{-5}	1.26×10^{-5}	6.09×10^{-6}	
	3.3≤MTTFd	3.46×10^{-5}		2.33×10^{-5}	1.79×10^{-5}	1.13×10^{-5}	5.41×10^{-6}	
	3.6≤MTTFd	3.17×10^{-5}		2.13×10^{-5}	1.62×10^{-5}	1.03×10^{-5}	4.86×10^{-6}	
	3.9≤MTTFd	2.93×10^{-5}		1.95×10^{-5}	1.48×10^{-5}	9.37×10^{-6}	4.40×10^{-6}	
	4.3≤MTTFd	2.65×10^{-5}		1.76×10^{-5}	1.33×10^{-5}	8.39×10^{-6}	3.89×10^{-6}	
	4.7≤MTTFd	2.43×10^{-5}		1.60×10^{-5}	1.20×10^{-5}	7.58×10^{-6}	3.48×10^{-6}	
	5.1≤MTTFd	2.24×10^{-5}		1.47×10^{-5}	1.10×10^{-5}	6.91×10^{-6}	3.15×10^{-6}	
	5.6≤MTTFd	2.04×10^{-5}		1.33×10^{-5}	9.87×10^{-6}	6.21×10^{-6}	2.80×10^{-6}	
	6.2≤MTTFd	1.84×10^{-5}		1.19×10^{-5}	8.80×10^{-6}	5.53×10^{-6}	2.47×10^{-6}	
	6.8≤MTTFd	1.68×10^{-5}		1.08×10^{-5}	7.93×10^{-6}	4.98×10^{-6}	2.20×10^{-6}	
	7.5≤MTTFd	1.52×10^{-5}		9.75×10^{-6}	7.10×10^{-6}	4.45×10^{-6}	1.95×10^{-6}	
	8.2≤MTTFd	1.39×10^{-5}		8.87×10^{-6}	6.43×10^{-6}	4.02×10^{-6}	1.74×10^{-6}	
	9.1≤MTTFd	1.25×10^{-5}		7.94×10^{-6}	5.71×10^{-6}	3.57×10^{-6}	1.53×10^{-6}	
Medium	10≤MTTFd	1.14×10^{-5}		7.18×10^{-6}	5.14×10^{-6}	3.21×10^{-6}	1.36×10^{-6}	
	11≤MTTFd	1.04×10^{-5}		6.44×10^{-6}	4.53×10^{-6}	2.81×10^{-6}	1.18×10^{-6}	
	12≤MTTFd	9.51×10^{-6}		5.84×10^{-6}	4.04×10^{-6}	2.49×10^{-6}	1.04×10^{-6}	
	13≤MTTFd	8.78×10^{-6}		5.33×10^{-6}	3.64×10^{-6}	2.23×10^{-6}	9.21×10^{-7}	
	15≤MTTFd	7.61×10^{-6}		4.53×10^{-6}	3.01×10^{-6}	1.82×10^{-6}	7.44×10^{-7}	
	16≤MTTFd	7.13×10^{-6}		4.21×10^{-6}	2.77×10^{-6}	1.67×10^{-6}	6.76×10^{-7}	
	18≤MTTFd	6.34×10^{-6}		3.68×10^{-6}	2.37×10^{-6}	1.41×10^{-6}	5.67×10^{-7}	
	20≤MTTFd	5.71×10^{-6}		3.26×10^{-6}	2.06×10^{-6}	1.22×10^{-6}	4.85×10^{-7}	
	22≤MTTFd	5.19×10^{-6}		2.93×10^{-6}	1.82×10^{-6}	1.07×10^{-6}	4.21×10^{-7}	
	24≤MTTFd	4.76×10^{-6}		2.65×10^{-6}	1.62×10^{-6}	9.47×10^{-7}	3.70×10^{-7}	
	27≤MTTFd	4.23×10^{-6}		2.32×10^{-6}	1.39×10^{-6}	8.04×10^{-7}	3.10×10^{-7}	
High	30≤MTTFd		3.80×10^{-6}	2.06×10^{-6}	1.21×10^{-6}	6.94×10^{-7}	2.65×10^{-7}	9.54×10^{-8}
	33≤MTTFd		3.46×10^{-6}	1.85×10^{-6}	1.06×10^{-6}	5.94×10^{-7}	2.30×10^{-7}	8.57×10^{-8}
	36≤MTTFd		3.17×10^{-6}	1.67×10^{-6}	9.39×10^{-7}	5.16×10^{-7}	2.01×10^{-7}	7.77×10^{-8}
	39≤MTTFd		2.93×10^{-6}	1.53×10^{-6}	8.40×10^{-7}	4.53×10^{-7}	1.78×10^{-7}	7.11×10^{-8}
	43≤MTTFd		2.65×10^{-6}	1.37×10^{-6}	7.34×10^{-7}	3.87×10^{-7}	1.54×10^{-7}	6.37×10^{-8}
	47≤MTTFd		2.43×10^{-6}	1.24×10^{-6}	6.49×10^{-7}	3.35×10^{-7}	1.34×10^{-7}	5.76×10^{-8}
	51≤MTTFd		2.24×10^{-6}	1.13×10^{-6}	5.80×10^{-7}	2.93×10^{-7}	1.19×10^{-7}	5.26×10^{-8}
	56≤MTTFd		2.04×10^{-6}	1.02×10^{-6}	5.10×10^{-7}	2.52×10^{-7}	1.03×10^{-7}	4.73×10^{-8}
	62≤MTTFd		1.84×10^{-6}	9.06×10^{-7}	4.43×10^{-7}	2.13×10^{-7}	8.84×10^{-8}	4.22×10^{-8}
	68≤MTTFd		1.68×10^{-6}	8.17×10^{-7}	3.90×10^{-7}	1.84×10^{-7}	7.68×10^{-8}	3.80×10^{-8}
	75≤MTTFd		1.52×10^{-6}	7.31×10^{-7}	3.40×10^{-7}	1.57×10^{-7}	6.62×10^{-8}	3.41×10^{-8}
	82≤MTTFd		1.39×10^{-6}	6.61×10^{-7}	3.01×10^{-7}	1.35×10^{-7}	5.79×10^{-8}	3.08×10^{-8}
	91≤MTTFd		1.25×10^{-6}	5.88×10^{-7}	2.61×10^{-7}	1.14×10^{-7}	4.94×10^{-8}	2.74×10^{-8}
	100≤MTTFd		1.14×10^{-6}	5.28×10^{-7}	2.29×10^{-7}	1.01×10^{-7}	4.29×10^{-8}	2.47×10^{-8}

MEMO

Chapter 6

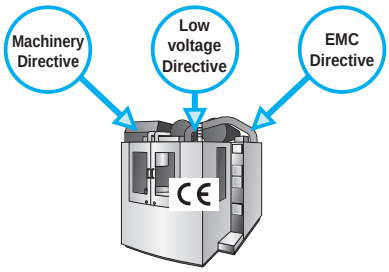
Annex

1. Regulations and Standards by Country

(1) Europe

• EC Directives and CE Marking

There are approximately 300 EC Directives issued for harmony in Europe. The EC Directives are equivalent to law in 27 countries in Europe. Twenty one Directives according to the New Approach Directives and several Directives require the CE Marking to indicate that products conformed with these Directives. The CE Marking attached to products indicates that the products conformed with the stipulated level of protection in all relevant EC Directives. Devices labeled with the CE Marking may be imported and exported to Europe without restriction. You might call the CE Marking a “passport” to Europe. Therefore you must identify the corresponding Directive before attaching the CE Marking to products. For industrial machineries, corresponding Directive is usually Low voltage Directive, EMC Directive, or Machinery Directive.



