Safety Standard ISO13849-1

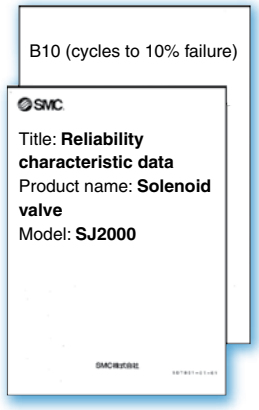
Corresponding to Category 2 to 4

Safety control system
by dual residual pressure release valve
with position detection sensor

SMC Support

Providing B10(d)/MTTF data

We will calculate and provide reliability characteristics concerning life and breakdown of individual parts.
(The customer should convert this to MTTFd.)



Providing operational components

We provide validated operational components that can be used to build safety control systems.

Note) Please note that these are not safety parts certified to the safety standard.

SMC

The ISO13849-1 safety standard has been extended globally since December 2011.
It is also incorporated into the standards in each country.
As an example, the specific work flow for Europe is explained below.

(Please note that the standards in each country are different – ANSI in America, JIS in Japan, GB in China - so the work flow will be different in each region.)

EN (Europe)
ANSI (America)
JIS (Japan)
GB (China)
•••

Machinery Directive (Europe)

ISO12100-1

Standard which specifies hazards and defines method for risk assessment

(1) Mechanical hazard
(2) Electrical hazard
(3) Thermal hazard
(4) Noise-related hazard
(5) Vibration-related hazard
(6) Radiation-related hazard
(7) Material-related hazard
(8) Ergonomics hazard
(9) Hazard relating to environment
(10) Hazard relating to combination

ISO13849-1

Standard for design and validation of safety related parts of the control system.
Methods to be adopted to achieve the necessary performance level using guard switches, interlock circuits etc.

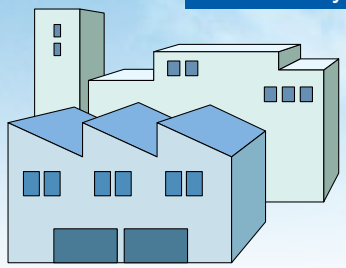
- Interlock device
- Emergency stop device
- ...

Machinery Directive (Europe) → ISO12100-1

ISO13849-1
(Check of safety control system)

(Other harmonized standards)

Certification



End user

Level "c" or above is necessary to ensure the safety of workers…. Let's instruct the equipment manufacturer.

Instruction

Equipment concept

The safety level of this equipment is "c" in the 5 stage evaluation from a to e.
(Refer to Q3&A on page 3 and ② Determining Performance Level (PLr) on page 5, for level of safety equipment.

Can be checked by a third party organization or consultant. The risk of injury to workers, safety equipment and control circuit are confirmed to determine the level of the hazard.

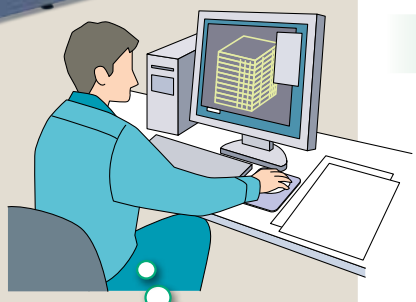
Equipment concept

Equipment manufacturer

Correspondence

Equipment design

Equipment certification



The end user has instructed that it must conform to **ISO13849-1***.
Let's consult SMC about the pneumatic equipment!

* Refer to Q2 on page 3, and pages 4 and 5.

ISO13849-1

SMC Support

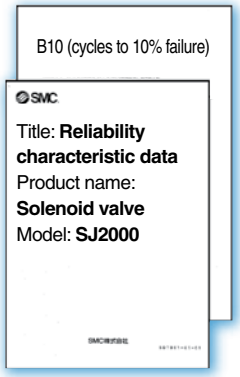
Dual residual pressure release valve with position detection sensor

This is a safety system valve. When the position detection sensor mounted to the valve detects that one of the two valves is out of position, the valve can be used with a safety system which vents the protected system when the position sensor signals a fault.

Refer to P.3 P.6 P.12 P.14 P.15

Providing B10(d)/MTTF data

We will calculate and provide reliability characteristics values concerning life and breakdown of individual parts.
(The customer should convert this to MTTFd.)



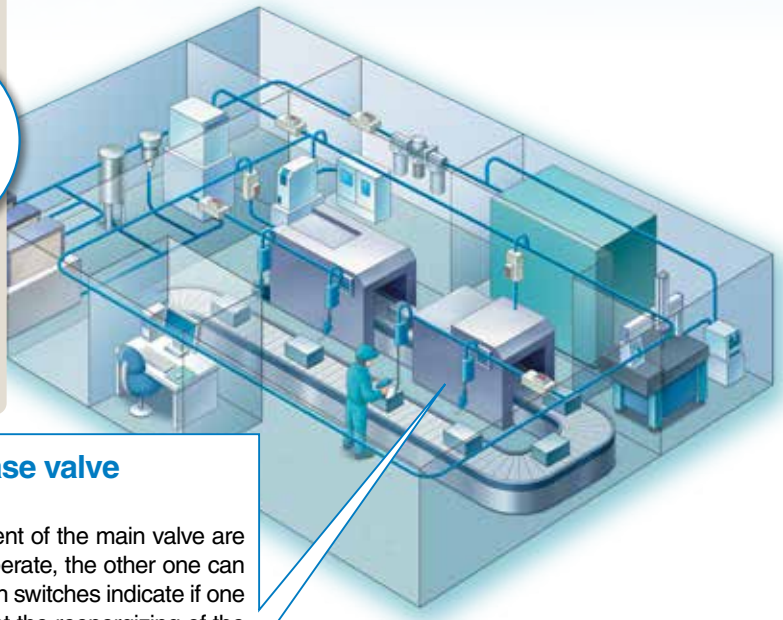
Refer to P.13

Supplying operational components

We provide validated operational components that can be used to build safety control systems.

Refer to P.16 to Back cover

Request



What is a dual residual pressure release valve with position detection sensor?

Two 3-port valves with switches to check the movement of the main valve are connected in series, so even if one of them fails to operate, the other one can safely release the residual pressure! The spool position switches indicate if one valve has failed to operate and can be used to prevent the reenergizing of the system until repaired.

SMC can supply products related to the safety control system.

Supply of products related to dual residual pressure release valve with position detection sensor

VG342-□-X87

VP544-□-X538

Position detection valve with redundancy

ISO13849-1 Simple! Q&A

Q1 What can SMC Sales do for customers in terms of the ISO13849-1 standard?

A See the three points below.

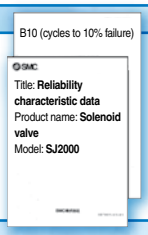
SMC Support

① Dual residual pressure release valve with position detection sensor

Two 3- port valves with switches to check the movement of the main valve are connected in series, so even if one of them fails to operate, the other one can safely release the residual pressure. Then, this valve can be used in the safety system where the spool position switches indicate if one valve has failed to operate and can be used to prevent the reenergizing of the system until repaired.

② Providing B10(d)/MTTF data

We will calculate and provide reliability characteristic values concerning estimated life of individual parts. (The customer should convert this to MTTFd.)



③ Supplying validated operational components.

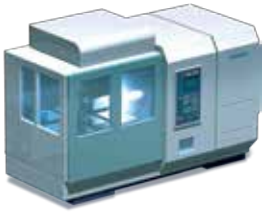
We provide components to ensure the safety of the safety control system.

Q2 Explained simply, what kind of standard is ISO13849-1?

A It is a standard that ensures that the design and construction of the safety related part of a machine control system is suitable to protect people from the hazards of the machine, based on the defined level of risk.

Q3 Who evaluates the required performance level for the equipment?

A The mechanical safety devices of the equipment (system) and the reliability of the equipment used should be evaluated.
This level is called PL (performance level). This is the evaluation criteria of the safety level of the equipment. Designer and manufacturer of the machine has the responsibility for the evaluation.
Then they have to perform the evaluation by themselves or they may ask a third party organization.
The responsibility remains with the manufacturer.



Q4 What happens after the level classification has been done?