• Low-voltage Directive (LVD)

According to the EC Directive (EC Directive 2006/95/EC), low voltage devices are devices 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

The EMC Directive (2004/108/EC) has been in force since July 20, 2007, and the old version EMC Directive (89/336/EEC) was revoked. 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 Annex I of Machinery Directive are introduced below.

(1) 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. In any event, requirements 1.1.2, 1.7.3 and 1.7.4 apply to all machinery covered by this directive.

(2) 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.

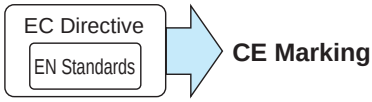
(3) The essential health and safety requirements have been grouped according to the hazards which they cover.

Machinery presents a series of hazards which maybe indicated under more than one heading in this Annex.
The manufacturer is under an obligation to assess the hazards in order to identify all of those which apply to his machine; he must then design and construct it taking account of this assessment.

• EN Directive 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 normally within six months. 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. Also recently the IEC ISO 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 EC Directives. Applicable standards for products intended are not indicated in the individual EC Directives. The list of EN Standards that can apply for each directive are published separately in the Official Journal of the European Communities (OJEC). The EN standards listed in this Official Journal are called "Harmonized standard." Manufacturers are therefore necessary to determine the design specifications based on the EN Standards published in the OJEC.

• Relation between the EC Directives, EN Standards, and CE Marking



As explained above, all relevant EC Directives must be satisfied for a product to be labeled with the CE Marking. EN Standards complement the EC Directives. Satisfying the EN Standards alone, however, does not result in the EC Directives being satisfied. Countermeasures for product liability is mainly required in instructions and catalogs.

• Product Liability

The General Product Safety Directive and Product Liability Directive are complementary regulations but their scope is not identical.
The Product Liability Directive applies to virtually all products, while the General Product Safety Directive 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 Standards Related to Machinery Safety

Type A Standards (Basic Safety Standards)

A

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

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

Type B Standards (Generic Safety Standards)

☆ Standards related to safety and safety equipment that can be applied to different types of machinery.

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

EN ISO 13855 : The positioning of protective equipment in respect of approach speeds of parts of the human body
EN ISO 13849-1 : Safety-related parts of control systems Part 1: General principles for design
EN1127-1 : Explosive atmospheres - Explosion prevention and protection Part 1: Basic concepts and methodology
EN60204-1 : Electrical equipment of machines Part 1: Specification for general requirements

B

B2: Standards on safeguards

EN ISO 13850 : Emergency stop equipment - Principles for design
EN574 : Two-hand control devices, functional aspects - Principle for design
EN ISO 14119 : Interlocking Devices Associated with Guards - Principles for Design and Selection
EN ISO 13856-1 : General principles for the design and testing of pressure sensitive mats and pressure sensitive floors
EN61469-1 : Electro-sensitive protective equipment Part 1: General requirements and tests
EN61496-2 : Electro-sensitive protective equipment
Part 2: Particular requirements for equipment using active opto-electronic devices
EN60947-1 : Low-voltage switchgear and controlgear Part 1: General rules

Type C Standards (Machine Safety Standards)

☆ Standards that specify detailed safety requirements for specific machinery.

EN 81 Series : Safety rules for the Construction and Installation of Lifts
EN 115 Series : Safety rules for the construction and installation of escalators and passenger conveyors
EN 201 : Rubber and plastic machines - Injection Moulding machines - Safety requirements
EN 415 Series : Safety of packaging machines
EN 422 : Rubber and plastics - Machines - Safety
EN 692 : Mechanical presses - Safety
EN 693 : Hydraulic presses - Safety
EN ISO 10218 Series : Manipulating Industrial robots - Safety
EN 869 : Safety requirements for high pressure metal diecasting units
EN 1010 Series : Technical safety requirements for the design and construction of printing and paper converting machines
EN 1034 Series : Technical safety requirements for the design and construction of paper making and finishing machines
(Section 3: winders, slitters, and plying machines)
EN 1114 Series : Extrusion molding machine safety
EN ISO 23125 : Safety of machine tools - turning machines
EN 12417 : Safety of machine tools - machining center
EN 13128 : Safety of machine tools - milling machines

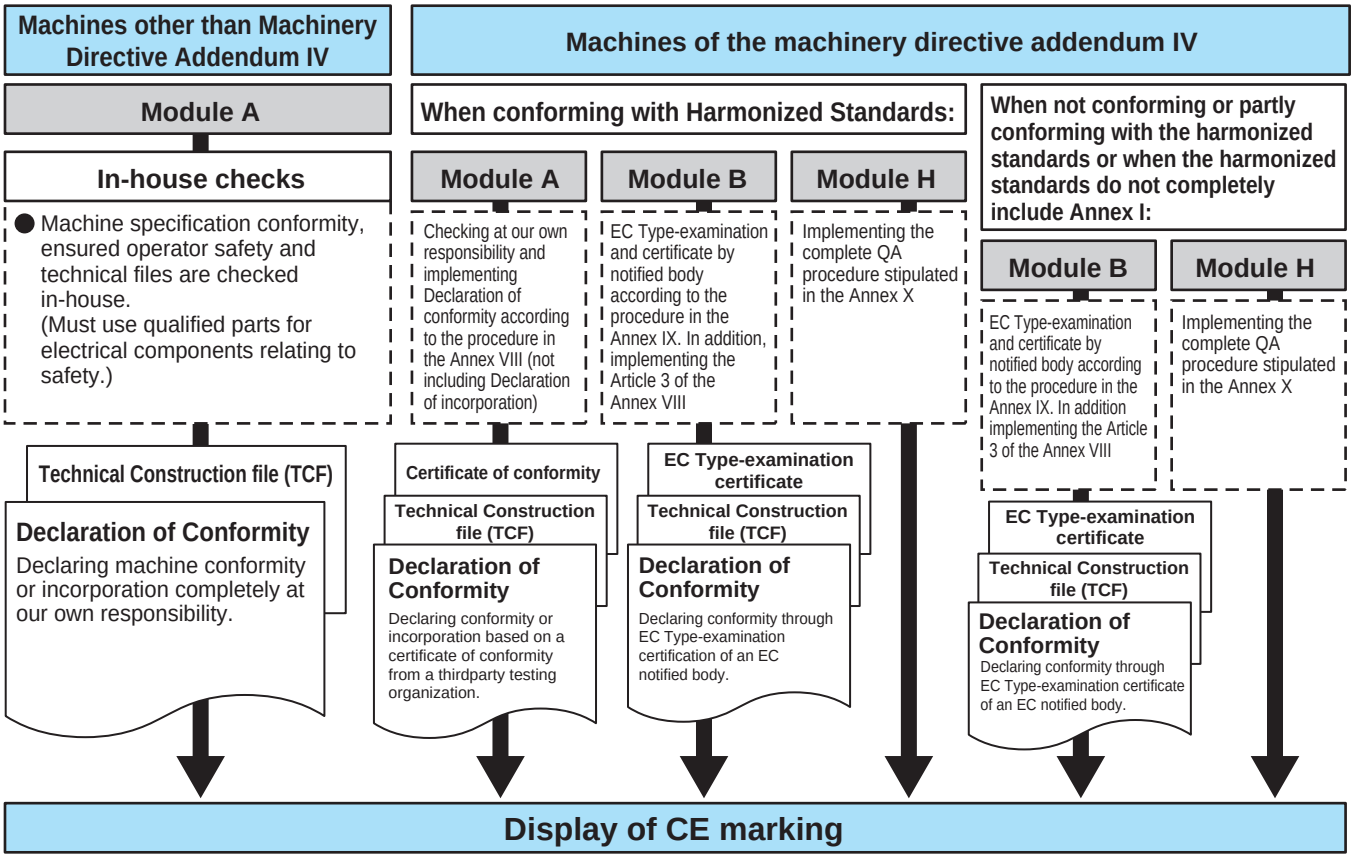
C

• Main EC Directives for which the CE Marking is mandatory (as of November, 2013)

Directive No.	Directive Name
2006/42/EC	Machinery
206/95/EC	Low Voltage devices
2004/108/EC	Electromagnetic compatibility (EMC)
2009/105/EC	Simple pressure vessels
94/9/EC	Equipment intended for use in Potentially Explosive Atmospheres (ATEX)
97/23/EC	Pressure Equipment
89/686/EEC	Personal Protective Equipment
95/16/EC	Lifts
99/5/EC	Radio and Telecommunications Terminal Equipment (R&TTE)
2004/22/EEC	Measuring instruments
2009/48/EC	Toys

Directive No.	Directive Name
2009/142/EC	Appliances burning gaseous fuels
00/9/EC	Cableway installations designed to carry persons
2011/65/EU	Directive on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment (recast)
93/15/EEC	Explosive for Civil uses
90/385/EEC	Medical devices: Active implantable
93/42/EEC	Medical devices: General
98/79/EC	Medical devices: In vitro diagnostic
92/42/EEC	Hot-water boilers (efficiency requirement)
2009/23/EC	Non-automatic weighing instruments
94/62/EC	Packaging and packaging waste
94/25/EC	Recreational craft (boats)

• Example of conformity evaluation based on machinery directive



• Machine requiring EC Type-examination by an EC notified body (Machines equivalent to the Machinery Directive Addendum IV)

(A) Machines

(1) Circular saw machines for cutting wood materials and meat (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 materials and meat
(5) Combined machines of the types referred to in (1) to (4) and (7)
(6) Tenoning machines
(7) Hand-fed vertical spindle moulding machines for working with wood and analogous materials.
(8) Portable chainsaws
(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 (OSHA) passed in 1970 to provide safe and healthy working conditions. Part 1910 of the 29th Code of Federal Regulations (CFR) 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.

For example, in 1976 ANSI approved the Underwriters Laboratories (UL), which was established by the fire insurance industry. Manufacturers of industrial robots in Japan and many other countries worldwide use the requirements for safety of industrial robots and robotic systems given in ANSI/RIA R15.06, which forms the basis of ISO 10218. ANSI/B11.19 safety standards for machine tools were established in 2003 and have become important standards.

1. Safety of Machine Tools

The American Society of Mechanical Engineers (ASME) collaborates in creating ANSI Standards, which are often adopted as ANSI B Standards.
The main safety standards for machine tools are stipulated by ANSI B11.

US Standards (B11 Standards)

Standard No.	Title
ANSI B11.1	Mechanical power presses
ANSI B11.2	Hydraulic power presses
ANSI B11.3	Power press brakes
ANSI B11.4	Shears
ANSI B11.5	Iron workers
ANSI B11.6	Turning machines
ANSI B11.7	Cold headers and cold formers
ANSI B11.8	Drilling, milling and boring machines
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	Automatic bar and chucking machines

Standard No.	Title
ANSI B11.14	Coil slitting machines
ANSI B11.15	Pipe tube and shape bending machines
ANSI B11.16	Metal powder 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 requirements for safeguarding
ANSI B11.20	Integrated manufacturing systems

ANSI B11.19 (Safeguarding when Referenced by the Other B11 Machine Tool Safety Standards - Performance Criteria for the Design, Construction, Care, and Operation) sets standards for barrier guards often referenced by other ANSI B11 standards. The main points in B11.19 are given on the next page.

Purposes for Using Safety Equipment

To ensure the safety of operators, safety and protective equipment is designed to prevent any hazardous machine motion or stop the machine when the operator's hand or other body part enters the hazard zone. The following items are demanded of safety and protective equipment.

1. Interlocked Protective Device

A protective barrier must be installed that is equipped with an interlock function that prevents the machine from operating unless the hazard is eliminated.
Safety related systems must be provided with a safety function that prevents the machine from starting due to a single fault.
Interlock equipment must be equipped with a tamper resistant function.

2. Presence-sensing Device

A device equipped with a function that detects the operator's hand or other body part, and outputs a signal to prevent any hazardous machine motion or to stop the machine.
The device must have a single fault detection function.
When mounted in a location that requires adjustment of the operating conditions, a blanking function must be provided.

3. Safety Mat

- The Safety Mat is a device that detects the presence of an operator who steps on it, and prevents any hazardous machine motion.
- The device must have a single fault detection function.

2. Safety of Industrial Robots

Safety items demanded of industrial robots by U.S. standards (ANSI/RIA R15.06)
Applicable scope (Section 1)

- Robot here refers to industrial robots and industrial robot systems.
- Date of ANSI standard implementation
  The standard has been implemented for industrial robots since June 2001.
  The standard has been implemented for industrial robot systems since June 2002.

Robot production, modification, re-assembly (Section 4)

- Electromagnetic compatibility (EMC) countermeasures for electrical devices
- Safety circuit designs (according to risk categories)
- Emergency stop buttons shall be shaped to fit the palm of the hand, or mushroom shaped, and shall be red on a yellow background.
- Enabling devices
  3-position switches

Safety and protective device performance (Section 5)

- Safeguarding devices
  Light Curtains, Safety Mats, two-handed operating devices

Installation of robot and robot systems (Section 6)

- Software or devices that are to be used with safety devices must be approved by an NRTL (U.S. Nationally Recognized Testing Laboratory).

Safeguarding of personnel (Sections 7, 8, 9, 10)

- Requirements for reducing risk due to risk assessment
  Requirements for robot risk reduction and design according to categories R1, R2 (A, B, C), R3 (A, B), and R4. (These categories differ from those of the ISO 13849-1 international standards.)