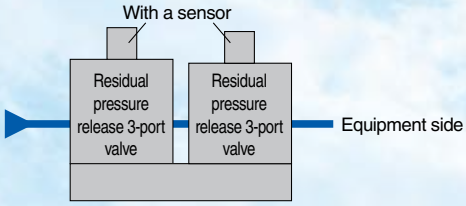
A After the evaluation criteria PLr has been determined, PL is found from the actual safety control system. This PL level is compared with PLr and if it is equal or above, it conforms to the standard, but if it is less, the measures are insufficient. If the measures are insufficient for the level of safety, the end user must introduce or modify equipment to ensure safety. According to these instructions, for example the equipment manufacturer will design parts and systems to ensure the safety of the equipment.

Q5 If a customer requires the ISO13849-1 standard, how should we respond?

A Take them the ISO13849-1 pamphlet. Explain about the services SMC can provide: ① dual residual pressure release valve with position detection sensor, ② providing data, ③ supplying validated operational components.

Q6 What is a dual residual pressure release valve with position detection sensor?

A It is a residual pressure release valve made to correspond to the safety standard. Two residual pressure release 3-port valves are connected in series (AND circuit), so even if one fails to operate, the other one will operate, so residual pressure is released safely. This is called a redundancy function. Also because it has a sensor to confirm the valve operation, the sensor shows whether the valve is operating correctly and reenergization can be prevented if not.



Q7 The standard is being enforced. Does existing equipment correspond to the standard?

A The standard came into force in December 2011 and new equipment must adapt.
Regarding existing equipment, if modification such as equipment change etc. is needed to increase the performance, it is necessary to conform to the standard. So safe components and circuits are used to conform to the standard. Even for modifications, there will be requirements for dual residual pressure release valve with position detection sensor, supply of data, and demand for safety equipment.

Q8 The standard mentions “redundancy”. What does this mean?

A Redundancy means that even if one part fails, the whole system will fulfill its required function. This is usually achieved by having dual channels of operation, such as dual valves, dual wiring, dual guard switches etc.
The dual residual pressure release valve with position detection sensor is said to have redundancy because two valves are connected in series, so even if one valve fails to operate, the other valve will function.

Q9 We often hear about “categories” in ISO13849-1. What does this mean?

A The categories mentioned in ISO13849-1 are one of the four elements to determine PL (Performance Level of the actual safety control system). There are five performance levels combining the configuration of the safety control system (hardware) and reliability (life, probability of failure, etc.).
There are five Categories: B, 1, 2, 3 and 4.

- **Category B, 1**.... Safety function can be accomplished by single channel. Single failure results in loss of safety function.
- **Category 2**..... Safety function can be accomplished by single channel and is automatically checked.
- **Category 3**..... It has redundancy so there is no loss of safety function with a single failure. The safety function must be checked before each use. An accumulation of undetected faults can cause loss of safety function.
- **Category 4**..... It has redundancy so there is no loss of safety function with a single failure. The safety function must be checked before each use. An accumulation of undetected faults does not affect the safety function. (Higher DC and MTTFd than Category 3.)

SMC responds to safety standard ISO13849-1.

The globalization of the concept of machine safety by international standards is currently accelerating.

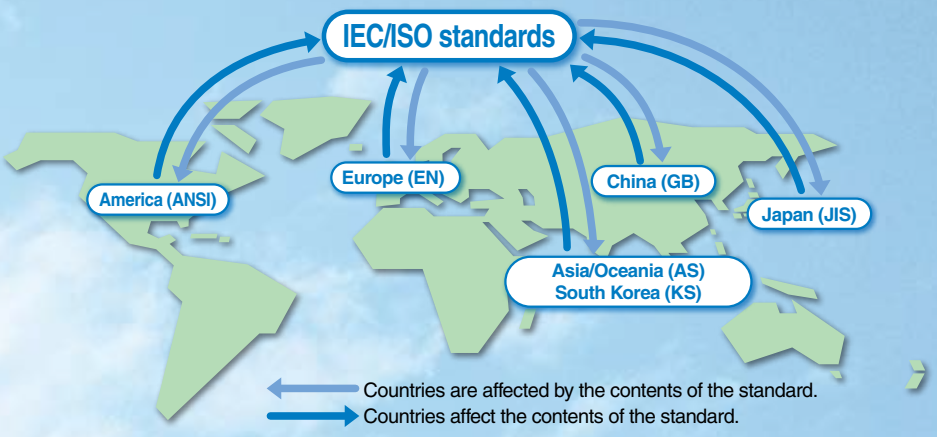
Conforming to international standards (IEC/ ISO standards) is becoming a main condition.

(Example: In Europe, the safety requirements of the Machinery Directive are mandatory and ISO13849 can be used to ensure compliance with this Directive, and equipment that does not conform to it cannot be distributed in the EU region. This safety concept is also being taken up in Japan, so safety construction done by conforming to international standards.)

Globalization is accelerating

Member countries of the WTO/TBT agreement must conform to international standards, and the standards in each country are aligned internationally.

Globalization concerning mechanical safety is accelerating.



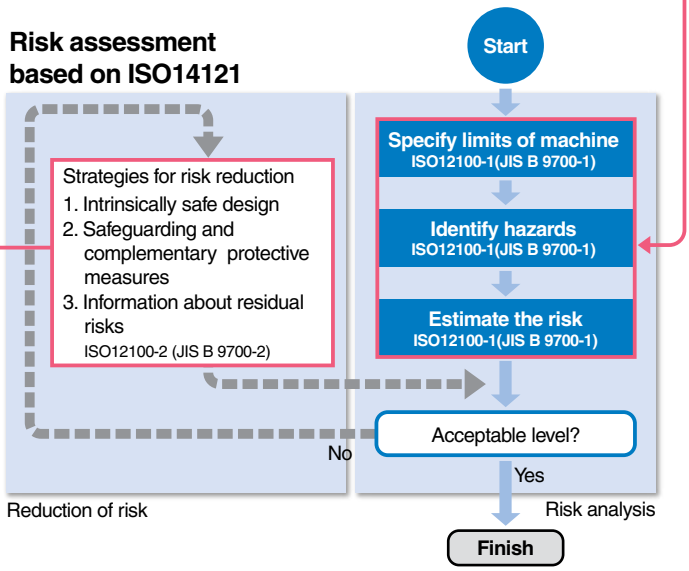
1 Risk Assessment (Analysis of Risk) Procedure

1 Risk analysis and risk reduction

The person responsible for design of a machine or process is required to design it such that it conforms to **necessary safety standards and restrictions**. To do that, first the "risk" of the whole machine is identified by a method based on **ISO14121 (JIS B 9702)** using the definition in **ISO12100 (JIS B 9702)**, the risk is estimated, and measures are taken to reduce it if there is a risk.

The risk generated in the entire machine is checked and reduced, based on the flow of ISO14121.

Risk assessment based on ISO14121



If this risk reduction is based on the safety control system, **the safety control system** is evaluated with **ISO13849-1** to reduce the risk. (In the past, EN954-1 was used.)

Estimation of risk

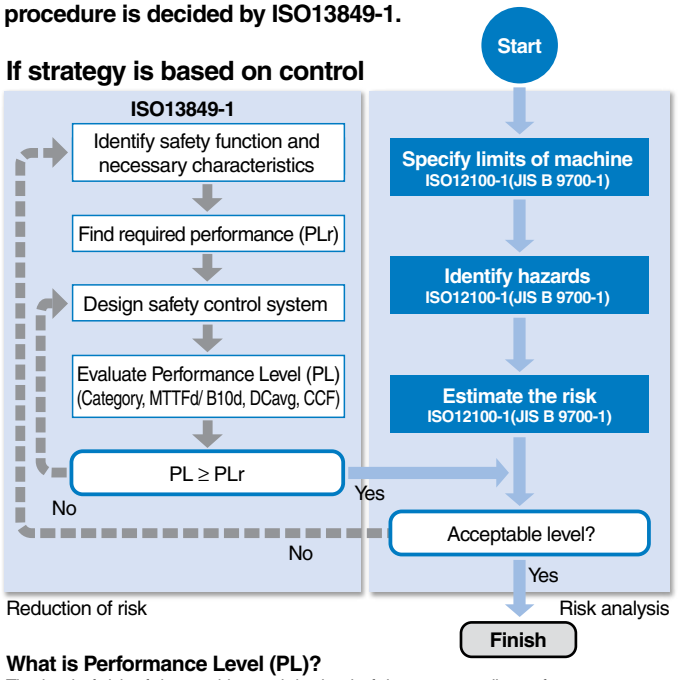
Mechanical hazards, the basis for estimation of risk, are defined as follows in ISO12100-1 (JIS B 9702).

(1) **Mechanical hazards** (crushing, getting caught, cutting etc.)
(2) **Electrical hazards** (electric shock, insulation failure, and static electricity etc.)
(3) **Thermal hazards** (fire, explosion, burns etc.)
(4) **Noise-related** hazards
(5) **Vibration-related** hazards
(6) **Radiation-related** hazards (low frequency, electromagnetic radiation etc.)
(7) **Material-related** hazards (hazardous substances etc.)
(8) **Ergonomics hazards** (human error etc.)
(9) Hazards relating to **operating environment**
(10) Hazards relating to **combination**

2 If risk reduction strategy is based on the safety control system

It is evaluated by Performance Level (PL), and the evaluation procedure is decided by ISO13849-1.

If strategy is based on control



What is Performance Level (PL)?

The level of risk of the machine and the level of the corresponding safety control system is comparatively evaluated in five stages "a" to "e".

2 Determining Performance Level (PL)

1 Determining Required Performance Level (PLr) as evaluation criteria

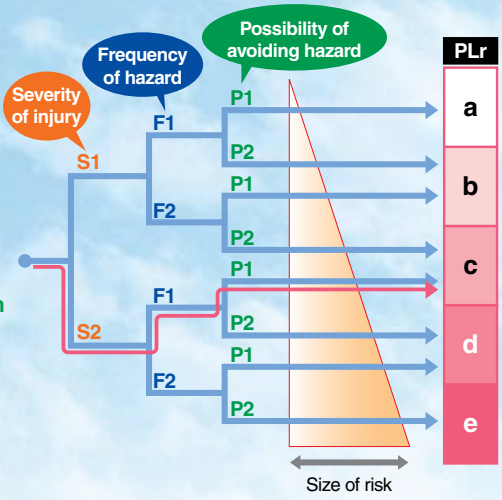
First, determine the Required Performance Level (PLr) which is the evaluation criteria.
Required Performance Level (PLr) is evaluated from Severity of Injury (S), Frequency and/or Exposure to Hazard (F) and Possibility of Avoiding Hazard (P).

ISO13849-1

S: Severity of Injury
S1: Slight injury
S2: Serious injury (after effects, death etc)

F: Frequency and/or Exposure to Hazard
F1: Seldom or short duration
F2: Often or long duration

P: Possibility of Avoiding Hazard or Limiting Harm
P1: Possible under specific conditions
P2: Impossible



Evaluation example

◎ **Determining PLr**
If injury is serious (S2), exposure to hazard is seldom (F1) and it is possible to avoid the hazard (P1), then the PLr is "c".

◎ **Determining PL**
From PL ≥ PLr,
the necessary PL is "c", "d" or "e".

To satisfy **the Performance Level (PL)**, it must be designed so that the combined value of the four parameters
❶Category ❷MTTFd
❸DCavg ❹CCF
exceeds the **Required Performance Level (PLr).**

Evaluation example

◎ **To satisfy PL,**
if category of equipment is 3
·**DCavg** = **Low**
·**MTTFd** = **Medium** or more
·**CCF**= **65** points or more

or
·**DCavg** = **Medium**
·**MTTFd** = **Low** or more
·**CCF**= **65** points or more
is necessary.

＊ See below for parameters of PL.

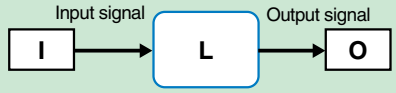
2 Determining Performance Level (PL) of the actual safety control system

The PL of the actual safety control system is determined separately from the Required Performance Level (PLr). To satisfy this PL, the combined value of four parameters (❶Category, ❷MTTFd, ❸DCavg and ❹CCF) must exceed the Required Performance Level (PLr).

Parameters of PL			Evaluation criteria
❶ Structure of hardware	Category	Architecture of safety control system (configuration of I, L, O). The category is composed of I (input equipment), L (logical operation equipment) and O (output equipment).	**B** **1** **2** **3** **4** 5 levels
❷ Life of components	MTTFd / B10d / Nop*	①Individual parts: 1. MTTF given by manufacturer 2. ＊ MTTF given in Annex C or if B10 is given, use: $MTTFd = \frac{B10d}{0.1 \times Nop}$ $B10d = 2 \times B10$ ＊ The designer of the machine needs to ascertain Nop (how many times that part operates in one year). ②Whole system: $MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$ $MTTFd = 2 \times MTTF$	**High** (30 years or more, less than 100 years) **Medium** (10 years or more, less than 30 years) **Low** (3 years or more, less than 10 years) 3 levels
❸ Reliability of system	DCavg / DC / MTTFd	①Individual parts ＊ Select DC from Table 1 of Annex E. Easy to calculate if using products certified to IEC/EN61508, IEC/EC62061, EN954-1 etc. ①Whole system: $DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$	**High** (99% or more) **Medium** (90% or more, less than 99%) **Low** (60% or more, less than 90%) **None** (less than 60%) 4 levels
❹ Certainty of design	CCF	＊ Score from checklist in Annex F is 65 or more. For Category 2 and above, CCF is required to be 65 points or more.	**Yes** (65 points or more) **No** (less than 65 points) 2 levels

＊ Refer to the ISO13849-1 standard.

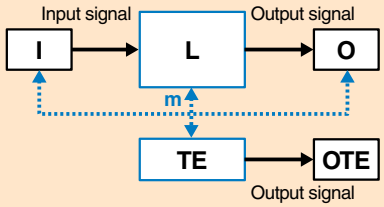
Differences in combinations and outline of Categories B, 1, 2, 3, 4.



Configuration applicable to Category B and Category 1

I : Input equipment (e.g. sensor)
L : Logical operation equipment
O : Output equipment (e.g. contactor)

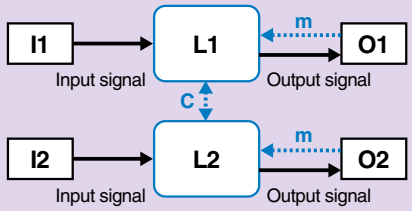
* MTTFd of Category 1 is higher than Category B, so probability of losing safety function is low, but a fault may lead to loss of safety function.



Configuration applicable to Category 2

m : Monitoring
TE : Testing equipment
OTE : Output of test result

* In Category 2, if a fault occurs, it may lead to a loss of safety function in the interval between two checks.



Configuration applicable to Category 3 and Category 4

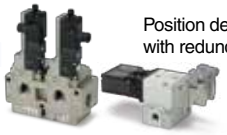
m : Monitoring
C : Cross monitoring

* In Category 3, safety function may be lost due to accumulation of undetected faults.
* The redundancy of architecture shown in these block diagrams can mean not just physical meaning but also internal logic from which the single fault tolerance is confirmed.

Category	Outline of requirements
B	Safety-related parts of control systems should achieve their functions, and should withstand expected stress (vibration, EMC etc.).
1	**Category B +** Use of well tried safety components
2	**Category B +** Safety function(s) shall be checked at appropriate intervals.
3	**Category B +** A single fault does not lead to the loss of safety function. Where practicable, a single fault shall be detected.
4	**Category B +** A single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to the loss of safety function.

Standard valves

Position detection valves



Position detection valves with redundancy

SMC can provide products related to the category of the system.

Related products such as dual residual pressure release valve with position detection sensor

The structure of the safety control system depends on the purpose of the machine, degree of hazard, scale of machinery and operation frequency.
For example if we think of an assembly process, there are differences depending on the purpose: robot, pick & place, semiautomatic etc. and the structure of equipment is different.
This classification of basic structure is what is called the Category of the safety control system.

SMC offers a full line-up of other recommended products related to safety.

Simplified procedure for evaluating PL achieved by SRP/CS

❶Category		B	1	2	2	3	3	4
❷MTTFd of each channel								
	Low	a	—	a	b	b	c	—
	Medium	b	—	b	c	c	d	—
	High	—	c	c	d	d	d	e
❸DCavg		None	None	Low	Medium	Low	Medium	High
❹CCF		None		65 points or more				

Example: If CCF is 65 or more, Category 3, MTTFd = Medium, and DCavg = Low, then PL is evaluated as "c".