Safeguarding devices (Section 11)

- The safeguarding devices (Section 5) must be installed, so that an operator cannot bypass them and access hazard.

Maintenance of robot and robot systems (Section 12)

- Establishing continuous safe operation programs

Testing and start-up of robot and robot systems (Section 13)

- Testing and start-up procedures

Safety training of personnel (Section 14)

- Training programs

Annex (A to E)

- B Safety distances and direct opening action switches
- C Risk assessment

OMRON safety components can be used when constructing safety-related systems conforming with the requirements of ANSI B11.19 and ANSI/RIA R15.06.

• National Fire Protection Association (NFPA)

Some standards created by NFPA, which is founded for protection from fire and/or fire prevention are employed by ANSI.

Major standards related to industrial machinery

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

(3) Canada

• CSA

Safety standards created by Canadian Standards Association These standards cover electrical products, medical devices, machines, appliances, etc.

These regulations on electrical product safety are mandatory standards for electrical products used in Canada, because in all the 10 provinces and 2 territories in Canada electrical machines and appliances used by connecting to power source, regardless their types and/or quantity, must conform with safety standards of this CSA standards for electrical safety.

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-General Safety Requirements

• Pre-Start Health And Safety Reviews (PSHSR)

Ontario's provincial law for safety and health, called "Occupational Health and Safety Act R.R.O.1990, REGULATION 851" includes implementation provisions of PSHSR review by professional technicians qualified by the Employment and Social Development Canada for new machine installation.

(4) Japan

• Industrial Safety and Health Act

The amended Industrial Safety and Health Act went into effect in 2006, with the purpose of providing an environment for the promotion of independent safety and health activities in offices. For example, the Act includes requirements to investigate dangers and hazards in the workplace and take necessary measures against them.
The Act incorporates a framework to identify dangers and hazards, evaluate risks, and implement measures to reduce these risks.

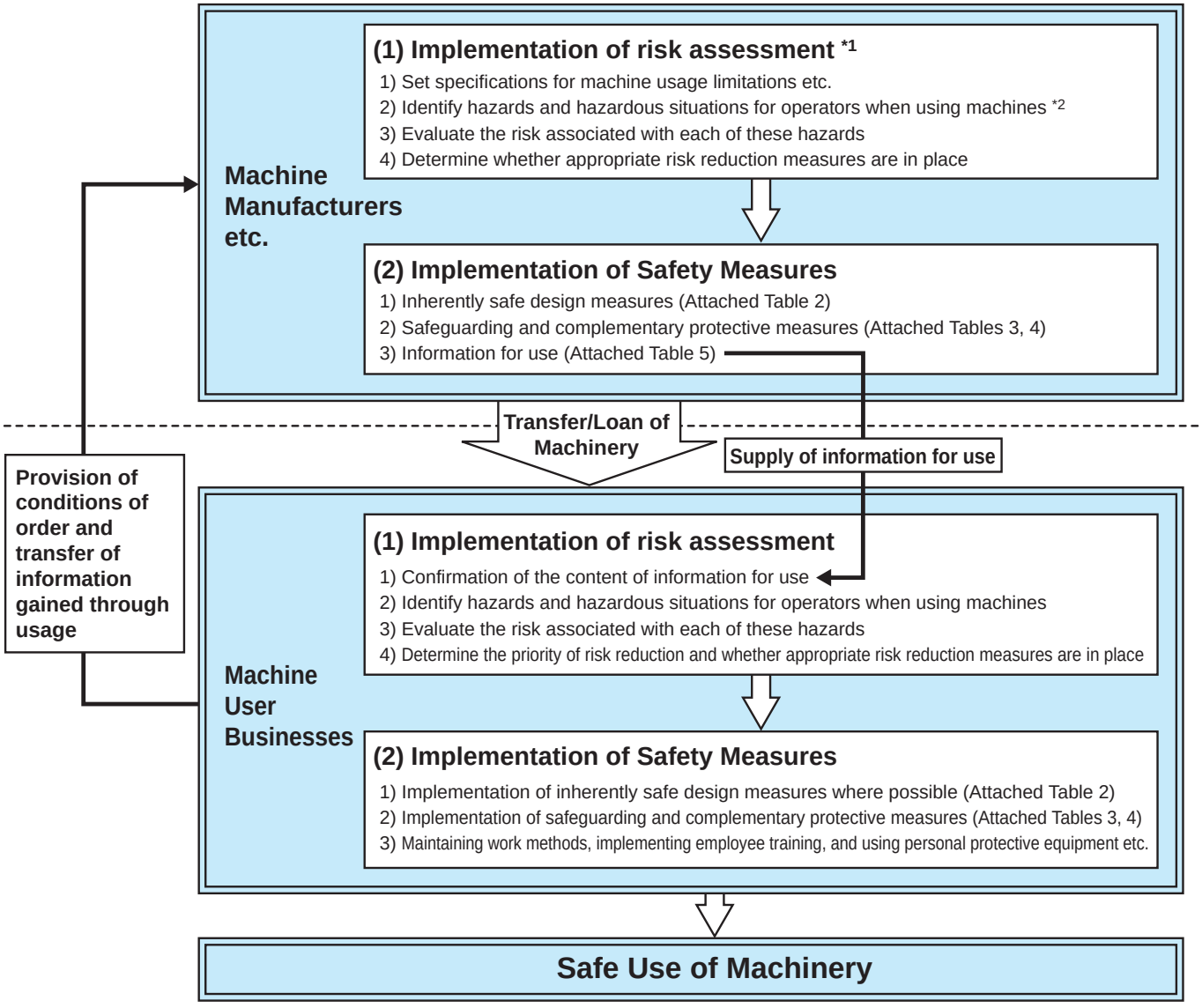
• Ordinance on Industrial Safety and Health

Individual hazard prevention standards are stipulated for machine tool, woodworking machine, food processing machine, press machine and shearing machine, centrifugal machine, crushing machine and mixer, rolling mills, etc. high speed rotating body, 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 Machinery Safety Standards

In July 2007, the Ministry of Health, Labor and Welfare in Japan amended its Guidelines for Comprehensive 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 to use in reducing safety risks and achieve designs that take safety into consideration in the manufacture of production equipment and machinery, and also request that users provide safety measures when they introduce and use the equipment and machinery.
In other words, 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 information in the Guidelines for Comprehensive Machinery Safety Standards.

Safety Procedure for Machinery



*1. In the Attachment, “risk assessment” is referred to as “assessment of hazards and dangers”.
*2. In the Attachment, “hazards” is referred to as “hazards and dangers”.

• JIS

The regulations and standards of individual countries must 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. Growing pressure to adopt international standards triggered a complete overhaul of the JIS standards, which were enacted under the Industrial Standardization Law, to bring them in line with the framework of the international IEC and ISO standards.The new JIS standards will be shifted to the hierarchical system comprised of type A (basic safety standards), type B (generic safety standards) and type C (machine safety standards) standards so that Japanese standards will conform to international 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 9718: 2013	Safety of machinery -- Safety distances to prevent hazard zones being reached by the upper and lower limbs	ISO 13857: 2008
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 9960-1: 2008 /A1: 2011	Safety of machinery -- Electrical equipment of machines - Part 1: General requirements	IEC 60204-1: 2005/A1: 2008
B 9961: 2008	Safety of machinery -- Functional safety of safety-related electrical, electronic and programmable electronic control systems	IEC 62061: 2005
B 9704-1: 2006 /A1: 2011	Safety of machinery -- Electro-sensitive protective equipment - Part 1: General requirements and tests	IEC 61496-1: 2004/A1: 2007
B 9704-2: 2008	Safety of machinery -- Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)	IEC61496-2: 2006
B 9704-3: 2004	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: 2001
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
TS B 62046: 2010	Safety of machinery -- Application of protective equipment to detect the presence of persons	IEC/TS 62046: 2008
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: 2000	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	IEC/CDV 61508-2: 1998
C 0508-3: 2000	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	IEC/FDIS 61508-3: 1998
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: 2000	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures	IEC/CDV 61508-7: 1998

(As of November 2013)

(5) China

• GB

Chinese national standards (GB: Guojia Biaozhun)

Standards for electrical equipment are produced based on IEC standards.

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

Mandatory National Standards (GB: Guojia Biaozhun)		International Standards
GB 16754-2008	Safety of machinery -- Emergency stop -- Principles for design	ISO 13850 : 2006
GB 18209.1/2/3-2010	Safety of machinery -- Indication, marking and actuation	IEC 61310-1/2/3 : 2007
GB 23821-2009	Safety of machinery -- Safety distances to prevent hazard zones being reached by the upper and lower limbs	ISO 13857 : 2008
GB 12265.3-1997	Safety of machinery -- Minimum gaps to avoid crushing of parts of the human body	ISO 13854 : 1996
GB 17888.1/2/3/4-2008	Safety of machinery -- Permanent means of access to machinery	ISO 14122-1/2/3 : 2001 ISO 14122-4 : 2004
GB 5226.1-2008	Safety of Machinery -- Electrical equipment of machines - Part 1: General requirements	IEC 60204-1 : 2005
GB 19436.2-2013	Safety of Machinery -- Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices	IEC 61496-2 : 2006
GB 28526-2012	Safety of Machinery -- Functional safety of safety-related electrical, electronic and programmable electronic control systems	IEC 62061 : 2005

Voluntary National Standards (GB/T: Guojia Biaozhun/ Tuijian)		International Standards
GB/T 15706-2012	Safety of machinery -- General principles for design - Risk assessment and risk Reduction	ISO 12100 : 2010
GB/T 19436.1-2013	Safety of machinery -- Electro-sensitive protective equipment - Part 1 : General requirements and tests	IEC 61496-1 : 2008
GB/T 16855.1-2008	Safety of machinery -- Safety-related parts of control systems - Part 1 : General principles for design	ISO 13849-1 : 2006
GB/T 16855.2-2007	Safety of machinery -- Safety-related parts of control systems - Part 2 : Validation	ISO 13849-2 : 2003
GB/T 18831-2010	Safety of machinery -- Interlocking devices associated with guards - Principles for design and selection	ISO 14119 : 1998/A1 : 2007
GB/T 19876-2012	Safety of machinery -- Positioning of safeguards with respect to the approach speeds of parts of the human body	ISO 13855 : 2010
GB/T 20438.1/2/3/4/5/6/7-2006	Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC 61508-1/3/4/5 : 1998 IEC 61508-2/6/7 : 2000

(As of November 2013)

• CCC

CCC: China Compulsory Certification mark system

CCC mark

Upon its entry into the World Trade Organization (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).

Products subject to the compulsory certification system: the "First list of the compulsory certification products" is expanded from 132 products in 19 groups (2003) to 157 products in 22 groups (revised in December, 2012). 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.

Electric wires and cables

Electric circuit switches, electronic equipment for protection or connection use

GB	International Standards
GB 14048.5-2008	IEC 60947-5-1-2003
GB/T 14048.10-2008	IEC 60947-5-2-2004
GB 14048.3-2008	IEC 60947-3-2005
GB 14048.2-2008	IEC 60947-2-2006
GB 14048.4-2010	IEC 60947-4-1-2009

Low-voltage electrical equipment

GB	International Standards
GB 14048.5-2008	IEC 60947-5-1-2003
GB 14048.6-2008	IEC 60947-4-2-2002

and others

(6) South Korea

• KS

South Korea became a WTO member and signatory to the TBT Agreement (Technical Barrier Treatment) in 1995, the year the WTO was created, and declared its commitment to a system of global cooperation. As a result, the Korean Industrial standards (KS) were established by the Industrial Standardization Law as part of an overall obligation to employ international standards, and are in line with the framework of the international IEC and ISO standards.

• KCs Marking System

ISHL (Industrial Safety and Health Low), Article 34 requires safety certification for harmful or hazardous machines, appliances, and equipment. Eleven machine/appliance items, eight safeguard items, and twelve personal protective equipment items are subject to safety certification (as of March, 2013).

Also the Article 35 in force since March 1, 2013 stipulates the Self-regulatory Safety Confirmation System. Manufacturers of machines/appliances subject to this system are required to confirm conformity and submit conformed document. Twenty-four machine/appliance product items, eight safeguard items, and four personal protective equipment items are subject to the Self-regulatory Safety Confirmation System (as of March, 2013).

Products that obtain a safety certification and products whose Self-regulatory Safety Confirmation 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 Industrial Safety Maintenance Law, Article 34, item 2, for product safety, product reliability, and the quality control capabilities of the manufacturer. Products that obtain a S-mark certification are not required to submit Self-regulatory Safety Confirmation System document, even if they are also subject to the Self-regulatory Safety Confirmation System.

The requirements are divided into Safety and EMC.

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)

Industrial standards created by the Standards Association of Australia

AS 4024.1 series is used as the safety standards applied to machinery. These standers are divided into 26 parts and created based on ISO standards and IEC standards.

Safety principles	AS 4024.1101	Terminology - General
	AS 4024.1201	Basic terminology and methodology
	AS 4024.1202	Technical principles
Risk assessment	AS 4024.1301	Principles of risk assessment
	AS 4024.1302	Reduction of risks to health and safety from hazardous substances emitted by machinery - Principles and specification for machinery manufacturers
Ergonomic principles	AS 4024.1401	Design principles - Terminology and general principles
Design of safety related parts of control systems	AS 4024.1501	General principles
	AS 4024.1502	Validation
Design of controls, interlocks and guarding	AS 4024.1601	Guards - General requirements for the design and construction of fixed and moveable guards
	AS 4024.1602	Principles for design and selection
	AS 4024.1603	Prevention of unexpected start-up
	AS 4024.1604	Emergency stop - Principles for design
Human body measurements	AS 4024.1701	Basic human body measurements for technological design
	AS 4024.1702	Principles for determining the dimensions required for openings for whole body access to machinery
	AS 4024.1703	Principles for determining the dimensions required for access openings
	AS 4024.1704	Anthropometric data
Safety distances and safety gaps	AS 4024.1801	Safety distances to prevent danger zones being reached by the upper limbs
	AS 4024.1802	Safety distances to prevent danger zones being reached by the lower limbs
	AS 4024.1803	Minimum gaps to prevent crushing of parts of the human body
Ergonomic requirements for the design of displays and control actuators	AS 4024.1901	General principles for human interaction with displays and control actuators
	AS 4024.1902	Displays
	AS 4024.1903	Control actuators
Indication, marking and actuation	AS 4024.1904	Requirements for visual, auditory and tactile signs
	AS 4024.1905	Requirements for marking
	AS 4024.1906	Requirements for the location and operation of actuators
	AS 4024.1907	System of auditory and visual danger and information signals

(As of November 2013)

(8) Relationships between Standard Numbers of Individual Countries and International Standards

Versions are different for each country.