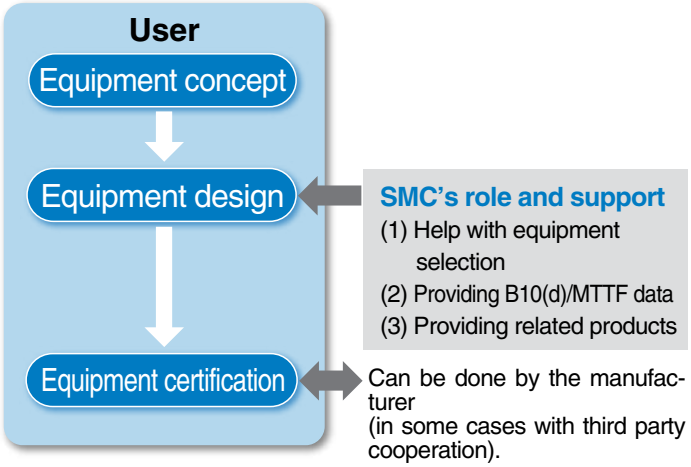
INDEX

Safety standard ISO13849-1 and role of SMC

ISO13849-1:2006 (Safety-related part of control system) was enacted to provide a quantitative and clear method of assessment (evaluation) of control systems for equipment and machines.
This ISO13849-1 is essential as a harmonized standard of the Machinery Directive (2006/42/EC).

For equipment manufacturers and end users considering safety design of equipment and machines, SMC will

(1) help with equipment selection.
(2) provide reliability data such as B10(d)*1 /MTTF data.
(3) provide operational products.



*1: **B10(d) data (MTTF only for electronic equipment that does not have wear-out failure)**
The reliability characteristics values (B10(d) or MTTF) provided by SMC are values particular to the components to be used.
The customer should separately convert these into the parameters for assessing the safety category within the equipment design specification.
These values are obtained under our standard (SMC internal test conditions), and are not guaranteed under the operating conditions of the customer's equipment.

1. Global trends in safety design

The JIS standards that form the standard for machine design in Japan now are being aligned with international standards ISO (International Standardization Organization) and IEC (International Electrotechnical Commission) standards.

As a background to this, the concept of machine safety is provided by an international standard and globalization is accelerating. Conformance to international standards (IEC/ISO standards) is becoming a major condition to satisfy machine safety.

For example, in Europe, the New Machinery Directive (2006/42/EC) which is one of the EU directives legally enforced in the EU, was made law on 29th December 2009. (Although it was enacted, the adaptation of the old standard EN954 was extended by two years. As a result, it was actually be enforced from 29th December 2011.) To conform to this new Machinery Directive, this ISO13849-1 is essential as a harmonized standard.
ISO13849-1 itself is not a compulsory standard, but in order to conform to this Machinery Directive, even in Japan pneumatics manufacturers including SMC are getting requests, particularly from equipment manufacturers and end users who are considering shipping equipment to Europe.

With this background, on a global level, people responsible for the design of machines or processes are required to make designs that conform to the necessary safety standards and restrictions.

Within these international standards, the standard which defines principles and performance required from safety control systems of equipment and machines used by pneumatic, hydraulic and electrical machines, is ISO13849-1.

2. Safety design of ISO13849-1

The architecture (safety construction) of safety control systems used before ISO13849-1:2006 were deterministic ones based on the internal construction of the equipment or machine. For example, the loss of the safety function due to the internal parts changing over time was not taken into consideration. So the idea of machine safety has changed to specifying it in terms of function and reliability. So in the revised ISO13849-1:2006, deterministic function and probabilistic reliability are amalgamated.
In addition to the existing structural definition, this gives a two-level definition which probabilistically evaluates the safety system, such as the life until dangerous failure at component level, and detection of dangerous failure.
With this definition, machine safety in the actual operating conditions of the machine can be quantitatively evaluated.

3. Safety of machinery / Safety-related parts of control system

ISO13849-1 provides general principles for machine design. It specifies safety requirements for the design of safety-related parts of the control system (SRP/CS) and general principles, and characteristics including the performance level necessary to perform the safety function.
It applies to all kinds of machines, regardless of the technology and type of energy used (electrical, hydraulic, pneumatic, mechanical etc).
ISO13849-2 covers validation. Using the theoretical grounds shown by the designer in the design, according to ISO13849-1, for safety-related parts of the control system, it specifies the procedure that should be followed to analyze the safety function and the category achieved, and validation by testing.

Risk assessment (analysis of risk) procedure

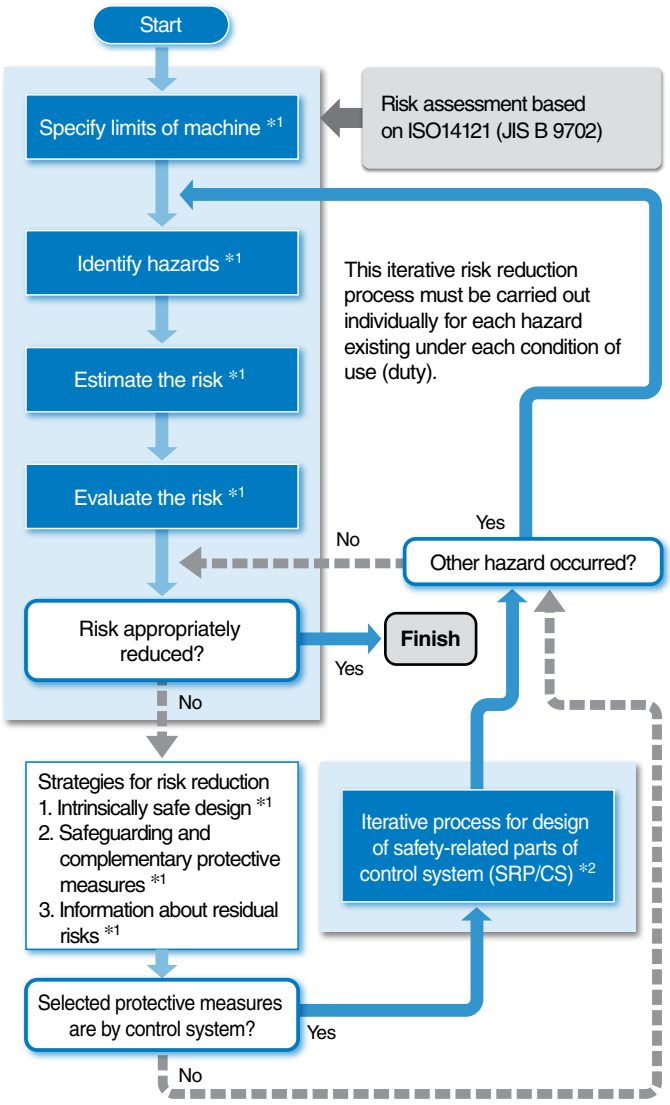
We will explain the specific method of safety design.

First, using the method based on ISO14121, identify the "risks of machine" of the machine as a whole, using the definitions in ISO12100 (JIS B 9702), estimate the risk, and take measures to reduce any risk. This is called risk assessment.

The machine safety hazards that risk assessment is based on, are defined as follows in ISO12100-1 (JIS B 9702).
(1) Mechanical hazards (crushing, getting caught, cutting etc)
(2) Electrical hazards (electric shock, insulation failure, and static electricity etc)
(3) Thermal hazards (fire, explosion, burns etc)
(4) Noise-related hazard
(5) Vibration-related hazard
(6) Radiation-related hazard (low frequency, electromagnetic radiation etc)
(7) Material-related hazard (hazardous substances etc.)
(8) Ergonomics hazard (human error etc)
(9) Hazard relating to operating environment
(10) Hazard relating to combination

Using this criteria, risk is determined, identified and estimated according to the following work flow, and if there is a problem, measures are considered to reduce the risk.

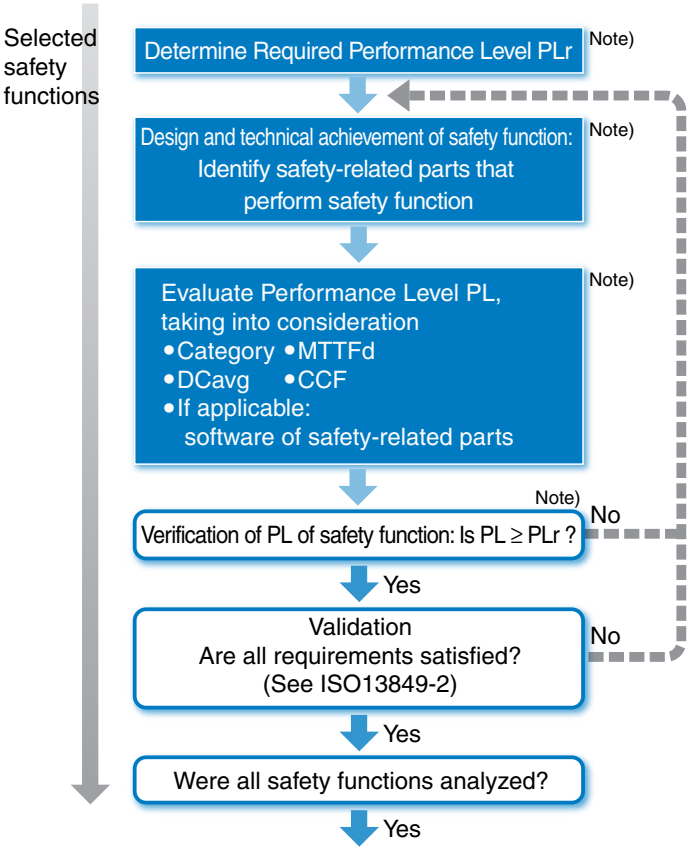
Overview of risk assessment/risk reduction



*1: Refer to ISO12100-1 (JIS B 9700-1).
*2: Refer to ISO13849-1 and "1" on page 10.

1. If risk reduction strategy is based on control

If this risk reduction is based on the control system, the machine safety of the safety control system is evaluated with ISO13849-1 aiming to reduce the risk. (In the past, EN954-1 applied to mechanical parts and IEC61508 applied to electronic parts.)



Note) Refer to ISO13849-1.

The standard for how to evaluate and reduce the risk of the safety control system in ISO13849-1 is Performance Level (PL).
Performance Level is a common rating scale to quantitatively show the definition of probabilistic reliability such as time elements at parts level. The level of risk and corresponding safety control system are comparatively evaluated on a 5 stage scale from “a” to “e”.

In order to satisfy Performance Level (PL), it must be designed such that the total value of four parameters (1) Category, (2) MTTFd, (3) DCavg and (4) CCF exceeds the Required Performance Level (PLr).

◎Determining Required Performance Level (PLr)

First the Required Performance Level (PLr) is determined. The Required Performance Level (PLr) is evaluated from Severity of Injury (S), Frequency and/or Exposure to Hazard (F) and Possibility of Avoiding Hazard (P).

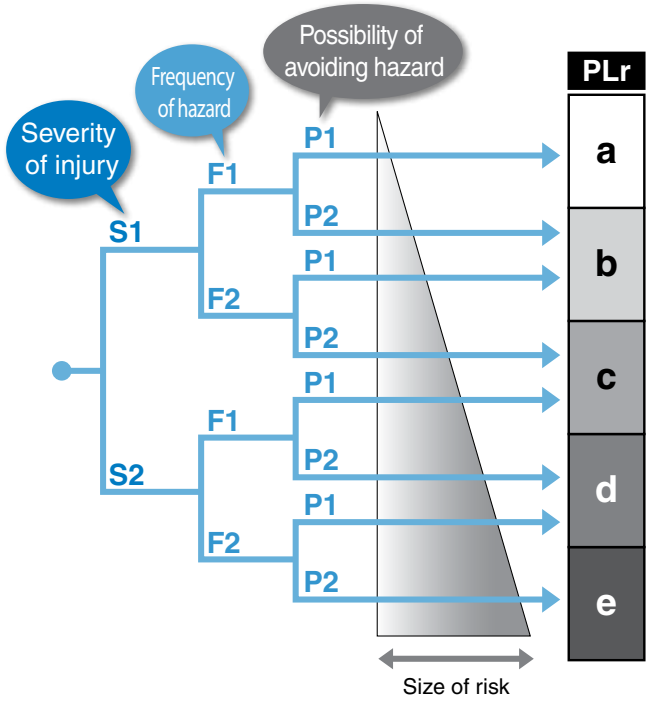
If injury is serious (S2), exposure to hazard is seldom (F1) and it is possible to avoid the hazard (P1), then the PLr is “c”.

ISO13849-1

S : Severity of Injury
S1: Slight injury
S2: Serious injury (after effects, death etc)

F : Frequency and/or Exposure to Hazard
F1: Seldom or short duration
F2: Often or long duration

P : Possibility of Avoiding Hazard or Limiting Harm
P1: Possible under specific conditions
P2: Impossible



◎Determining Performance Level of actual control system (PL)

Next, the Performance Level (PL) of the actual safety control system is determined with four parameters.
The PL of the actual safety control system level is determined separately from the Required Performance Level PLr.
PL can be determined from a combination of the four parameters (① Category, ② MTTFd, ③ DCavg and ④ CCF).

(1) **Category** : Structure of safety control system
(2) **MTTFd (B10d)** : Mean time to dangerous failure of components
(3) **DCavg** : Reliability of failure detection of the entire system
(4) **CCF** : Reliability of the entire system against foreseeable common cause failures

Parameters of PL | **Evaluation criteria**

1 Structure of hardware

Category → Architecture of safety control system (configuration of I, L, O)

The category is composed of I (input equipment), L (logical operation equipment) and O (output equipment).

→ **B**, **1**, **2**, **3**, **4** — 5 levels

2 Life of components

MTTFd
- **B10d**
- **Nop***

①Individual parts
1. MTTF given by manufacturer
2. ∗ MTTF given in Annex C or if B10 is given, use:

$$MTTFd = \frac{B10d}{0.1 \times Nop} \qquad B10d = 2 \times B10$$

∗ The designer of the machine needs to ascertain Nop (how many times that part operates in one year).

②Whole system

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

$$MTTFd = 2 \times MTTF$$

→ **High** (30 years or more, less than 100 years)
Medium (10 years or more, less than 30 years)
Low (3 years or more, less than 10 years) — 3 levels

3 Reliability of system

DCavg
- **DC**
- **MTTFd**

①Individual parts
∗ Select DC from Table 1 of Annex E.

Easy to calculate if using products certified to IEC/EN61508, IEC/EC62061, EN954-1 etc.

②Whole system

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

→ **High** (99% or more)
Medium (90% or more, less than 99%)
Low (60% or more, less than 90%)
None (less than 60%) — 4 levels

4 Certainty of design

CCF → ∗ Score from checklist in Annex F is 65 or more.

For Category 2 and above, CCF is required to be 65 points or more.

→ **Yes** (65 points or more)
No (less than 65 points) — 2 levels

∗ Refer to the ISO13849-1 standard.

The reliability parameters MTTFd and DCavg are found from mathematical formulae. CCF is found from a checklist.
Using standard values, MTTFd is classified into 3 levels, DCavg into 4 levels, and CCF into 2 levels.
PL is evaluated from these four parameters to find the corresponding PL.

As a result, PL is determined by a combination of these four factors: ① **Category**, ② **MTTFd**, ③ **DCavg and** ④ **CCF**.

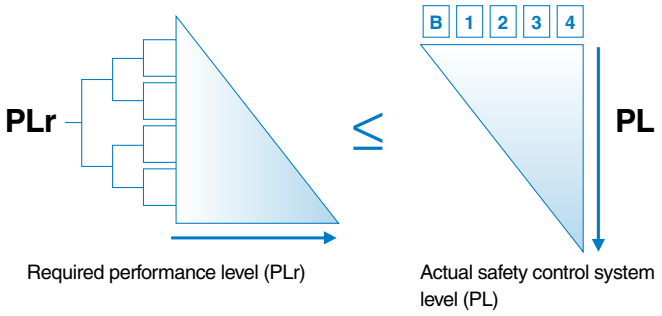
Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High
CCF	None		65 points or more				

Example: If CCF is 65 or more, Category 3, MTTFd = Medium, and DCavg = Low, then PL is evaluated as “c”.

2. Determining PL from four parameters

The Performance Level (PL) of the safety control system is required to be equal to or exceeding the Required Performance Level (PLr).