Item	Country	Japan	Europe	U.S.A.	Canada	China	South Korea	Australia
TBT Agreement (WTO signatory)		○	○	○	○	○	○	○
International standards		National standards						
ISO	12100-1	JIS B 9700-1	EN ISO 12100-1	ANSI/ISO 12100-1	—	GB/T 15706.1	KS B ISO 12100-1	AS 4024.1201
	12100-2	JIS B 9700-2	EN ISO 12100-2	ANSI/ISO 12100-2	—	GB/T 15706.2	KS B ISO 12100-2	AS 4024.1202
	14121	JIS B 9702	EN ISO 14121	—	—	GB/T 16856	KS B ISO 14121	AS 4024.1301
	13849-1	JIS B 9705-1	EN ISO 13894-1	—	—	GB/T 16855.1	KS B ISO 13849-1	AS 4024.1501
	13850	JIS B 9703	EN ISO 13850	—	—	GB 16754	KS B ISO 13850	AS 4024.1604
	13852	JIS B 9707	EN ISO 13852	—	—	GB 12265.1	KS B ISO 13852	AS 4024.1801
	13853	JIS B 9708	EN ISO 13855	—	—	GB 12265.2	KS B ISO 13853	AS 4024.1802
	13857*1	—	EN ISO 13857*1	—	—	—	—	—
	13854	JIS B 9711	EN 349	—	—	GB 12265.3	KS B ISO 13854	AS 4024.1803
	13855	JIS B 9715	EN ISO 13855	—	—	—	KS B ISO 13855	AS 4024.2
IEC	60204-1	JIS B 9960-1	EN 60204-1	—	—	GB 5226.1	KS C IEC 60204-1	AS 60204.1
	61496-1	JIS B 9704-1	EN 61496-1	UL 61496-1	CSA-E61496-1	GB/T 19436.1	KS C IEC 61496-1	AS 4024.2
	61310-1	JIS B 9706-1	EN 61310-1	—	—	GB 18209.1	KS C IEC 61310-1	AS 4024.1904
	61310-2	JIS B 9706-2	EN 61310-2	—	—	GB 18209.2	KS C IEC 61310-2	AS 4024.1906
	61310-3	JIS B 9706-3	EN 61310-3	—	—	GB 18209.3	KS C IEC 61310-3	AS 4024.1907
Certification mark		—	CE-Mark *2	UL *3	CSA *3	CCC *4	S-Mark *5	—

(As of November 2013)

*1. A standard integrating ISO 13852 and ISO 13853
*2. Self-declaration is allowed for general machines in the Machinery Directive.
*3. UL and CSA are mutual certification systems.
*4. As of November 2013. Certification is not required for the field of industrial machinery.
*5. S-mark certification requires Labor Department approval of safety certification regulations in addition to standards conformity.

(9) 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 11 offices in 8 countries 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	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 November 2013)

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 European EN numbers and JIS standard numbers. (As of November 2013)

ISO 12100:2010

Safety of machinery - General principles for design -
Risk assessment and risk Reduction
EN standards: EN ISO 12100: 2010
JIS standards: JIS B 9700

- **Description**

Standards integrating ISO 12100-1, ISO 12100-2, and ISO 14121.

ISO 12100-1

Basic concepts, general principles for design
Part 1 : Basic terminology, methodology
EN standards: EN ISO 12100-1
JIS standards: JIS B 9700-1

- **Description**

This part of these standards defines the basic concepts of machinery safety and stipulates safety design procedures.
These standards were merged with ISO 12100-2 and ISO 14121 into ISO 12100 and revoked in 2010.

- **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 12100-2

Basic concept, general principles for design
Part 2 : Technical principles
EN standards: EN ISO 12100-2
JIS standards: JIS B 9700-2

- **Description**

This part of these standards describes the safety design procedures stipulated in part 1 in greater detail.
These standards were merged with ISO 12100-1 and ISO 14121 into ISO 12100 and revoked in 2010.

- **Main Points**

This part of these standards takes 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.), and step 5 (Inform and warn users about any residual risks.) given in part 1 and describes them in greater detail.

ISO 13849-1

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) These standards 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 categories and stipulates safety functions that control systems should have in every category.

ISO 13849-2

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

• Description

Regarding the verification of the conformity of claims in relation to ISO 13849-1 categories.

• Main Points

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

ISO 13850

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 devices.

• Main Points

(1) Electrical emergency stop devices must 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

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) Output signal shall be designated only when both control actuating devices are actuated less than or equal to 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

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 must 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

Pressure-sensitive protective devices
Part 1 : General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors
EN standards: EN 1760-1
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 must be category 2 or higher.
(3) Enclosure rating of mats must be IP54 or higher.

ISO 13856-2

Pressure-sensitive protective devices
Part 2 : General principles for the design and testing of pressure-sensitive edges and pressuresensitive bars
EN standards: EN 1760-2

• 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

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 two types of interlocking devices: those with and those without a guard lock.
(2) The guard must not allow machinery to operate until it is closed and it sends a stop command if it is open.

ISO 14121

Principle of risk assessment
EN standards: EN ISO 14121
JIS standards: JIS B 9702

• Description

These standards pertain to risk assessment in the safety design procedures described in ISO 12100-1. These standards were merged with ISO 12100-1 and ISO 12100-2 into ISO 12100 and revoked in 2010.

• Main Points

Assess risk is performed using the following systematic methodology:
A) Determine how the machinery will be used.
B) Check foreseeable hazardous events.
C) Identify risk elements based on hazardous events.
D) Assess the risk and design accordingly to reduce the risk.

IEC 60204-1

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

• Description

This part of these standards applies 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

This part of these standards stipulates 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 Section one-Electromechanical control circuit devices
EN standards: EN 60947-5-1
JIS standards: JIS C 8201-5-1

• Description

This part of these standards applies 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) This part of these standards consists 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

An IEC 60947-5 Series standard that stipulates 3-position enabling switches, for enable devices under the IEN60204-1 standard. 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) The 3-position enabling switch verification mark has been changed.

IEC 61310-1

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

This standard sets 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

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

• Description

This standard sets 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

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

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 devices, 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 either type 4, which complies with category 4 requirements in ISO 13849-1, or type 2, which complies with category 2 requirements in that same standard.
(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

Electro-sensitive protective equipment
Part 2 : Particular requirements for equipment using active opto-electronic protective devices
EN standards: EN 61496-2
JIS standards: JIS B 9704-2

• Description

This part of these standards applies to the type of ESPE protective equipment 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

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

• Description

This part of these standards applies 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 parts of the power drive system (PDS(SR)), and created based on the IEC 61508 Series Functional Safety Standards.