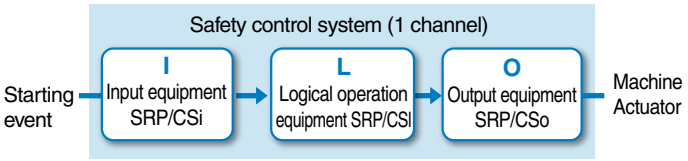
If PL, the result of combining the four parameters ① Category, ② MTTFd, ③ DCavg and ④ CCF, expressed as a, b, c, d or e, exceeds PLr, then it satisfies ISO13849-1.

Four parameters for determining PL

1. Category

This parameter concerns the construction of the safety-related parts of the control system (hardware). The construction to ensure safety depends on the purpose of the machine, degree of hazard, scale of machinery and operation frequency. The Category is a basic classification of this construction. The basic structure of the Category is illustrated as I (input equipment), L (logical operation equipment) and O (output equipment).

The safety function in ISO13849-1 is considered to be one channel where as I (input equipment), L (logical operation equipment) and O (output equipment) are connected in series.



Starting event: Manual operation of push-button, opening of door

(Safety control system)

I (input equipment): Detection equipment (sensor) of starting event
L (logical operation equipment): Relay sequence circuit
PLC control program
O (output equipment): Electromagnetic switch, output relay, solenoid valve

Machine actuator: Motor, fluid (hydraulic/ pneumatic) actuator

∗ Does not apply to fluid actuators.

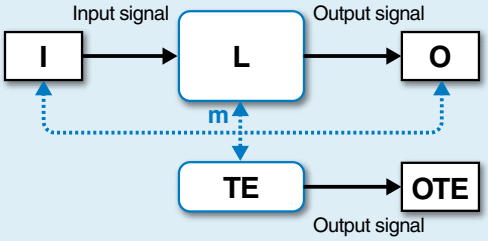
I is the detection equipment of starting event, pressure sensor, L is relay sequence circuit and PLC control program, O is electromagnetic switch, output relay, solenoid valve.

There are five categories, B to 4, as shown below. The structure of I (input equipment), L (logical operation equipment) and O (output equipment) of the safety control system is different. As the level increases, the requirements of each safety-related part also increase.

Configuration applicable to Category B and Category 1

I : Input equipment (e.g. sensor)
L : Logical operation equipment
O : Output equipment (e.g. contactor)

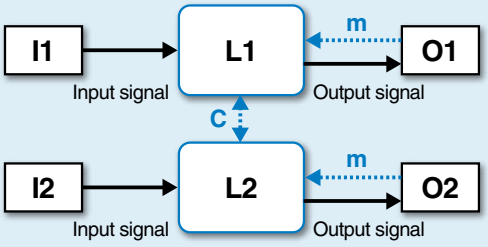
∗ MTTFd of Category 1 is higher than Category B, so probability of losing safety function is low, but a fault may lead to loss of safety function.



Configuration applicable to Category 2

m : Monitoring
TE : Testing equipment
OTE : Output of test result

∗ In Category 2, if a fault occurs, it may lead to loss of safety function in the interval between two checks.



Configuration applicable to Category 3 and Category 4

m: Monitoring
C : Cross monitoring

∗ In Category 3, safety function may be lost due to accumulation of undetected faults.
∗ The redundancy of architecture shown in these block diagrams can mean not just physical meaning but also internal logic from which the single fault tolerance is confirmed.

2. MTTFd

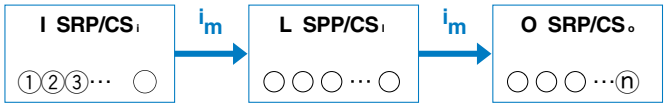
MTTFd indicates the mean time until the safety function is lost in a safety control system.

In order to evaluate PL, the equipment manufacturer needs reliability data (MTTF, B10) of individual parts used in the safety control system.
This is because the loss of the safety function is caused by the failure of parts making up the system, so it is based on the mean time to failure of individual parts.

The criteria of MTTFd are as follows.

MTTFd	
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

If one channel of I, L, O of the safety control system is made up of n parts, then MTTFd is as follows. In reliability engineering, the probability of a system breaking down is shown by the sum of the failure rates of the individual parts making up the channel. The same applies to dangerous failure. There is an inverse relationship between the dangerous failure rate and mean time to dangerous failure. Therefore the mean time to dangerous failure (MTTFd) of the whole system is found from the sum of the reciprocals of the mean time to dangerous failure of individual parts (MTTFdi).



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

MTTFd: Mean time to failure of individual parts

An additional note about the B10(d) data (MTTF only for electronic equipment that does not have wear-out failure) provided by SMC.
The reliability characteristics values (B10(d) or MTTF) provided by SMC are values particular to the components to be used.
The customer should separately convert these into the parameters for assessing the safety category within the equipment design specification.
Note that these values are obtained under our standard (SMC internal test conditions), and are not guaranteed under the operating conditions of the customer's equipment.

3. DCavg

The average self-diagnosis rate, an index of the reliability of the entire safety control system, is provided by DCavg (average Diagnostic Coverage).
The reliability of the function of the entire system, including software as well as parts, is evaluated.

DC	
None	DC < 60%
Low	60% < DC < 90%
Medium	90% < DC < 99%
High	99% ≤ DC

4. CCF

CCF (Common Cause Failure) is an index of reliability in terms of design, so that the function of the whole safety control system will not be lost due to a common cause. All parts of the safety-related parts of control system must be taken into consideration. Points are lost if a strategy is only partially achieved. It will pass if this score is 65 or more.

SMC's response

Regarding ISO13849-1, which is the safety standard for equipment and machinery, SMC supports equipment manufacturers and users in the following three ways.

(1) Help with equipment selection

Explanation of the parts of the standard relating to SMC's pneumatic equipment, and selection of suitable equipment that can be used in the equipment planned by equipment manufacturer and users.

(2) Providing B10(d)/MTTF data

We will provide MTTF/B10(d) data, which is one of the parameters needed when equipment manufacturers and users evaluate PL (Performance Level).

(3) Providing products for use in the safety circuit

SMC will supply products validated according to ISO 13849-2.

Recommended valves and wiring examples

Recommended valves for each Category and usage examples are shown below for control circuits that supply and cut off air, for equipment that uses air as an energy source. Note that these usage examples are for reference, and are one part of the safety system, so for actual circuits, we recommend getting confirmation from a third party certification organization about the safety of the system as a whole, as well as conforming to other related standards.

Category B, 1

Outline of requirements of Category

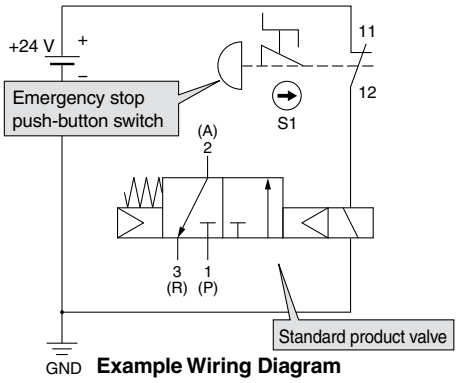
Category	Outline of requirements	System behavior	Principles used to achieve safety	MTTFd of each channel	DCavg (self diagnosis)	CCF (common cause failure)
B	Use of basic safety principles	Failure results in loss of safety function (probability is 1<B)	Selection of components	Low to medium	None	Not applicable
1	Requirements of B + well tried (components + safety principles)			High		

Combination of requirements of Category

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High

Can correspond with validated products.

Electrical equipment: Commercially available electrical equipment that can correspond to Category 1.



Example Wiring Diagram

Specified construction of requirements of Category

Configuration applicable to Category B and Category 1

I : Input equipment (e.g. sensor)
L : Logical operation equipment
O: Output equipment (e.g. contactor)

Category 2

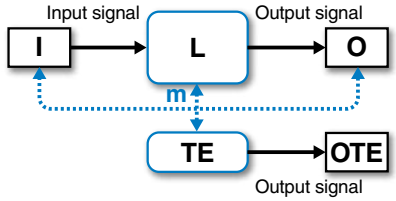
Outline of requirements of Category

Category	Outline of requirements	System behavior	Principles used to achieve safety	MTTFd of each channel	DCavg (self diagnosis)	CCF (common cause failure)
2	· Requirements of B + well tried safety principles · Safety function is checked at appropriate intervals.	Loss of safety function between checks	From construction	Low to high	Low to medium	65 points or more

Combination of requirements of Category

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High

Specified construction of requirements of Category



Configuration applicable to Category 2

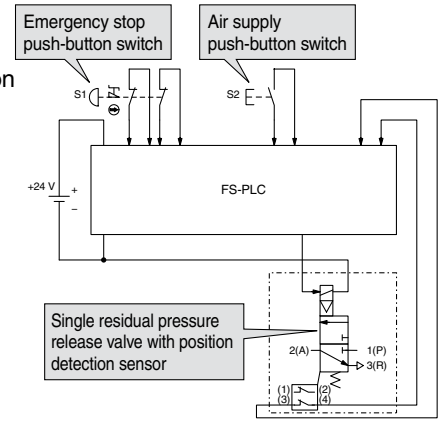
m : Monitoring
TE : Testing equipment
OTE: Output of test result

Recommended valves

Single residual pressure release valve with position detection sensor
(VP542-□-X536
VP742-□-X536)

Electrical equipment: Commercially available electrical equipment that can correspond to Category 2.

Example Wiring Diagram with Safety PLC (Category 2)



Category 3, 4

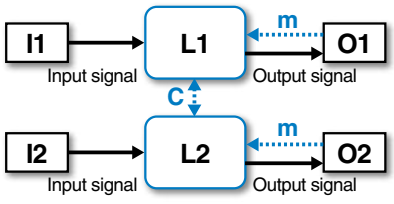
Outline of requirements of Category

Category	Outline of requirements	System behavior	Principles used to achieve safety	MTTFd of each channel	DCavg (self diagnosis)	CCF (common cause failure)
3	· Requirements of B + well tried safety principles · Safety function is not lost with a single fault. · Single fault can be detected.	· Safety function implemented when fault generated · All faults are not detected. · Safety function may be lost by accumulation of undetected faults.	From construction	Low to high	Low to medium	65 points or more
4	· Requirements of B + well tried safety principles · Safety function is not lost with a single fault, and · Single fault is detected before the next demand on the safety function. If this is not possible, an accumulation of faults must not lead to loss of the safety function.	· Safety function implemented when fault generated · Detection of accumulated faults increases probability of safety function (high DC). · Faults detected while it is safe		High	High	

Combination of requirements of Category

Category		B	1	2	2	3	3	4
MTTFd of each channel								
	Low	a	—	a	b	b	c	—
	Medium	b	—	b	c	c	d	—
	High	—	c	c	d	d	d	e
DCavg		None	None	Low	Medium	Low	Medium	High

Specified construction of requirements of Category



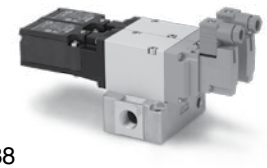
Configuration applicable to Category 3 and Category 4

m: Monitoring
C : Cross monitoring

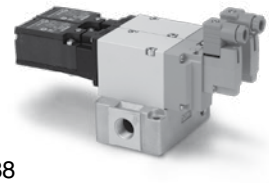
∗ The redundancy of architecture shown in these block diagrams can mean not just physical meaning but also internal logic from which the single fault tolerance is confirmed.

Recommended valves

Dual residual pressure release valve with position detection sensor



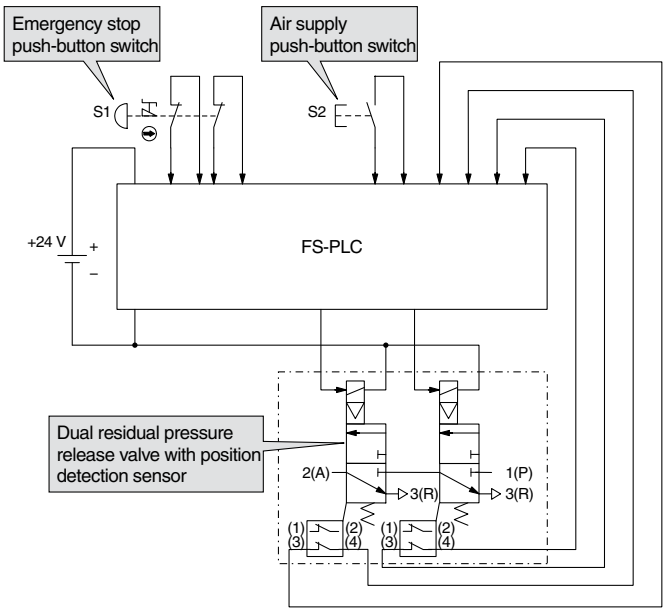
VP544-□-X538



VP744-□-X538

VG342-□-X87

Example Wiring Diagram with Safety PLC (Category 3, 4)



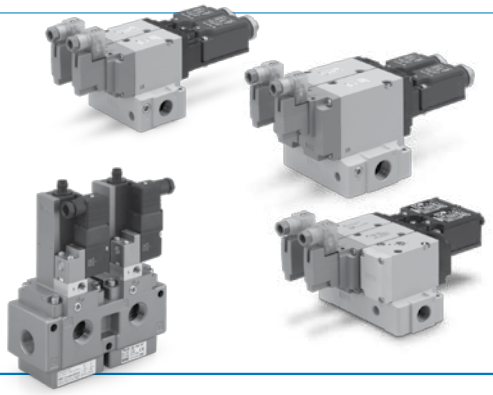
Pneumatic equipment products

The products below are available to support the safety of the equipment itself. However (other than VG342-□-X87, VP542-□-X536, VP544-□-X538, VP742-□-X536 or VP744-□-X538) these products are not certified to safety standard ISO13849-1; they are operational parts that can be used in the control system of the machine. We recommend getting confirmation from a third party certification organization about the safety of the actual control system as a whole.

1. Directional control equipment

Dual residual pressure release valve with position detection sensor

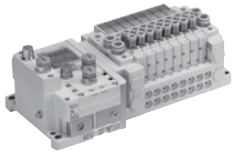
· Position detection possible
· Position detection possible with redundancy

Category	Model		Feature / Specification
Category **2**	Residual pressure release valve VP542-□-X536 VP742-□-X536		· Valve position can be detected.
Category **3, 4**	Dual residual pressure release valve VP544-□-X538 VP744-□-X538 Dual residual pressure release valve with soft start-up function VP544-□-X555 Dual residual pressure release valve VG342-□-X87		· Valve position can be detected. · Valve has 2 stations, so if one of them fails to operate, residual pressure is released by the remaining valve.

Please refer to P. G. Information for details.

Specification with residual pressure release valve

· Can hold intermediate stop position for a long time.
· Air supply can be stopped for each valve.

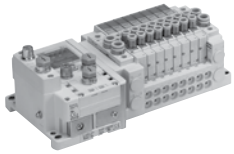


Applicable models

Name	Series
5 port solenoid valve	**SY3000/5000**

Back pressure prevention valve specification

· Prevents malfunction of actuator due to back pressure.

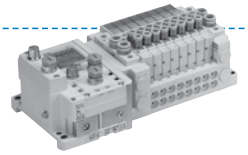


Applicable models

Name	Series
	Body ported type
4 port solenoid valve	**SJ**
5 port solenoid valve	**SY3000/5000**
5 port solenoid valve	**S0700**
5 port solenoid valve	**VQ**
5 port solenoid valve	**VQC**
5 port solenoid valve	**VQZ**
5 port solenoid valve	**SQ**
5 port solenoid valve	**VQ7**

Specification with switch

· Signal of each valve cut off individually.

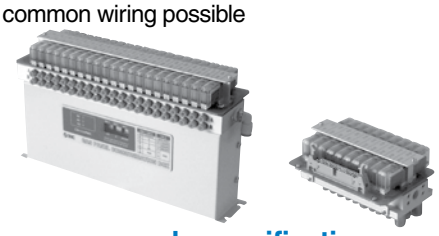


Applicable models

Name	Series
5 port solenoid valve	**SY3000/5000**

Specification with interlock

· Individual common wiring possible

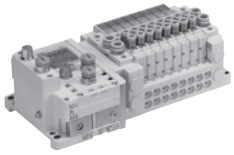


Applicable models

Name	Series
5 port solenoid valve	**SV**
5 port solenoid valve	**VQC**

Separate power supply specification

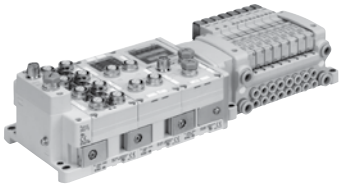
· Signal of each valve individually cut off for each power supply.