• Main Points

(1) Fourteen types of safety 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 failure exclusion are explicitly indicated.

IEC/TS 62046

Application of protective equipment to detect the presence of persons
EN standards: CLC/TS 62046
JIS standards: JIS B 62046

• Description

These standards stipulate requirements for selection/installation of light curtains and/or safety mats.

• 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

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

• Description

This standard specifies those matters applicable to the machinery portion of the industry as included in the IEC 61508 Series Functional Safety Standards.
This standard applies to the design and verification of safety related control systems that use electric, electronic, or 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 Failure per Hour).
(2) Integration by combining safety-related parts with subsystems
(3) Explicit indication of considerations for applying failure exclusion
(4) Calculation examples

EN 50205

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 operating 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

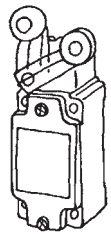
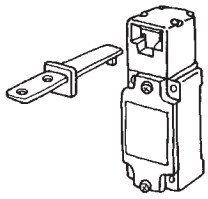
Principles of testing and certification for direct opening action switches

• 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, and an enclosure rating 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 an enclosure rating of IP54, and must not operate with a tool other than a special tongue.

(2) Terminology

1) General Terminology

• Pollution Degree (IEC 60664-1)

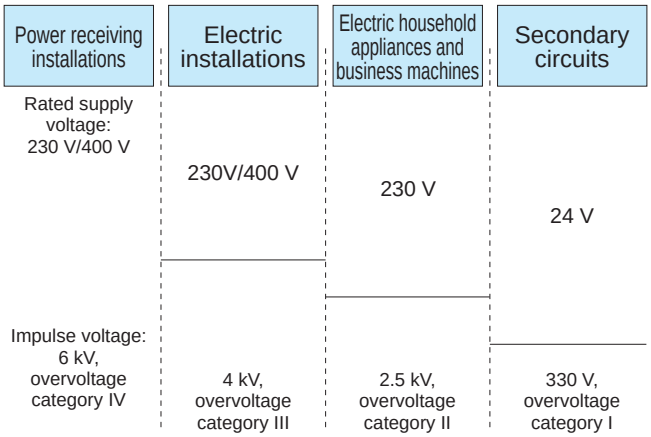
Pollution degree is the most important factor in deciding clearances (determined by the pollution degree and overvoltage categories) as well as creepage (determined by the pollution degree and CTI value), and it is classified into four degrees depending on the air pollution of the equipment used.

Pollution Degree 1	There is no pollutant or only a dry, non-conductive pollutant that has no effect on components. Pollution degree 1 is possible in clean rooms or other places with clean air.
Pollution Degree 2	There is only a non-conductive pollutant. The non-conductive pollutant may be conductive on occasions due to unexpected condensation. Pollution degree 2 is normal for electric products that are used inside control panels, electric household appliances, and business equipment.
Pollution Degree 3	There is a conductive pollutant or a dry, non-conductive pollutant that becomes conductive due to expected condensation. Pollution degree 3 is normal in ordinary factories.
Pollution Degree 4	There is a pollutant that is continuously conductive due to the presence of conductive dust, rainfall, or snowfall. Pollution degree 4 is normal for outdoor areas.

• Overvoltage Category (IEC 60664)

The overvoltage category classifies overvoltages into categories I, II, III and IV depending on whether the rated voltage is the rated impulse voltage or the rated voltage of the equipment as shown in the table below. Rated impulse voltage levels are set individually with respect to the rated voltages as shown in the figure below. The overvoltage category is one of the factors that decide spacing (determined by the overvoltage category and pollution degree).

Overvoltage category	Equipment description	Example
I	Devices connected to circuits with measures that limit excessive overvoltage to a low level.	Electronic circuits protected from power supplies by isolating transformers
II	Energy-saving equipment supplied by hard-wired power supply installations (i.e., electrical outlets)	Data processing equipment, portable tools, and electric household appliances
III	Equipment in hard-wired facilities where equipment reliability and efficiency are particularly important	Switches in hard-wired power supply installations and industrial equipment permanently connected to hard-wired power supply installations
IV	Equipment used in power receiving installations	Primary side overcurrent protection equipment

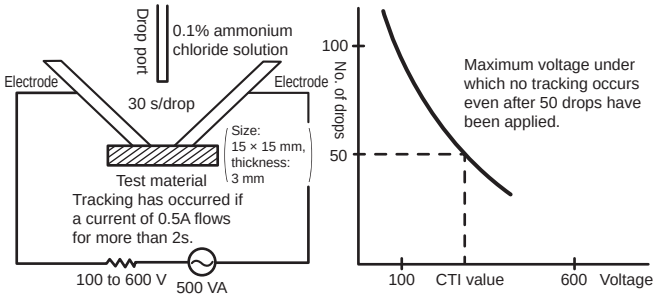


• CTI Value (IEC 60112)

CTI (Comparative Tracking Index)

Measurement of CTI Value

(The value is measured using method A from the CTI/PTI value measurement methods stipulated in IEC 60112.)
The CTI value of an insulation material is the maximum possible voltage that does not cause tracking when 50 drops of 0.1% ammonium chloride solution are dripped onto the material at a rate of 30 seconds per drop.



Materials Classified with CTI Value Range (IEC 60664-1)

Group I: CTI value greater than 600
Group II: CTI value greater than 400 but less than 600
Group IIIa: CTI value greater than 175 but less than 400
Group IIIb: CTI value greater than 100 but less than 175
Standard limit switches use group IIIa or better insulation material

• PTI Value (IEC 60112)

PTI (Proof Tracking Index)

Materials that conform to CTI values of 175, 250, 300, 375 and 500 are called PTI-175, PTI-250, PTI-300, PTI-375 and PTI-500 respectively. IEC 60335 and IEC 60065 stipulate that electric household appliances and consumer electronic appliances such as TVs, VTRs and radios must use PTI-175 or PTI-250 materials.

• 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 by direct and indirect contacts:
(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.

• Protection degree by enclosure (IP code) (IEC 60529: 2001)

IEC (International Electrotechnical Commission) Standard (IEC 60529: 2001)

IP-□□

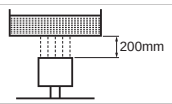
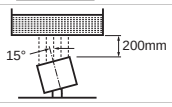
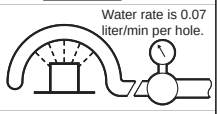
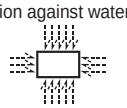
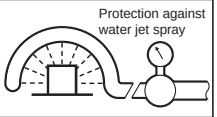
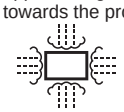
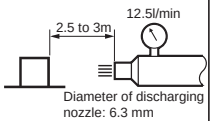
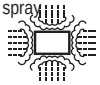
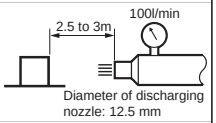
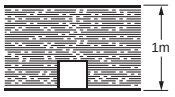
International Protection Mark
First symbol: Degree of protection against solid materials

Degree	Protection	
0		No protection
1		Protects against penetration of any solid object such as a hand that is 50 mm or more in diameter.
2		Protects against penetration of any solid object that is 12.5 mm or more in diameter. Any object with a diameter of 12 mm, such as a finger, will not reach a hazardous part even if it penetrates 80 mm.
3		Protects against penetration of any solid object such as a wire that is 2.5 mm or more is diameter.
4		Protects against penetration of any solid object such as a wire that is 1 mm or more in diameter.
5		Protects against penetration of dust of a quantity that may malfunction the protect or obstruct the safety operation of the product.
6		Protects against penetration of all dust.