Applicable models

Series	Applicable valves
EX250	SY3000/5000 VQC1000/2000/4000, S0700

With disconnection short-circuit detection function



Applicable models

Series	Applicable valves
EX600	SY3000/5000 VQC1000/2000/4000, S0700

Two-handed operation specification

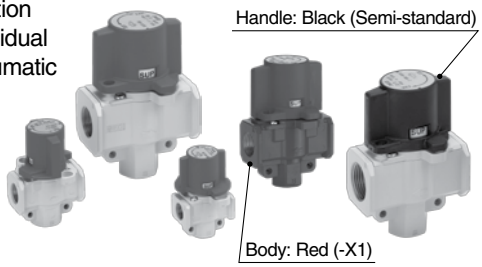
· Safety measures equipment of circuit
· Safety measures by signal output when operated with two hands simultaneously

Applicable models

Name	Series
Two hand control valve	**VR51**

Residual pressure relief specification

· Accident prevention by release of residual pressure in pneumatic line



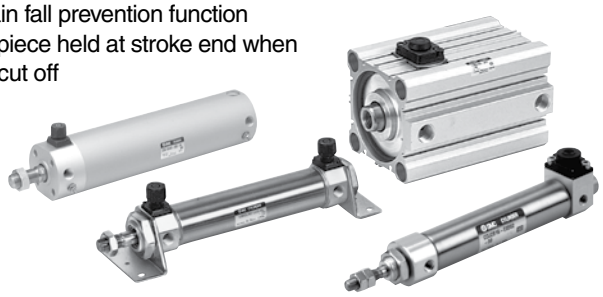
Applicable models

Name	Series
Residual pressure relief 3 port valve (Conforming to OSHA standard/ Pressure relief 3 port valve with locking holes)	**VHS**

2. Actuators

End lock specification

· Certain fall prevention function
· Workpiece held at stroke end when air is cut off



Basic type air cylinders

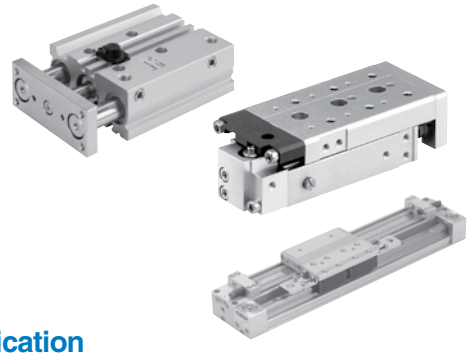
Shape	Model	Bore size
Round	**CBJ2**	ø16
	CBM2	ø20 to ø40
	CBG1	ø20 to ø100
	CBA2	ø40 to ø100
	MBB	ø32 to ø100
Square	**CBQ2**	ø20 to ø100

Pneumatic equipment products

The products below are available to support the safety of the equipment itself. So they are not certified to safety standard ISO13849-1; they are component operational parts that can be used in the control system of the machine. We recommend getting confirmation from a third party certification organization about the safety of the actual control system as a whole.

End lock specification

· Certain fall prevention function
· Workpiece held at stroke end when air is cut off



Guide cylinders

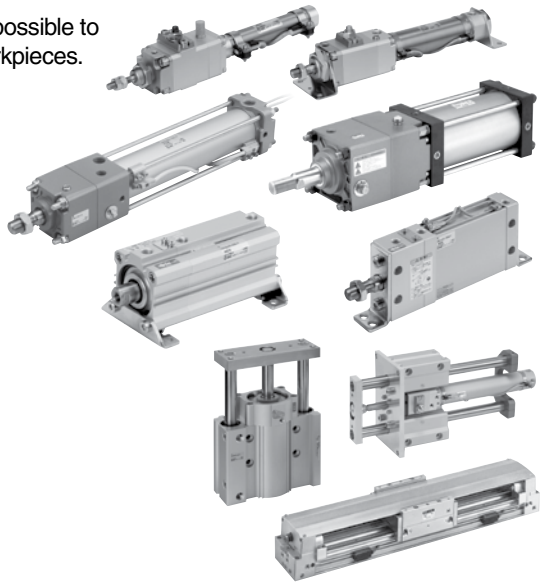
Type	Model	Bore size
Shaft guide	**MGG**	ø20 to ø100
	MGP	ø20 to ø100
	CXS	ø6 to ø32
	CXW	ø10 to ø32
	MGZ	ø40 to ø63
	MTS	ø12 to ø40
Linear guide	**MXS**	ø8 to ø25
	MXQ	ø8 to ø25

Mechanically jointed rodless cylinder

Type	Model	Bore size
Linear guide	**MY1H**	ø16 to ø40

With lock specification

· Fall prevention function by emergency stop (not safety products)
· Locking is possible to suit the workpieces.



Basic air cylinders

Type	Model	Bore size
Round	**CLJ2**	ø16
	CLM2	ø20 to ø40
	CNG	ø20 to ø40
	CNA2	ø40 to ø100
	MNB	ø32 to ø100
	CNS	ø125 to ø160
	CLS	ø125 to ø250
	CL1	ø40 to ø160
	C95N	ø32 to ø100
Square	**CLQ**	ø20 to ø100
	RLQ	ø32 to ø63
Rectangular	**MLU**	ø25 to ø50

Guide cylinders

Type	Model	Bore size
Shaft guide	**MLGP**	ø20 to ø63
	MLGC	ø20 to ø40
	CLK1	ø32 to ø63

Mechanically jointed hy-rodless cylinder with brake

Type	Model	Bore size
Cam follower guide	**ML1C**	ø25 to ø40

3. Flow control equipment

Residual pressure release specification

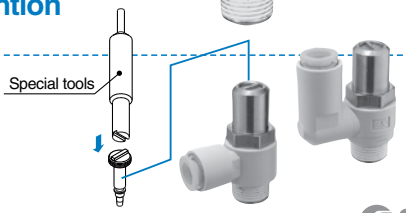
· Residual pressure can be instantly released by pressing a button on the product.

Applicable models

Name	Series
Speed controller with residual pressure release valve with One-touch fitting	**AS□□□1FE**
Residual pressure release valve with One-touch fitting	**KE□**

Mis-operation prevention specification

· Prevents unintended manual operation.



Applicable models

Name	Series
Speed controller adjustable by flat head screwdriver	**AS□□□1F-D**
Tamper proof speed controller	**AS□□□1F-T**

Intermediate stop/drop prevention specification

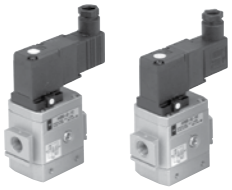
· Allows temporary stop and speed control of cylinder.

Applicable models

Name	Series
Speed controller with pilot check valve	**ASP**
Check valve	**AK**

Quick extension prevention specification

· Possible to cut off supply for rapid exhaust. (Soft start-up valve)
· Flow control is possible in two directions. (Dual speed controller)



Applicable models

Name	Series
Soft start-up valve	**AV**
Dual speed controller	**ASD**

4. Detection switches

Mis-operation prevention specification

· Unintentional changes prevented by password input

Sensor/amp integrated type

Name	Series
2-color display high precision digital pressure switch	**ZSE30A(F)/ISE30A**
	ZSE40A(F)/ISE40A
Compact digital pressure switch	**ZSE10(F)/ISE10**

Sensor/amp separate type

Name	Series
Compact pneumatic pressure sensor	**PSE53□**
	PSE54□
Low differential pressure sensor	**PSE55□**
Pressure sensor for general fluids	**PSE56□**
Multi-channel digital pressure sensor controller	**PSE200**
2-color display digital pressure sensor controller	**PSE300**

Residual pressure check specification

· Allows visual confirmation of residual pressure in cylinder, production line.

Applicable models

Name	Series
Residual pressure indicator for air	**CB-97XH**

Revision history

Edition B
* Changed from B10 to B10(d).
* Example wiring diagram with safety PLC corrected.
* Recommended pneumatic equipment products revised.
* Number of pages decreased from 24 to 20. UT

SMC Corporation of America
10100 SMC Blvd., Noblesville, IN 46060
www.smcusa.com

SMC Pneumatics (Canada) Ltd.
www.smcpneumatics.ca

(800) SMC.SMC1 (762-7621)
e-mail: **sales@smcusa.com**
International inquiries: **www.smcworld.com**