*1. OMRON Test Methods
The Proximity Sensor's IP67 degree of protection was confirmed by performing the tests described in the table below and making sure that the sensing distance and installation resistance satisfied the performance specifications after repeating a heat shock cycle 5 times, consisting of immersing the Sensor in cold water at 0°C for 1 hour followed by hot water at 70°C for 1 hour.

*2. Precautions on OMRON Testing
Operating conditions for E2F Proximity Sensors: Underwater within 10 m
(1) No penetration of water when immersed in water for 1 hour at an atmospheric pressure of 2
(2) Satisfies sensing distance and insulation resistance performance specifications after the heat shock cycle described in *1 is repeated 20 times

Second symbol: Degree of protection against water

Degree	Protection		Test method (with pure water)
0	No protection	Not protected against water.	No test
1	Protection against water drop 	Protects against vertical drops of water towards the product.	Water is dropped vertically towards the product from the test machine for 10 min. 
2	Protection against water drop 	Protects against drops of water approaching at a maximum angle of 15° to the left, right, back, and front of vertical towards the product.	Water is dropped for 2.5 min each (i.e., 10 min in total) towards the product inclined 15° to the left, right, back, and front from the test machine. 
3	Protection against sprinkled water 	Protects against sprinkled water approaching at a maximum angle of 60° from vertical towards the product.	Water is sprinkled at a maximum angle of 60° to the left and right from vertical for 10 min from the test machine. 
4	Protection against water spray 	Protects against water spray approaching at any angle towards the product.	Water is sprayed at any angle towards the product for 10 min from the test machine. 
5	Protects against water jet spray approaching at any angle towards the product. 	Protects against water jet spray approaching at any angle towards the product.	Water is jet sprayed at any angle towards the product for 1 min per square meter for at least 3 min in total from the test machine. 
6	Production against high-pressure water jet spray 	Protects against highpressure water jet spray approaching at any angle towards the product.	Water is jet sprayed at any angle towards the product for 1 min per square meter for at least 3 min in total from the test machine. 
7	Protection underwater  *1	Resists the penetration of water when the product is placed underwater at specified pressure for a specified time.	The product is placed 1 m deep in water (if the product is 850 mm max. in height) for 30 min. 
8	Protection underwater  *2	Can be used continuously underwater.	The test method is determined by the manufacturer and user.

In-house Standards for Oil Resistance

Degree of protection	
Oilproof	No harmful effect when subjected to oil drops or oil spraying from any direction.
Oil-resistant	No penetration into internal parts when subjected to oil drops or oil spraying from any direction.

Note: Oil resistance is confirmed using oils and cutting oils stipulated by OMRON (equivalent to previous JEM standards).

2) Switch/Relay Terminology

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

The rated operational voltage (Ue) 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 (Ie) (IEC 60947-1)

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

• Conventional Free Air Thermal Current (Ith) (IEC 60947-1)

The Conventional Free Air Thermal Current (Ith) 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 (Ithe) (IEC 60947-1)

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

• Rated Impulse Withstand Voltage (Uimp) (IEC 60947-1)

The rated impulse withstand voltage (Uimp) 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 (Ui) (IEC 60947-1)

The rated insulation voltage (Ui) 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 (Ui) must be greater than that of the rated operating voltage.

• Switching Over Voltage (IEC 60947-1)

The switching over voltage 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.

• Name of contact rating (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	Load type	Closed thermoelectric current (Ithe)
A600	AC-15	10A

120V(Ue) ···	380V(Ue) ···	600V(Ue)
6A(Ie)	1.9A(Ie)	1.2A(Ie)

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

Utilization Category for Switching Elements
(Classified by switching path and current.)

Current	Category	Main application
AC	AC-12	Control of resistive loads and solid-state loads with photocoupler isolation.
	AC-13	Control of solid-state loads with transformer isolation.
	AC-14	Control of small electromagnetic loads (≤72 VAC).
	AC-15	Control of electromagnetic loads (>72 VAC).
DC	DC-12	Control of resistive loads and solid-state loads with photocoupler isolation.
	DC-13	Control of electromagnetic loads.
	DC-14	Control of electromagnetic loads with economic resistors in the circuit.

3) Sensor Terminology

• Type4 (IEC 61496-1)

Type 4 safety devices satisfy category 4 requirements prescribed in ISO 13849-1.

• ESPE (IEC 61496-1)

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

• AOPD (IEC 61496-2)

Active Opto-electronic Protective Device
AOPD protective devices are electro-sensitive protective devices that operate on the principle of detection by emitted and received light.

• Protective Height (IEC 61496-2)

The protective height is the range within which objects can be detected. The height is the length from the first optical beam to the last optical beam.

• 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 Function (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.
For F3SJ-A/B, the muting function can be added by attaching the F39-CN6 (Muting Cap).
For more details, refer to the catalogue.

• Test Rod or Test Piece (IEC 61496-2)

A 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 from the Detection Zone to the Danger Zone (ISO 13855)

Minimum Distance from the Detection Zone to the Danger Zone
The safety zone is the minimum distance that must be allowed from hazardous parts of machinery to the protection equipment.
It is prescribed so that machinery will turn OFF before someone entering the detection zone of the protection equipment reaches hazardous parts of the machinery.

• Light Beam Axis (IEC 61496-2)

The imaginal line that top beam and bottom beam of light curtain is connected. It is the reference line that is used to measure the Safety distance from hazardous parts of machinery to the light curtain.

• Effective Aperture Angle (IEC 61496-2)

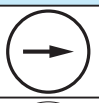
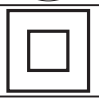
The effective aperture angle is the angle to which area sensors must be rotated to switch the output from ON to OFF. Measurements can be taken in two directions with lateral rotation as long as the rotation follows the axis formed by the light beams.

• Lock-out condition (IEC 61496-1)

A lock out 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) Other Terminology (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 EN 50205)	
Indicates double insulation (displayed on conforming products to IEC 60204-1)	

OMRON Corporation **Industrial Automation Company**
Tokyo, 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 SCIENTIFIC TECHNOLOGIES INC.
6550 Dumbarton Circle Fremont
CA 94555 U.S.A
Tel: (1) 510-608-3400/Fax: (1) 510-744-1442

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 (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:

Printed in Japan
Cat. No. Y107-E1-04 1214